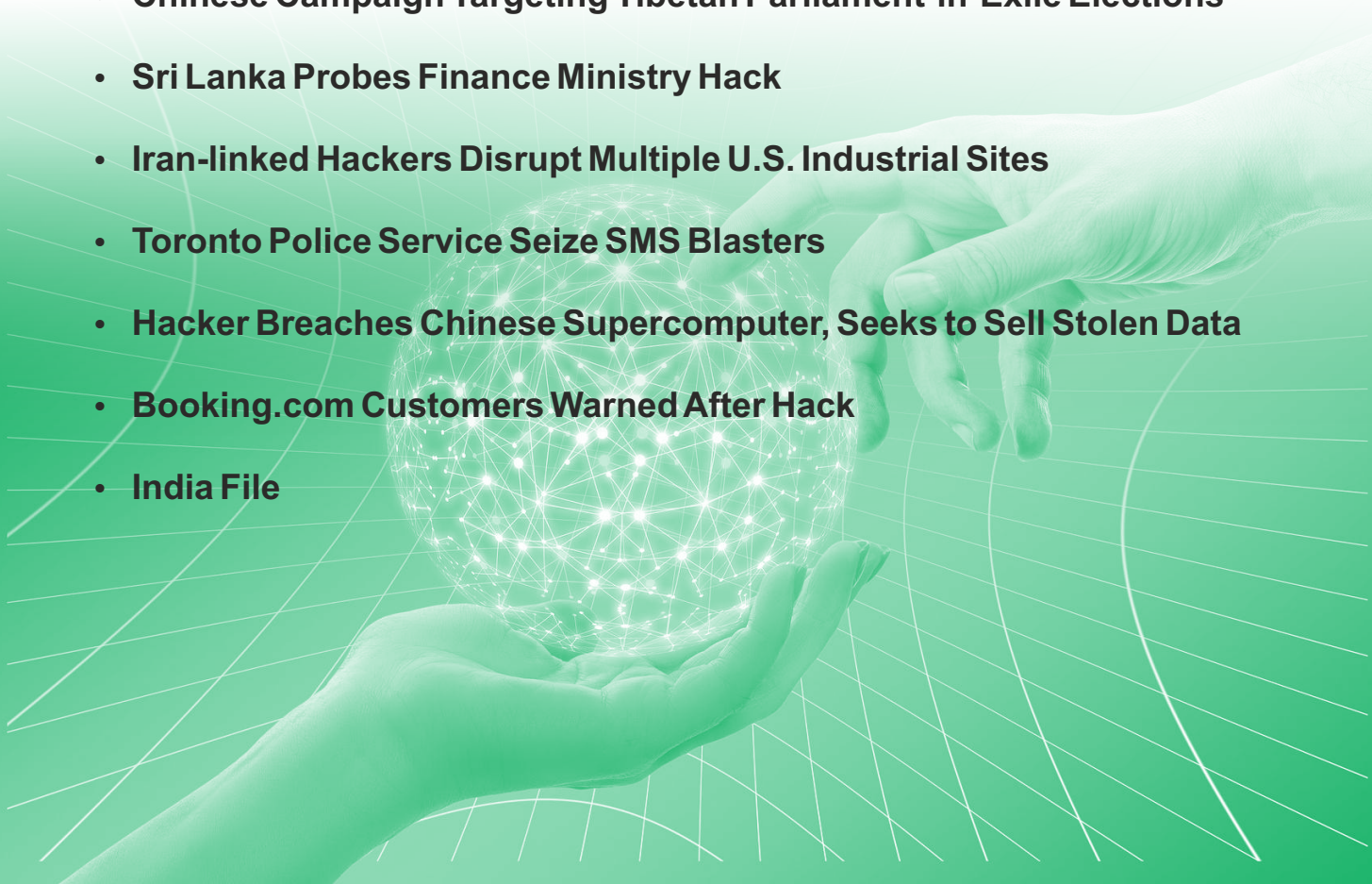
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

May 2026

- AI Pushes Cybersecurity Frontiers with Anthropic's New Mythos Model
- Ukraine Busts Bot Farm Supplying Fake Accounts
- Chinese Campaign Targeting Tibetan Parliament-in-Exile Elections
- Sri Lanka Probes Finance Ministry Hack
- Iran-linked Hackers Disrupt Multiple U.S. Industrial Sites
- Toronto Police Service Seize SMS Blasters
- Hacker Breaches Chinese Supercomputer, Seeks to Sell Stolen Data
- Booking.com Customers Warned After Hack
- India File



AI Pushes Cybersecurity Frontiers with Anthropic's New Mythos Model

Anthropic announced that its new model, Claude Mythos, can surpass human performance in certain hacking and cybersecurity tasks, raising concerns among regulators, lawmakers, and financial institutions about potential risks to digital systems.[1] To address these concerns, several major tech firms have been granted access to Mythos under an initiative called Project Glasswing, aimed at enhancing defenses against threats posed by the model itself.

