DAILY CURRENT AFFAIRS

13th AUGUST, 2024

The Hindu Analysis- 13th August

TUESDAY August 13, 2024
DELHI CITY EDITION
18 Pages ₹12.00

www.thehindu.com

THE HINDU
INDIA'S NATIONAL NEWSPAPER SINCE 1878

https://newsth.live/fb
https://newsth.live/x
https://newsth.live/ig

Regd. DL(ND)-11/6110/2006-07-08
RNI No. UPENG/2012/49940

Vol. 14 • No. 193

DAMAGE CONTROL
Tungabhadra dam gate repair begins
STATES » PAGE 5

TEMPLE TRAGEDY
Seven dead, 16 injured in Bihar stampede
NEWS » PAGE 10
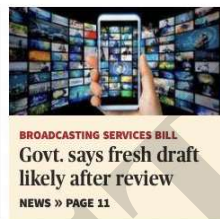
BROADCASTING SERVICES BILL
Govt. says fresh draft likely after review
NEWS » PAGE 11

RAISING VIGILANCE
Disinformation, AI and 'cyber chakravyuh'
There is a growing danger of digital threats
EDITORIAL » PAGE 6

COLLECTIONS IMPROVE
Net direct tax kitty surges by 22.5%
BUSINESS » PAGE 13

Adieu Paris

Flag bearers: Manu Bhaker and P.R. Sreejesh led the Indian contingent at the closing ceremony of the Paris Olympics on Monday. Los Angeles will host the 2028 edition of the Games. ANI (REPORT ON: PAGE 15)

SAMMAAN CAPITAL
Ab hoga desh ka sapna poora,
Sammaan Se!
Jiyo Sammaan Se
Formerly known as *Indiabulls* HOME LOANS

Statistical effects pull inflation to 59-month low

Vikas Dhoot
NEW DELHI

Inflation in India's consumer prices cooled dramatically from 5.1% in June to an almost five-year low of 3.54% in July, with food price rise moderating to a 13-month low of 5.4% from a six-month high of 9.4% a month earlier.

However, this was driven by the base effect from last July when retail inflation stood at 7.4% and the food index was up 11.5%, rather than a tangible relief for consumer wallets with overall prices rising 1.4% over June and food prices ticking up by 2.8%. The decline in headline inflation was accompanied by a rise in core inflation (excluding food and energy prices), which is estimated at 3.4%-3.5%, from 3.1% in June, economists noted.

CONTINUED ON » PAGE 10

SEBI row: BJP rejects calls for JPC probe

It alleges 'wider conspiracy' between Congress, Hindenburg Research; Opposition party threatens nationwide protest if demand is not met

The Hindu Bureau
NEW DELHI

The Bharatiya Janata Party (BJP) and the Congress on Monday continued to spar over Hindenburg Research's allegations against Securities and Exchange Board of India (SEBI) Chairperson Madhabi Puri Buch, with the ruling party rejecting the Opposition demand for a Joint Parliamentary Committee (JPC) probe.

The BJP alleged that the Congress was part of a "wider conspiracy" involving Hindenburg Research and "a tool kit" gang to destabilise the Indian economy, crash the stock market on a Monday and create economic anarchy in the country.

CONTINUED ON » PAGE 10

❝ Why is the government afraid of a JPC? Doesn't it imply that there is something to hide and be afraid of?
K.C. VENUGOPAL
Congress general secretary (organisation)

Stock markets remain calm

Lalatendu Mishra
MUMBAI

Contrary to fears of a massive fall owing to the publication of the Hindenburg Research report on Saturday, the benchmark stock indices on Monday remained nearly calm and ended range-bound.

However, Adani Group stocks lost an estimated $13.4 billion in value, as per estimates by *Reuters*.

The S&P BSE Sensex, which opened weaker, and down 375 points from Friday's close, gradually recovered lost ground during the day and closed with a minor loss of 57 points at 79,649 points, led by public sector stocks. Similarly, the NSE Nifty-50 index closed with a loss of 20.50 points at 24,347.

