Nasa Mars rover: Perseverance robot launches to detect life on Red Planet

NEW YORK: The US space agency's Perseverance robot has left Earth on a mission to try to detect life on Mars. The one-tonne, six-wheeled rover was launched out of Florida by an Atlas rocket on a path to intercept the Red Planet in February next year.

When it lands, the Nasa robot will also gather rock and soil samples to be sent home later this decade.

Perseverance is the third mission despatched to Mars inside 11 days, after launches by the UAE and China.

Lift-off from Cape Canaveral Air Force Station occurred at 07:50 local time (12:50 BST; 11:50 GMT).

Nasa made this mission one of its absolute priorities when the coronavirus crisis struck, establishing special work practices to ensure Perseverance met its launch deadline. "I'm not going to lie, it's a challenge, it's very stressful, but look - the teams made it happen and I'll tell you, we could not be more proud of what this integrated team was able to pull off here, so it's very, very exciting," Administrator Jim Bridenstine told reporters.

Perseverance is being targeted at a more-than 40km-wide, near-equatorial bowl called Jezero Crater. Satellite images suggest this held a lake billions of years ago.

Scientists say the rocks that formed in this environment stand a good chance of retaining evidence of past microbial activity - if ever that existed on the planet.

Perseverance will spend at least one Martian year (equivalent to roughly two Earth years) investigating the possibility. Unlike the previous four rovers Nasa has sent to Mars, its new machine is equipped to directly detect life - either current or in fossilised form.

But any evidence it uncovers will almost certainly have its sceptics, which is why researchers want to bring whatever Perseverance finds back home for the deeper analysis only sophisticated laboratories on Earth can perform. The rover will therefore package its most interesting rock discoveries in small tubes. An elaborate mix of future missions will then launch later this decade to try to retrieve these samples. How is Perseverance different from earlier rovers? At first glance, Perseverance looks to be a copy of the Curiosity robot Nasa sent to Mars' Gale Crater in 2012. Indeed, the new robot even incorporates some leftover parts from the earlier mission.

But the seven instruments on Perseverance are either major upgrades or totally new. Expect some remarkable new imagery from the 23 cameras on the vehicle - and sound, because the Perseverance mission carries microphones as well. "We hope to capture some of the sounds of entry, descent and landing; and some of the sounds of driving around, merging that with the video we can take," explained Jim Bell, the principal investigator on the rover's mast-mounted camera system, MastcamZ. In addition to geological investigations and the search for life, there's an emphasis on future human exploration. **—Reuters**

Extinction: Quarter of UK mammals 'under threat'

BERLIN: A quarter of native mammals now at risk of extinction in the UK. This is according to the first Red List of UK mammals - a comprehensive review of the status of species, including wildcats, red squirrels and hedgehogs. The report's authors are calling for urgent action to prevent their loss. Prof Fiona Mathews from the Mammal Society told BBC News: "What this is clearly saying is that we have to act now - we can't continue on this same trajectory." What is the Red List? It is the official list categorising species based on their conservation status - or how threatened they are. Compiled after a review of all the available evidence on mammal populations, threats to their survival and to their habitats, the list has to meet the internationally-agreed criteria for assessing the conservation status of different species.

"When we draw all the evidence together - about population size and how isolated and fragmented those populations are - we come up with this list of 11 of our 47 native species being threatened imminently," explained Prof Mathews. "And there are more species that are categorised as 'near threatened'. "That means that we need to keep an eye on these species, because while we don't yet have a red flag waving, they're still abundant enough to be able to turn things around." The Scottish wildcat and the greater mouse-eared bat are both listed in the most severely threatened category of Critically Endangered. And much more familiar animals - the red squirrel and the water vole - have been put in the second most urgent category of Endangered.

The mammals in the most threatened categories are as follows: Different animals face different threats. The now Critically Endangered Scottish wildcat population has not recovered from decades of persecution and, for the red squirrel, disease and competition from introduced grey squirrels has driven a steep decline. But something most conservation scientists agree on is that we we need to leave more wild space across the landscape for these species to recover. Dr Kat Fingland, from Nottingham Trent University, explained that while there were pockets of good habitat, it was vital to link that together and give mammals the space to move. "We need to do a lot more urban greening," she said. "And to make space for nature and build around it, rather than trying to move animals out of the way when we want to build." Dr Fingland added that access to nature have proven to be particularly important for people's physical and mental health during lockdown.

