Indian Express News Analysis (IENA)

English PDF Notes – 01 November 2023

UN report on groundwater extraction: Every drop counts

#GroundwaterExtraction #GroundwaterReplenishment #MihirShahCommittee #AtalBhujalYojana #Geography #GS1

A report published, last week, by United Nations University has warned that **27 of the 31 aquifers in the country are depleting faster than they can be replenished**. The alarm bells have been ringing for at least a decade. **In 2016, the Mihir Shah Committee** argued that there is little "understanding of river systems or their interconnections with the health of catchment areas or groundwater". **Several other reports, including those commissioned by the Niti Aayog and the Central Water Commission, have underlined the poor state of the country's aquifers.** Conversations in the wake of these studies pushed the **Union Jal Shakti Ministry to initiate the Atal Bhujal Yojana in 78 water-stressed districts.** The **programme, which commenced in 2020, aims to bring about behavioural changes at the community level in seven states**. It's a welcome initiative and Ministry data does show that **groundwater extraction for irrigation, domestic and industrial uses came down by about 6 billion cubic metres in 2022 from 2020**. However, the gravity of the crisis is such that much more is required from the Centre and the states.

India pumps up the most groundwater globally — more than China and the US combined. According to the Central Ground Water Board, about 70 per cent of the water used in the country is from groundwater sources. The emphasis on the use of tubewells and borewells played an important role in ensuring food security. But as the Shah Committee pointed out, there has been little emphasis on institutional innovations in the water sector. **The link between power subsidies and the falling water table in states such as Punjab has been long apparent**. Yet, addressing demand-side management remains a complex problem. The **UN report shows that 78 per cent of the wells in the state are overexploited.**

In recent years, **researchers have joined the dots between groundwater extraction and the climate crisis. The problem could become acute in the country's southwest, where aquifers of hard rock already impose limits on recharging**. Hotter temperatures could leave less moisture to soak in the soil and replenish groundwater sources. In recent years, the Centre has been trying to promote less thirsty crops like millets and the use of efficient watering techniques. But because borewells and tubewells are covered structures, people don't realise the gravity of the crisis till it's too late. The **use of technologies that allow people to monitor the water available in their borewells could be the first step to nudge them to manage aquifers responsibly.** These could be the catalyst for bringing about behavioural changes.

London Summit and how to make AI responsible

#UK_AI_summit   #ArtificialIntelligenceGovernance   #ArtificialIntelligenceRegulation #ArtificialIntelligence #InternationalRelations #GS2

The London summit this week on the safe use of Artificial Intelligence could be an important first step towards the global governance of a technology that offers much promise and unprecedented danger.

Convened by the British Prime Minister Rishi Sunak on Wednesday and Thursday at **Bletchley Park outside London**, the summit will have the US Vice President Kamala Harris and several other world leaders in attendance. Many top honchos of the technology companies are expected to join them. The participation has been limited to about 100 people to facilitate serious and intensive discussion.

In convening the summit at Bletchley Park, Sunak is also reminding the world of AI's origins in Britain. **It was at Bletchley Park that early research on AI was pioneered by Alan Turing, who is widely considered as the "father of AI".** Turing and his team of mathematicians had helped crack "Enigma", a German code during World War II, giving the Allies a huge advantage in their military operations. Although the United States and China are the leading powers in AI development today, Britain has retained its place as one of the major hubs of AI development in the world.

The London AI summit comes amid steps by various governments to address the challenges of governing AI. Earlier this week, the **US President Joe Biden issued an executive order to ensure that "America leads the way in seizing the promise and managing the risks of artificial intelligence (AI)". It establishes "new standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, stands up for consumers and workers, promotes innovation and competition, advances American leadership around the world, and more."**

The **EU, meanwhile, is discussing the promulgation of what could be the world's first comprehensive framework for regulation. It will define rules to govern the development and use of AI across the European Union. It will involve the setting up of a European Board for Artificial Intelligence to audit and administer the new rules.**

Last month, China outlined a broad set of principles for international cooperation and global governance of AI.

Beijing called for an increase in the "voice of developing countries in global AI governance, and ensure equal rights, equal opportunities, and equal rules for all countries in AI development and governance." China also expressed support for UN discussions on establishing an "international institution to govern AI, and to coordinate efforts to address major issues concerning international AI development, security, and governance."

Last week also saw the **United Nations Secretary-General Antonio Gueterres establish an advisory body to examine the risks, opportunities and international governance of AI.** He believes AI "could supercharge climate action and the efforts to achieve the sustainable development goals" that the world has set for itself.

At the summit, Sunak is expected to announce **the setting up of an AI Safety Research Institute that will "carefully examine, evaluate and test new types of AI so that we understand what each new model is capable of" and the kind of risks it might present.**

While many civil society groups demand outright ban on the development of AI or impose a moratorium, the companies rushing to invest in AI would want to prevent over-regulation that will kill innovation.