FULL REPORT » PAGE 13

IN BRIEF

CM gives police 7 days to crack W.B. murder case
KOLKATA
West Bengal Chief Minister Mamata Banerjee on Monday gave the police seven days to solve the case of alleged rape and murder of a doctor at the R.G. Kar Medical College and Hospital. » Page 11

20 Afghan Sikhs get citizenship under CAA
NEW DELHI
Twenty Sikhs from Afghanistan, part of the first group of Afghan Sikhs who had applied for citizenship online nearly 100 days ago, have been accorded citizenship under the Citizenship (Amendment) Act, 2019 in the past one week in New Delhi. » Page 10

MAINS ORIENTED NEWS

1. Kashmir Files
2. Disinformation, AI and 'cyber chakravyuh'

Prelims Oriented News

1. Mullaperiyar Dam
2. AUKUS

KASHMIR FILES

❖ **J&K needs a participatory democratic set-up to deal with people's needs**

Context:

❖ The article discusses the recent visit of the Election Commission of India (ECI) to Jammu and Kashmir (J&K) and the growing demand for holding Assembly elections in the Union Territory.

❖ **Background:**
   ☞ The Supreme Court has directed the ECI to conduct elections in J&K by September 30, 2024, despite the region's uncertain status since the abrogation of Article 370 in 2019.
   ☞ J&K saw its last Assembly election in 2014. And the region has been without a representative government since 2018.
   ☞ The erstwhile State of J&K was bifurcated into two UTs, and its special status scrapped in 2019.

❖ The people of J&K has shown faith in the Lok Sabha elections: Voters chose to depart from the previous trend, especially in the Kashmir Valley, of election boycotts, and instead posted a historic turnout of 58% in five Lok Sabha seats. Since 1990, J&K's voting percentage had never crossed the 50% mark.

Why Elections?

1. Holding Assembly elections in Jammu and Kashmir **would show that the central government trusts the democratic process and respects the voters' enthusiasm.**

2. Since the region lost its special status in 2019, some groups have accused the government of restricting democracy there. Allowing people to elect their representatives would be **a big step toward restoring political processes.**

3. Although there are still militant attacks, **delaying elections because of security concerns would mean giving in to the threats of terrorists.** The government should continue to fight militancy while also starting political activities.

4. Elections **can help reduce feelings of alienation** and prevent enemies of the country from taking advantage of it.

5. J&K needs a democratic government **to address problems like unemployment, electricity shortages, and poor healthcare.**

6. These elections could help heal a region that has suffered from over 30 years of conflict.

Disinformation, AI and 'cyber chakravyuh'

M.K. Narayanan

a former Director, Intelligence Bureau, a former National Security Adviser, and a former Governor of West Bengal

The year 2024 had dawned with forebodings of a new wave of security threats, and security specialists the world over, had braced for a wave of attacks along a wide spectrum. Their concerns essentially stemmed from fears arising out of new threats posed by Artificial Intelligence (AI) and its different manifestations, including Generative AI and Artificial General Intelligence (AGI). Together with the expanding horizons of disinformation and cyber threats, the outlook seemed distinctly gloomy.

The 33rd Summer Olympic Games in France, during July-August 2024, were seen as a real and tempting target for digital, including cyber and other criminals. Experts across the world were, hence, bracing themselves for digital attacks of a kind they had not encountered hitherto, quite apart from those launched by known terror groups.

Such fears were not unfounded, given the rising profile of both AI and cyber, and the consequential increase in disinformation attacks. Several months down the road, the absence of any spectacular attack has been a relief. This is no reason to relax the vigil as newer variations of digital threats are beginning to emerge. The Paris Games ended peacefully, but eternal vigilance is still the price that security agencies need to pay to ensure proper safety. Undoubtedly, an Olympic Games of this size passing off without a major incident is indeed a triumph for security managers engaged in providing security for the Games, yet vigil can hardly be relaxed.