Anthropic's announcement of its frontier model, Mythos, has also been accompanied by mounting concerns.[2] One key fear is that, despite not being publicly released, the model could still fall into the wrong hands. That concern appears to have materialised, when there were reports that a small number of users on a private online forum were able to gain access to the system.[3]

India's Finance Minister, Nirmala Sitharaman convened a high-level meeting with bank chiefs to evaluate emerging cybersecurity risks associated with advanced AI models, amid growing global concern over Anthropic's Claude Mythos and its potential impact on financial data security.[4] Japan has also announced plans to establish a task force to tackle cybersecurity risks in its financial system, following concerns over potential vulnerabilities associated with Mythos AI model.[5]

Ukraine Busts Bot Farm Supplying Fake Accounts

Ukrainian authorities have dismantled a so-called "bot farm" that was supplying thousands of fake social media accounts to Russian intelligence services for use in disinformation campaigns targeting Ukraine.[6] Security Service of Ukraine and the National Police confirmed the detention of the alleged organiser and the blocking of nearly 20,000 fraudulent online profiles believed to have been used in Russian-directed information operations. According to investigators, the suspect sold over 3,000 fake Telegram accounts each month to Russian clients. These accounts were created using Ukrainian mobile phone numbers and then advertised on specialised online platforms frequented by pro-Russian actors

Chinese Campaign Targeting Tibetan Parliament-in-Exile Elections

A China-linked influence operation involving Facebook accounts and Instagram profiles was reported to have targeted the April 26 elections for the Tibetan Parliament-in-Exile.[7] The campaign appears to be part of a broader network that also circulates narratives related to countries such as the Philippines, the United States, Taiwan, and Japan.

The operation has been linked to "Spamouflage," a previously identified China-associated influence network known for using AI to enhance election interference efforts. Coordinated accounts on platforms like Tumblr and X have been used to target specific candidates, while the Facebook-based network has promoted overlapping narratives.

Among the most prominent themes are personal attacks against re-elected leader, being portrayed as corrupt and power-hungry. Other narratives question the

integrity of the electoral process by highlighting internal controversies, or depict the exile government as being dominated by monks and the Dalai Lama. Overall, the campaign appears aimed at deepening divisions within the Tibetan exile community.

Sri Lanka Probes Finance Ministry Hack

Sri Lanka has launched an investigation after hackers breached its Finance Ministry's computer systems and stole $2.5 million, officials have confirmed.[8] The funds were part of a bilateral debt repayment to Australia, with the settlement originally due in September 2025. Authorities believe the diversion occurred sometime in January, although details have only recently come to light. While the exact method remains unclear, investigators suspect that the attackers manipulated email-based payment instructions within the sovereign debt repayment process. The breach was detected only after the Australian creditor reported that the payment had not been received, prompting Sri Lankan officials to identify the missing $2.5 million.

Iran-linked Hackers Disrupt Multiple U.S. Industrial Sites

Iran-linked hackers have targeted and disrupted multiple oil, gas, and water facilities in the United States, according to a federal advisory.[9] The campaign represents an escalation in cyber operations attributed to Tehran, particularly in the context of the ongoing US-Israel-Iran conflict. Notably, the attacks probed safety systems at industrial facilities, critical mechanisms designed to protect human life, raising serious concerns about potential physical consequences. The intrusions forced some affected sites to shut down automated processes and switch to manual operations, resulting in operational disruptions and financial losses. In certain cases, the attackers attempted to deploy destructive malware, or wipers, aimed at erasing data from victim systems, although it remains unclear whether these efforts were successful.

Toronto Police Service Seize SMS Blasters

Toronto Police Service have arrested three individuals and seized several SMS blasters, which is an advanced cybercrime tool not previously encountered in Canada.[10] SMS (Short Message Service) blasters operate by mimicking legitimate cellular towers. When nearby mobile devices connect to them, users receive fraudulent text messages that appear to originate from trusted organisations. These messages typically contain links directing recipients to fake websites designed to steal personal information, a technique known as smishing (SMS phishing). Authorities noted that this is the first recorded use of such technology in Canada, underscoring a growing threat to both public safety and financial security.

Hacker Breaches Chinese Supercomputer, Seeks to Sell Stolen Data

A hacker has allegedly exfiltrated a vast cache of sensitive data including highly classified defence documents and missile schematics from a state-run Chinese supercomputer, in what could amount to one of the largest known data breaches in China.[11] The dataset, reportedly exceeding 10 petabytes, is believed to have been taken

from the National Supercomputing Center in Tianjin, a major computing hub that supports more than 6,000 clients, including scientific institutions and defence-related agencies. Cybersecurity experts who interacted with the alleged attacker and examined samples of the leaked data suggest that the breach may have occurred with relative ease. The attacker is believed to have maintained access over several months, enabling the extraction of large volumes of data without detection.