The People's Trust for Endangered Species has also warned though that existing conservation projects may be forgotten during the pandemic. "Decades of work could be undone," the charity warned, through neglect and "unintended consequences".

The new Red List, researchers hope, provides a guide for how to prioritise the most urgent conservation funding.

Prof Mathews added: "While we bemoan the demise of wildlife in other parts of the world, here in Britain we are managing to send even rodents towards extinction. "Things have to change rapidly if we want our children and grandchildren to enjoy the wildlife we take for granted." **—Reuters**

Australia unveils plan to force Google and Facebook to pay for news

SYDNEY: The Australian government has unveiled its plan to force tech giants such as Google and Facebook to pay news outlets for their content.

Treasurer Josh Frydenberg said the "world-leading" draft code of conduct aimed to give publishers "a level playing field to ensure a fair go".

Many news outlets have shut or shed jobs this year amid falling profits. Facebook and Google strongly oppose the proposal, even suggesting they could walk away from Australia's news market.

Mr Frydenberg said the code of conduct - drafted by Australia's competition regulator - would be debated by parliament. It could impose "substantial penalties" worth hundreds of millions of dollars on tech companies which fail to comply, he said.

What's in the draft code? The Australian Competition and Consumer Commission draft calls on tech companies to pay for content, though it does define what it is worth. It would allow news companies to negotiate as a bloc with tech giants for content which appears in their news feeds and search results.

If negotiations fail, the matter could be arbitrated by the Australian Communications and Media Authority. The draft code covers other matters too, including notifying news companies of changes to algorithms. Penalties could be up to A$10m (£5m; $7m) per breach, or 10% of the company's local turnover. The code will initially focus on Google and Facebook but could be expanded to other tech companies, the treasurer said.

What are the arguments? Mr Frydenberg said: "Nothing less than the future of the Australian media landscape is at stake with these changes."

"Today's draft legislation will draw the attention of many regulatory agencies and many governments around the world," he said.

Australia's biggest media companies have lobbied hard for the proposal. It was a "watershed moment" in efforts to end "free-riding" by the tech companies, News Corp Australia executive chairman Michael Miller said on Friday. Google's local managing director, Mel Silva, said the company was "deeply disappointed" and argued the move would discourage innovation. "The government's heavy-handed intervention threatens to impede Australia's digital economy and impacts the services we can deliver to Australians," she said. Facebook has previously suggested it could remove Australian news from its platform if such requirements were imposed - arguing the cost to its business would be negligible. The code of conduct will be subject to a month-long consultation period before being debated in parliament "shortly after" August, Mr Frydenberg said.

If legislation is passed, the code is designed to be reviewed after a year. **—Reuters**

Climate change 'driving UK's extreme weather'

LONDON: Climate change driven by industrial society is having an increasing impact on the UK's weather, the Met Office says.

Its annual UK report confirms that 2019 was the 12th warmest year in a series from 1884.

Although it does not make the top 10, the report says 2019 was remarkable for high temperature records in the UK. There was also a severe swing in weather from the soaking winter to the sunny spring.

The temperature extremes were: A new UK maximum record (38.7° C) on 25 July, in Cambridge.

A new winter maximum record (21.2° C) on 26 February, in Kew Gardens, London - the first time 20C has been reached in the UK in winter A new December maximum record (18.7° C) on 28 December, in Achfary, Sutherland A new February minimum record (13.9° C) on 23 February, in Achnagart, Highland No national low temperature records were set in the State of the UK Climate report, published by the Royal Meteorological Society. Media captionWhat's the difference between weather and climate?

It shows that UK temperatures in 2019 were 1.1° C above the 1961-1990 long-term average. Mike Kendon, lead author of the report, said: "Our report shows climate change is exerting an increasing impact on the UK. "This year was warmer than any other year in the UK between 1884 and 1990, and to find a year in the coldest 10 we have to go back to 1963." The Central England Temperature series is the longest instrumental record of temperature in the world, stretching back to 1659.

UK warned over coronavirus climate trap. A really simple guide to climate change. Climate change: Where we are in seven charts Dr Mark McCarthy, from the Met Office, added it was a particularly wet year across parts of central and northern England.