The year so far

It might be worthwhile to look back and see what did, or did not, happen in 2024. The year started seeming to confirm the prognosis that 2024 may well be the year when the world confronts a cornucopia of security threats. Disinformation was already having a field day in the run up to the elections in Taiwan in January 2024, and the atmosphere was loaded with fake posts and videos, causing widespread confusion. This was attributed to China, but we live in a world today where nothing is what it seems. What was, however, evident was that the advent of AI seemed to have made it far easier to spread disinformation cloaked in the garb of reality. AI was the principal, though not, perhaps, the sole culprit.

It is indeed true that spreading disinformation has become far easier with the advent of AI. Deep fakes, comprising digitally manipulated video, audio, or images, repeatedly hit the headlines today, causing a miasma of disinformation. The truth is revealed much later – and after the damage has been done.

Yet, there is not enough comprehension today, about the threat posed by AI generated or other types of deep fakes. Together with cyber attacks, the world needs to realise that we face a new and grim reality which cannot be ignored any longer. National security stands imperilled by these newer threats. But even when it manifests itself, there is not enough comprehension of what is taking place. A combination of cyber attacks and AI-enabled disinformation had and is still, causing grave havoc in the conflict in Ukraine. Ukraine is a good case study of how two sides in a conflict could employ disinformation – including AI-enabled disruption – against one another, to each other's disadvantage. Together with cyber attacks, this has led to major disruptions in critical infrastructure, including telecommunications and power grids.

The CrowdStrike outage as 'preview'

The world had a preview last month of what could happen, or is in store, in the event of a massive cyberattack, whether AI-enabled or otherwise. A 'glitch' in a software update concerning Microsoft Windows caused a massive outage, which initially affected parts of the United States, but rapidly spread to different parts of the globe, including India. It disrupted flight operations, air traffic, stock exchanges and more. The Indian Computer Emergency Response Team (CERT-IN) issued a severity rating of 'critical' for the incident. This was, however, not a cyberattack, but it provided a preview of the kind of disruption that could take place in the event of a cyberattack. According to Microsoft, over eight million Windows devices failed, leading to global disruption on a massive scale.

Human memory tends to be short, and it may be necessary to remind the world about some of the better known cyberattacks in the past, which caused mayhem across the globe. The world may, or may not, remember the widespread disruption that occurred in 2017 in the wake of the WannaCry ransomware attack employing the WannaCry ransomware cryptoworm, which infected well over 2,30,000 computers in 150 countries, resulting in damage amounting to billions of dollars. The same year witnessed another cyberattack using the Shamoon Computer Virus which was directed mainly against oil companies such as SA ARAMCO (Saudi Arabia) and RasGas (Qatar), and was labelled, at the time, as the 'biggest hack in history'. Again, around the same period, a cyberattack involving the 'Petya' Malware severely affected banks, electricity grids and a host of other institutions across Europe and the United Kingdom, as also the U.S. and Australia.

Few cyberattacks have, however, had a more devastating impact than that caused by the Stuxnet 'attack' in 2010. Over 2,00,000 computers were impacted and physically degraded as a result. Stuxnet was a malicious computer worm, believed to have been in development for nearly five years, and specifically targeting supervisory control and data acquisition systems. The target in this case was the Iran nuclear programme, leading to the inference that it was state sponsored. What is now known is that Stuxnet's design and architecture is not domain specific, but could be tailored for attacking most modern systems in use.