Booking.com Customers Warned After Hack

Booking.com has experienced a data breach in which unauthorised parties gained access to certain customer details.[12] The company reported detecting suspicious activity that allowed third parties to access some guests' booking information. However, it clarified that no financial data was compromised. Booking.com has not disclosed how many users were affected. In notifications sent to impacted customers, the company indicated that hackers may have accessed specific booking-related information linked to past reservations.

India File

- According to reports, Inter-Services Intelligence (ISI) allegedly orchestrated a covert operation targeting India by exploiting compromised Chinese-made CCTV systems.[13] By accessing cameras installed near sensitive military locations across border states and Union Territories, the agency was reportedly able to monitor troop movements and equipment logistics in real time. Investigators believe the objective was to enable more precise targeting of Indian defence installations and critical security infrastructure in the event of a future conflict between New Delhi and Islamabad.

- CERT-In hosted a three-day national conference, "CERT-In SAMVAAD 2026" that brought together participants, including policymakers, Chief Information Security Officers (CISOs), representatives from empanelled auditing organisations, regulators, and cybersecurity professionals from across the country.[14] The conference saw several key developments in the cybersecurity domain. These included the launch of AMBAK (Audit Monitoring, Benchmarking, Analysis and Kinetic Interventions) and the release of progress reports by working groups focused on emerging areas.

- Centre for Development of Advanced Computing (C-DAC), Hyderabad in collaboration with Reliance Foundation, has announced the launch of "e-SafeHER," a cybersecurity awareness training programme aimed at empowering one million women across rural India.[15] The initiative seeks to strengthen last-mile cybersecurity awareness, particularly among rural women who are increasingly using digital platforms for financial transactions, livelihoods, and access to essential services. The collaboration will focus on structured training modules and community-based interventions to enable women to participate in the digital ecosystem safely and with greater confidence.

[1] BBC, What is Claude Mythos and what risks does it pose? , 17 April 2026, https://www.bbc.com/news/articles/crk1py1jgzko

[2] The Guardian, What is Mythos AI and why could it be a threat to global cybersecurity? , 22 April 2026 , https://www.theguardian.com/technology/2026/apr/22/what-is-anthropic-mythos-ai-threat-global-cybersecurity

[3] BBC, Anthropic investigating claim of unauthorised access to Mythos AI tool , 22 April 2026 https://www.bbc.com/news/articles/cy41zejp9pko

[4] The Hindu, Nirmala Sitharaman urges bankers to brace for AI threats amid concerns over Anthropic's Mythos , 23 April 2026, https://www.thehindu.com/news/national/nirmala-sitharaman-meets-heads-of-banks-on-ai-risks-following-concerns-over-anthropics-mythos/article70897628.ece

[5] Reuters, Japan launches financial task force amid AI security fears, 24 April 2026, https://www.reuters.com/sustainability/boards-policy-regulation/japan-launches-financial-task-force-amid-ai-security-fears-2026-04-24/

[6] The Record, Ukraine busts 'bot farm' supplying thousands of fake Telegram accounts to Russian spies, 21 April 2026, https://therecord.media/ukraine-sbu-busts-bot-farm-supplying-russian-spies

[7] DFR Lab, "China-linked Spamouflage targets Tibetan parliament-in-exile elections", 24 April 2026, https://dfrlab.org/2026/04/24/china-linked-spamouflage-targets-tibetan-parliament-in-exile-elections/

[8] BBC, Sri Lanka investigates after hackers steal $2.5m, 23 April 2026, https://www.bbc.com/news/articles/cn53vlvn3lvo

[9] CNN, Iran-linked hackers have disrupted multiple US industrial sites, 8 April 2026, https://edition.cnn.com/2026/04/07/politics/iran-linked-hackers-disrupt-us-industrial-sites

[10] National Post, Toronto police seize 'SMS blasters,' a cybercrime weapon never before seen in Canada, 23 April 2026, https://nationalpost.com/news/canada/toronto-police-seize-sms-blasters-cybercrime-canada

[11] CNN, A hacker has allegedly breached one of China's supercomputers and is attempting to sell a trove of stolen data, 8 April 2026, https://edition.cnn.com/2026/04/08/china/china-supercomputer-hackers-hnk-intl

[12] The Guardian, Booking.com warns customers of hack that exposed their data, 13 April 2026, https://www.theguardian.com/technology/2026/apr/13/booking-com-customers-hack-exposed-data

[13] The Hindu, Pakistan used Chinese CCTV networks to access Indian assets for potential strikes, 12 April 2026, https://www.thehindubusinessline.com/news/national/pak-used-chinese-cctv-network-to-access-live-indian-strategic-asset-info-for-potential-israel-like-strikes/article70854019.ece

[14] PIB, CERT-In SAMVAAD 2026, 29 April 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2256581&reg=3&lang=1

[15] PIB, e-SafeHER – a Cyber Security Awareness Training Programme to enable one million Cyber Sakhis across rural India, 13 April 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2251715&reg=3&lang=2