War's impact on fertilisers stirs food producer fears

AFP | Paris

Even as Gulf tanker traffic slowly resumes, the road back to normal food production will be long and arduous, given the war's impact on fertiliser supplies, the UN has warned.

With factories shuttered and soaring gas prices driving up production costs around the world, fertiliser prices have risen across the board and are unlikely to fall back easily.

"If the Strait of Hormuz reopened immediately, i.e. not only a ceasefire but vessels moving, the impact would be significantly positive -- but incomplete and uneven," the Food and Agriculture Organization's chief economist Maximo Torero told AFP.

A farmer sprinkles fertiliser on crops in a field on the outskirts of Amritsar

"The FAO is clear that damage has already been done."

According to Argus Media, the price of urea from the Middle East has, for example, risen by 70 percent in a matter of weeks.

Gulf countries are major exporters of nitrogen fertiliserslike urea -- which provides plants with nitrogen to aid green leafy growth -- as well as ammonia and phosphate.

Italy notably called last week for a "humanitarian corridor" in the Strait of Hormuz for fertiliser as Torero warned that if high prices continue, farmers would face a stark choice: "Farm the same with fewer inputs, plant less, or switch to less intensive fertiliser crops," which would reduce food supply well into 2027.

Lasting blow to supplies

Torero warned the bottleneck in marine traffic since the conflict began on February 28 meant even if Hormuz were to reopen immediately "infrastructure damage is not fully reversible in the short term."

According to Kpler data, around 1.9 million tonnes of fertiliser are trapped on 41 vessels, equal to 12 percent of all produce shipped out of the strait in 2024.

On March 2, the ammonia plant at the Ras Laffan refinery in Qatar was attacked. Plants have also suspended or reduced production in the UAE, Saudi Arabia, Iran, Jordan and Qatar, whose Qafco complex accounted for 14 percent of global trade in urea.

Overall, about one third of urea trade has been choked off, says the FAO.

In India and Bangladesh, nitrogen fertiliser plants have slowed down, unable to cope with the soaring cost of the gas required to operate.

Price breaks

Even if production and shipping resumes in the Gulf, prices for nitrogen fertilisers will fall slowly and unevenly, warned Torero.

"Unlike oil, the fertiliser sector does not have internationally coordinated strategic reserves, making supply disruptions more difficult to manage.

"Repair timelines are measured in months, not days."

Purchasers have also been hit by the fact that many pre-war contracts governing prices have been suspended as producers cite "force majeure," forcing reliance on higher spot market prices.

The FAO forecasts global fertiliser prices could average 15–20 percent higher in the first half 2026.

"A meaningful decline would likely take four to eight weeks after reopening, as production ramps up and shipping reschedules," says Torero. "Prices are unlikely to return to February 2026 levels before the third quarter of 2026, if at all this year."

YOU KNOW WHAT

The fertilizer sector is more vulnerable than the oil industry during conflicts because it lacks internationally coordinated strategic reserves, making it nearly impossible for nations to manage sudden, large-scale supply disruptions

Too late for some

He added many crop planting decisions have already been missed with the Northern Hemisphere already in planting seasons, meaning those yields will not be recovered.

"It's too late" in India, Bangladesh, Pakistan, Sri Lanka, Sudan, Kenya, Somalia, Turkey, and Jordan, all heavily reliant on Gulf fertilizers. But perhaps not for second harvests in Asia if fertilizers arrive within 4 to 6 weeks."

He explained that "the time between a fertiliser shock and a harvest failure is measured in months. The time between a harvest failure and a food price surge is measured in months more. We are already inside that window."

"Ripple effect"

Prices spiked following previous disruptions during the financial crisis of 2008 and the Russian invasion of Ukraine in 2022.

"I think what makes this one potentially more critical is the number of production hubs that are involved and countries that are involved," says Sarah Marlow, global editor for fertiliser at Argus Media.

"And then the ripple effect has spread out from the Gulf to other countries, which have also been affected by a lack of raw materials, a lack of gas."

OpenAI CEO's California home hit by Molotov cocktail, man arrested

OpenAI CEO Sam Altman

AFP | San Francisco

The luxury San Francisco home of OpenAI boss Sam Altman was hit by a Molotov cocktail on Friday, the company said, as police announced the arrest of a suspect.

No one was injured in the incident, and the firm behind the popular ChatGPT artificial intelligence chatbot would not confirm if the CEO was home at the time.

The motive for the attack and subsequent threats to set fire to OpenAI's San Francisco headquarters -- apparently by the same 20-year-old man -- were not immediately known.

But they come as Altman's profile has risen with the increasing use of AI, amid fears it could massively disrupt employment patterns and cause irreversible societal changes.