Growing cyber threats

While the potential threat posed by AI disinformation looms large across the global landscape, for ordinary individuals, cyber is already a persisting threat. The number of victims of cyber fraud and cyber hacking has grown exponentially in recent years. Our day-to-day existence is threatened by fraudsters posing as delivery company agents and making delivery attempts, and, in the process, obtaining personal information for malicious use.
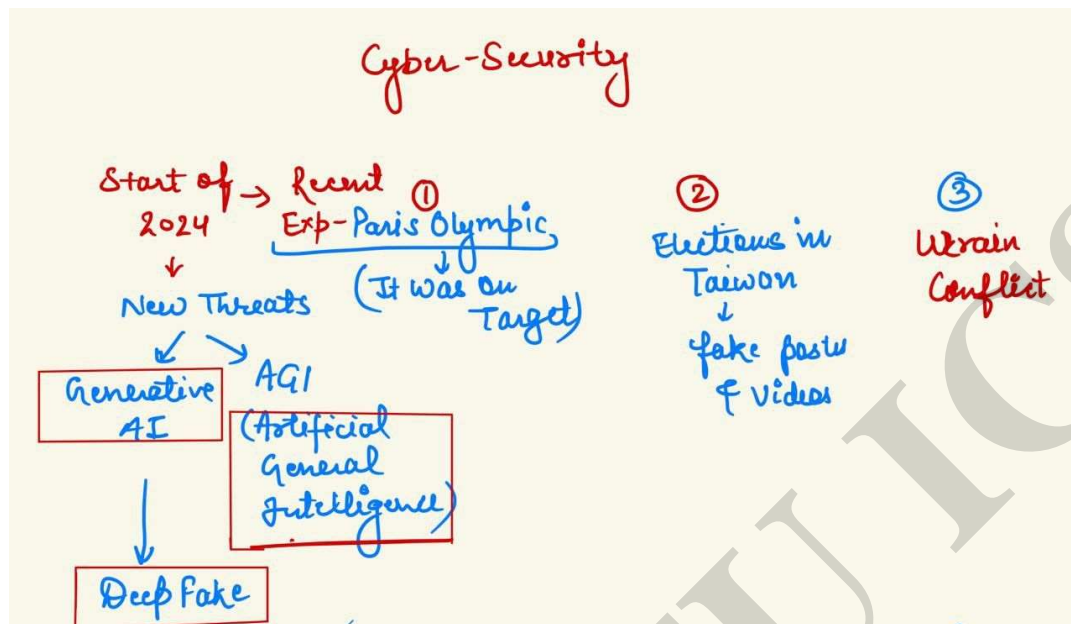
There is today a rising curve of false credit card transactions, obtaining personal information in the process to defraud unwitting individuals. Compromising business e-mails is on the increase. One of the most widespread cyber frauds is 'phishing', that involves stealing personal information such as customer ID, credit\debit card numbers, and even PIN. The list is extensive and extends to 'spamming' as well (where someone receives unsolicited commercial messages sent through one of the many electronic messaging systems). 'Identity theft' is among the most serious dangers that has now become widespread.

Across the democratic world, governments are seeking to put in place proper systems to deal with digital threats. Industry and private institutions, however, appear to be lagging behind. It is the latter segment that is, perhaps, the most vulnerable to digital attacks. Having in place firewalls, anti-virus defences and a good back-up and disaster recovery system are not enough. Most CEOs of companies, again, are not adequately equipped to deal with digital threats. Hence it might be useful to have a chief information and security officer to look at their systems and advise them as to what they should do.

Awareness of the growing danger of digital threats is but the first step in the battle against cyber and AI-directed threats. Unauthorised use of Generative AI content has already become the stock-in-trade of digital bullying. Preventing this demands a great deal of effort and adequate budgetary allocations – whether in the private or public domain.