He said Lincolnshire, Nottinghamshire, Derbyshire, Leicestershire and Cheshire received between a quarter to one third more rainfall than normal. For northern England this was the ninth wettest year in a series from 1862. He said: "It's worth noting that since 2009 the UK has now had its wettest February, April, June, November and December on record – five out of 12 months."

Hannah Cloke, professor of hydrology at the University of Reading, identified a number of concerning trends. She said: "As well as extreme hot temperatures, the stand-out weather events in 2019 were the many different types of floods, causing millions of pounds worth of damage and causing misery to many people. "The picture that emerges is of the multiple flooding threats that are facing the UK, many of which are exacerbated by climate change."

She cited as examples summer flash floods caused by extreme downpours, extensive autumn and winter river floods caused by persistent heavy rain and storms, and a backdrop of continued sea-level rises heightening the risk of coastal floods. Professor Ilan Kelman, from University College London, said heat would become an increasing problem. He said: "These UK records show that if we do nothing about stopping climate change we are on track for summer

Staff tricked by phone spear-phishing scam

CALIFORNIA: The unprecedented hacking of celebrity Twitter accounts this month was caused by human error and a spear-phishing attack on Twitter employees, the company has confirmed.

Spear-phishing is a targeted attack designed to trick people into handing out information such as passwords. Twitter said its staff were targeted through their phones.

The successful attempt let attackers tweet from celebrity accounts and access their private direct messages. The accounts of Microsoft founder Bill Gates, Democratic presidential hopeful Joe Biden and reality star Kim Kardashian West were compromised, and shared a Bitcoin scam. It reportedly netted the scammers more than $100,000 (£80,000). The attack has raised concerns about the level of access that Twitter employees, and subsequently the hackers, have to user accounts. By obtaining employee credentials, they were able to target specific employees who had access to our account support tools. They then targeted 130 Twitter accounts - Tweeting from 45, accessing the DM inbox of 36, and downloading the Twitter Data of 7.

Twitter acknowledged that concern in its statement, saying that it was "taking a hard look" at how it could improve its permissions and processes.

"Access to these tools is strictly limited and is only granted for valid business reasons," the company said.

Not all the employees targeted in the spear-phishing attack had access to the in-house tools, Twitter said - but they did have access to the internal network and other systems. Once the attackers had acquired user credentials to let them inside Twitter's network, the next stage of their attack was much easier. They targeted other employees who had access to account controls.

Twitter isn't clarifying whether or not their employees

were duped by an email or a phone call.

The consensus in the information security community is that it was the latter. Phonecall spear-phishing, commonly known as vishing, is bread and butter for the sort of hackers who are suspected of this attack.

The criminals obtained the phone numbers of a handful of Twitter staff and, by using friendly persuasion and trickery, got them to hand over usernames and passwords that gave them an initial foothold into the internal system. As Twitter puts it, the scammers "exploited human vulnerabilities". You can imagine how it possibly went: Hacker to Twitter employee: "Hi, I'm new to the department and I've locked myself out of the Twitter internal portal, can you do me a huge favour and give me the login again?" The fact that Twitter staff were susceptible to these basic attacks is embarrassing for a company built on being at the forefront of digital technology and internet culture.

Twitter said the initial spear-phishing attempt happened on 15 July - the same day the accounts were compromised, suggesting the accounts were accessed within hours. "This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems," the company said. "This was a striking reminder of how important each person on our team is in protecting our service." Media captionTechnology explained: What is phishing? Twitter did not state whether the attack involved voice calls, despite a previous report from Bloomberg stating that at least one Twitter employee was contacted by attackers through a phone call.

Phishing is most commonly done by email and text message, encouraging recipients to click on links that take them to websites with fake log-in screens.

Spear-phishing is a version of the scam targeted at one person or a specific company, and is usually heavily customised to make it more believable.

One victim whose account was compromised told the BBC there were several things Twitter could have done differently. "They shouldn't give the ability to a single employee to remove both email address on file and two-factor authentication," they said.

"I understand why there's a need for this - for example if a dormant account has a very old email that's inaccessible and you've lost your phone or something- but it should require two employees to sign off." They also said communication from Twitter was poor. "It took 10 days to reset this account with no actual personal response from Twitter. I literally got a 'click here to continue' automated email from their system when they added my email back to the account to allow me to reset it - and it looked like a phishing email." **—Reuters**