Police in San Francisco responded after reports that someone had tried to set fire to a gate at the sprawling home.

A statement from the San Francisco Police Department said officers were dispatched to the home just after 4:00 am (1100 GMT).

"At the scene, officers learned that an unknown male subject threw an incendiary destructive device at a home, causing a fire to an exterior gate. The suspect then fled on foot," SFPD said.

A short time later they were called to the firm's offices where a man was making threats.

"When officers arrived on scene, they recognized the male to be the same suspect from the earlier incident and immediately detained him," the statement said of the unnamed 20-year-old suspect.

A spokesman for OpenAI confirmed the attack on the chief executive's residence and the threats to the San Francisco headquarters.

"The individual is in custody, and we're assisting law enforcement with their investigation," the spokesman said.

Altman and OpenAI have become targets for people protesting AI as a threat to society.

Detractors have been particularly troubled by OpenAI's decision to provide its technology to the US Department of Defense.

In a rare post on his personal blog, Altman shared a photo of his husband and their baby "in the hopes that it might dissuade the next person from throwing a Molotov cocktail at our house."

Mythos AI alarm bells: Fair warning or marketing hype?

Powerful coding AI sparks fears of hacker misuse while experts debate real risks

- **Anthropic delays Claude Mythos release**
- **Experts warn of cyber risks**
- **Critics question fear-driven marketing**

AFP | San Francisco

8

major companies were included in the restricted preview of Claude Mythos under Project Glasswing

Anthropic postponing the release of its new AI model Claude Mythos, said to be so skilled at coding it could be a wicked weapon for hackers, has encountered a mix of alarm and skepticism.

The company is among several contenders in a fierce artificial intelligence race. Promoting the awe of Anthropic's own technology boosts business and enhances its allure in the event it soon goes public, as is rumored.

"The world has no choice but to take the cyber threat associated with Mythos seriously," said David Sacks, an entrepreneur and investor who heads President Donald Trump's council of advisors on technology.

"But it's hard to ignore that Anthropic has a history of scare tactics."

Mythos has sparked fears of hackers commanding armies of AI agents able to break through computer defenses with ease.

At this week's HumanX AI conference in San Francisco, Alex Stamos of startup Corridor, which addresses AI safety, acknowledged a real threat from agentic hackers.

And Stamos quipped about what he referred to as Anthropic's "marketing schtick."

"They have these adorable cutesy cartoons about these products that are so incredibly dangerous that they won't even let people use them," Stamos said of the San Francisco-based startup.

"It's like if the Manhattan Project announced the nuclear bomb within a cute little Calvin and Hobbes cartoon."

The heads of America's biggest banks met this week with Federal Reserve Chairman Jerome Powell and Treasury Secretary Scott Bessent to weigh the security implications of the yet-to-be released Claude Mythos, according to reports Friday.

"Mythos model points to something far more consequential than another leap in artificial intelligence," Cato Networks co-founder and chief executive Shlomo Kramer said in a blog post.

"It signals a shift that could redefine the balance between attackers and defenders in cyberspace."

A tightly restricted preview of Mythos was shared with partner organizations this week, under an initiative called Project Glasswing. They include Amazon, Apple, Microsoft, Google, Cisco, CrowdStrike and JPMorgan Chase.

According to Anthropic and partners, Mythos can autonomously scan vast amounts of code to find and chain together previously unknown security vulnerabilities in all kinds of software, from operating systems to web browsers.

Crucially, they warn, this can be done at a speed and scale no human could match, meaning it could be used to bring down banks, hospitals or national infrastructure within hours.

"What once required elite specialists can now be per

formed by software agents," Shlomo said.

"The immediate consequences will be a surge in vulnerability discovery, a true tsunami" of exploiting known and unknown vulnerabilities.

'Agent-to Agent War'

At HumanX, the apparent consensus was that it makes sense that AI agents already adept at coding will excel at finding weaknesses in software.

"We're not in an era where human beings can write code when we have superhuman (AI models) that are then going to find bugs in it," Stamos contended.

"It's just not possible."

He predicted the coming dynamic will involve humans supervising AI agents to protect networks against hackers using that same technology to attack.

Stamos referred to it as "agent-to-agent war," with humans on the sidelines giving advice.

Wendy Whitmore, of cybersecurity firm Palo Alto Networks, expects "some sort of catastrophic attack" this year connected to AI agent capabilities.

"The thing that keeps me up at night is that we're staring down the barrel of a massive influx of new vulnerabilities that are going to be found by AI," said Adam Meyers of CrowdStrike.

Meyers saw embedding a tiny AI model directly into malicious code infecting networks as a natural tactic to be explored by hackers.

"The ultimate weapon would be malware that has no pre-programming," Meyers said.

"It can do whatever you ask it to."