More than anything else, potentially dangerous digital technologies require more, and the specific, attention of those in-charge, specially in the case of democracies. Awareness about digital bullying and other forms of manipulation is fundamental if we are to prevent situations getting out of hand. More than anything else, there is a need to create a realisation that the struggle against digital threats calls for coordinated action. Also, a realisation that nations, especially democracies, are today under attack from a new and different source. There is, hence, every need to counter digital surveillance, disinformation, bullying and manipulation, for our survival.
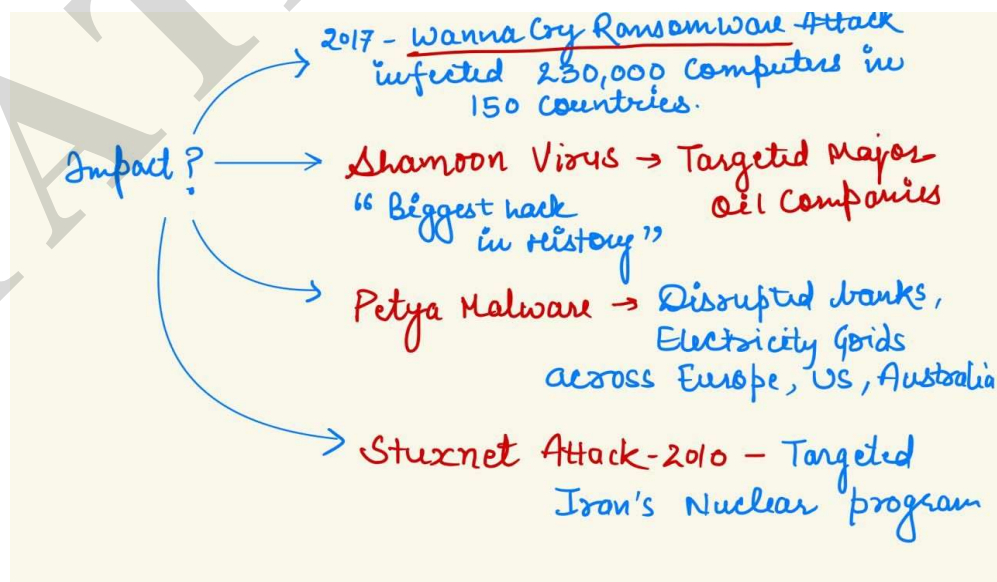
This year may well be the one when the world confronts a cornucopia of security threats

Cyber-Security

Start of → Recent ① Exp-Paris Olympic (It was on Target) ② Elections in Taiwon → fake posts & videos ③ Ukrain Conflict

New Threats → Generative AI → AGI (Artificial General Intelligence) → Deep Fake

- ❖ **Generative AI:** Generative Artificial Intelligence, is a form of artificial intelligence (AI) in which **algorithms automatically produce content in the form of text, images, audio, and video.**
- ❖ Unlike traditional AI systems that are designed to recognize patterns and make predictions, generative AI creates new content.
- ❖ **Artificial General Intelligence (AGI)** refers to a type of artificial intelligence that possesses the ability to understand, learn, and apply knowledge across a wide range of tasks at **a level comparable to human intelligence.**
- ❖ **(Human Like Features: Understanding and Reasoning, Learning and Adaptation, Self-Awareness)**

What is Deepfake (Synthetic Media)?

- ❖ Deepfakes use a form of **artificial intelligence called deep learning** to make fake images, fake videos and fake sounds.
- ❖ The term "deepfake" combines the deep learning concept with something fake.

2017 - Wanna Cry Ransomware Attack infected 230,000 Computers in 150 countries.

Impact? → Shamoon Virus → Targeted Major Oil Companies "Biggest hack in History"

Petya Malware → Disrupted banks, Electricity Grids across Europe, US, Australia

Stuxnet Attack - 2010 → Targeted Iron's Nuclear program

Growing Cyber Attacks

Phising → where personal information like
Card Numbers & PIN are stolen.
led to Identity Theft.

Spamming → where people recieve unwanted
Commercial messages.

Way Forward ? →

Recognising → Specially people,
the Private Instt" &
Threat Businesses

For digital → Effects from
Bullying Govt as well
as private
Sector

Raising → about digital
Awareness Bullying &
Fake AI.

MULLAPERIYAR DAM

❖ Kerala wants to **decommission the dam** and build a new one.

❖ Tamil Nadu seeks to complete strengthening work and **restore levels to 152 feet**. (At present- 142 feet by Supreme Court in 2014)

Minister denies any immediate threat to Mullaperiyar dam

The Hindu Bureau
IDUKKI

There was no immediate concern regarding the safety of the Mullaperiyar dam, Kerala Water Resources Minister Roshy Augustine has said.

Speaking to presspersons after a review meeting at the Idukki Collectorate on Monday, Mr. Augustine warned against unwanted public expression over the safety of the dam.

"The State government has made clear its stance to construct a new dam in Mullaperiyar. The government is in agreement with the people regarding the safety of the Mullaperiyar dam. However, there was no immediate concern over the structural safety of the dam," Mr. Augustine said.

"The District Collector will closely monitor the situation and will make arrangements, if needed, to open the shutters of the dam," he said.

Restrict vloggers
The meeting also decided to restrict vloggers who stir up fears regarding the Mullaperiyar dam safety.

Mr. Augustine said the government would direct the police to take strict action against those who spread fake news through social media.

Mr. Augustine further said that the government was hopeful of a positive judgment from the Supreme Court soon.

"The State government will also explore the possibility of resolving the Mul-

Petitioner moves SC for lowering water level

The Hindu Bureau
NEW DELHI

A petition has been filed in the Supreme Court to bring down the permissible water level of the British-era Mullaperiyar dam, situated in the Western Ghats in Kerala, from 142 feet to 120 feet to obviate the possibility of a breach.

The petition referred to the landslides in Wayanad, and said that if the dam breached, five million people would be be gravely affected.

laperiyar issue through discussions outside the court," Mr. Augustine said.

Meeting to be held
A ward-level vigilant meeting will be held in In Vandiperiyar soon. The meeting will be presided over by Peerumade MLA Vazhoor Soman. Idukki MP Dean Kuriakose, Devikulam MLA A. Raja, District Collector V. Vigneshwari, District Police Chief Vishnu Pratheep T.K., and District panchayat president K.T. Binu attended the review meeting.

The water level in the Mullaperiyar dam on Monday was 130tmcft. The maximum level fixed by the top court is 142tmcft.

AUKUS

SYDNEY

Australia, U.S. and U.K. sign nuclear transfer deal for AUKUS submarine
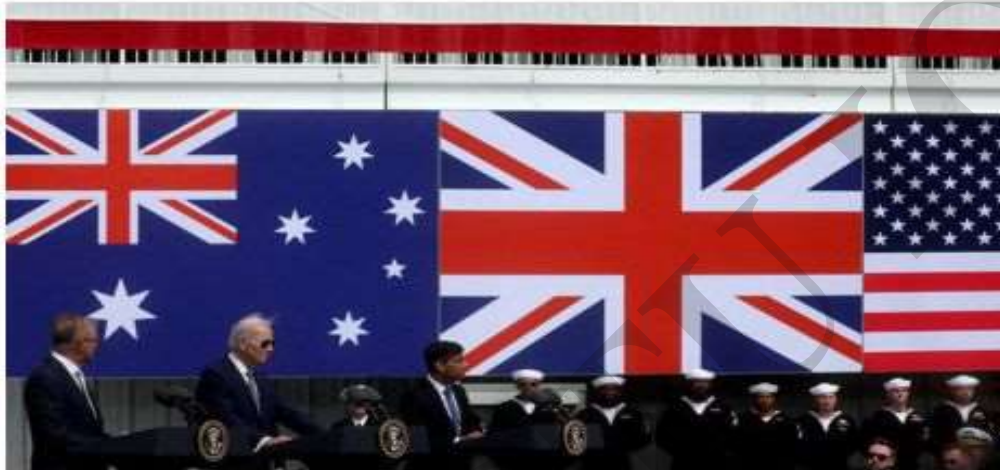
REUTERS

Australia said it had signed a deal to allow the exchange of nuclear secrets and material with the United States and Britain, a key step toward equipping its navy with nuclear-powered submarines. It will allow the transfer of sensitive U.S. and U.K. nuclear material and knowhow as part of the tripartite 2021 AUKUS accord. AFP

Context:

- ❖ Australia, U.S., U.K. sign nuclear transfer deal for AUKUS submarines
  - ☞ It aimed at building a fleet of nuclear-powered submarines for Australia and developing advanced military technology together. It is viewed as a strategic response to China's growing military power in the Pacific region.
- ❖ **AUKUS is a trilateral security partnership between Australia, the United Kingdom, and the United States intended to "promote a free and open Indo-Pacific that is secure and stable.**