One of the issues that the London summit is discussing is **the establishment of an international register of frontier AI models that will allow governments to assess the risks involved. This is unlikely to pass muster with private companies.**

That brings us to one of the core challenges of regulating AI. **In the past, frontier technology development, in nuclear and space, was led by governments. Today, AI development outside China is with large digital corporations.**

Whether it comes up with specific answers or not, the London Summit is likely to lay out some important markers for the unfolding global discourse on AI regulation. **India, which played a key role in the 20th century discussions on regulating advanced technologies, will have to find its own voice on AI governance. With one major difference — this time India is a contributor to the global development of AI.**

Southern peninsular India sees sixth driest October in 123 years, gets 60% less rainfall

#LessRainfall #DriestOctober #Monsoon #IndianMeterologicalDepartment #ClimateChange #Environment #GS3

The **India Meteorological Department (IMD)** said that **southern peninsular India this year experienced the sixth driest October in 123 years.**

This region **– comprising Kerala, Mahe, south interior Karnataka, Tamil Nadu, Karaikal, Puducherry, coastal Andhra Pradesh, Yanam and Rayalaseema – received only 74.9mm of rain in October, which was over 60 per cent below normal.**

Southern peninsular India during October sees rainfall from both the retreating southwest monsoon and the incoming northeast monsoon. But this year, the region remained dry for nearly 25 days in October, IMD officials said. Unlike the past few years, the southwest monsoon ended nearly on time after a 134-day season this year.

One of the major contributors to this poor rainfall was the timing of the northeast monsoon coinciding with other oceanic factors. **While the northeast monsoon onset date was realised on October 21, the active Bay of Bengal and cyclogenesis around the same time influenced the monsoon onset.**

"This year, the commencement of the northeast monsoon coincided with the genesis of the **cyclone Hamoon** which crossed the Bangladesh coast. As a result, most of the moisture was dragged away from southern peninsular India. So much so that it even altered the wind flow pattern. Thus, it was a weak northeast monsoon onset," explained Mrutyunjay Mohapatra, director general, IMD.

With 2023 being an El Nino year, when combined with the positive phase of the Indian Ocean Dipole (IOD), such rainfall deficits are commonly observed during October and have been previously recorded, added Mohapatra. **Notably, 2023, 2016 and 1988, among the six driest October months over the southern peninsula, were El Nino years.**

"During El Nino years and the positive IOD phase, there is less rainfall over northern Tamil Nadu and adjoining areas. Whereas, the southernmost areas of Tamil Nadu and Kerala receive good rainfall in October," he said.

Despite a slow start, the northeast monsoon has picked up during the past two days. During this active phase, widespread good rainfall is predicted over Kerala and Tamil Nadu during the week ahead, the IMD has forecast.

The rainfall forecast for November, too, for this region is promising. **The Long Period Average (LPA) of rainfall for south peninsular India during November (based on 1971 to 2020) is about 118.69 mm.**

Why a 'normal' monsoon isn't normal anymore for India

#NormalMonsoon #MonsoonPattern #RainfallPattern #ClimateChange #Environment #GS3

The **monsoon season this year ended with 94 per cent overall rainfall, making it the eighth year in succession that the seasonal rainfall has been broadly in the normal range**. This makes it seem as though monsoon rainfall in the country has been remarkably consistent in recent years.
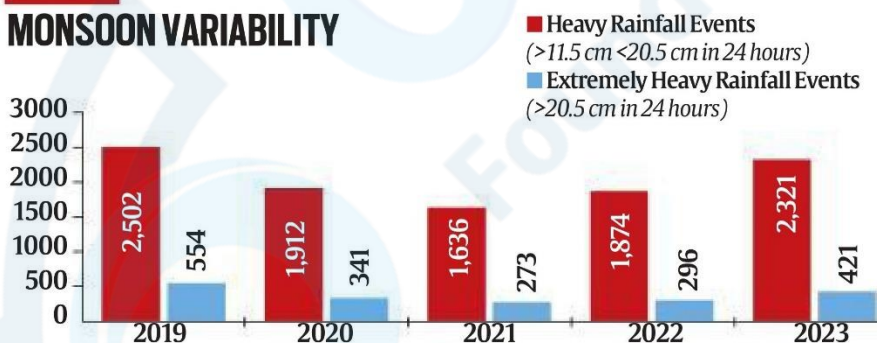
CHART-1
INDIA OVERALL RAINS
Seasonal Rainfall (June-September, in mm)

Year	Rainfall
2012	823.6
2013	937.4
2014	781.6
2015	765.8
2016	864.4
2017	845.9
2018	802.7
2019	971.7
2020	958.5
2021	874.5
2022	924.8
2023	820

But that is far from being the case, as is evident from common experience too. **There have been large variations in the distribution of rainfall, in spatial as well as temporal terms**. While some days produced very heavy rainfall, prolonged periods went extremely dry. Similarly, a majority of the districts received very little rainfall during most of the season. **This rainfall variability only seems to be increasing, possibly because of climate change.**

CHART-4
MONSOON VARIABILITY

■ Heavy Rainfall Events *(>11.5 cm <20.5 cm in 24 hours)*
■ Extremely Heavy Rainfall Events *(>20.5 cm in 24 hours)*

Year	Heavy Rainfall Events	Extremely Heavy Rainfall Events
2019	2,502	554
2020	1,912	341
2021	1,636	273
2022	1,874	296
2023	2,321	421

Rarely normal

At the district level, rainfall has been highly erratic. **During the four-month monsoon period, there have been very few instances of districts receiving normal daily rainfall**. A new analysis by Climate Trends, a research organisation, found that **districts getting normal daily rainfall was an extremely rare occurrence. Out of the nearly 85,000 district rain-days — 121 days of rainfall for each of the 718 districts — only 6 per cent were found to be normal.**

In contrast, over 60 per cent of the daily district wise rainfall showed deficits of over 60 per cent, or no rain at all on days when rains were expected. The analysis also showed that large excess days — days on which districts received 60 per cent or more than normal rainfall — were the next most frequent instances.

The **season also produced the second largest number of extreme rainfall events in the past five years**, which compensated for the deficit on the dry days and brought in an illusion of normalcy.

Dry North-East, drying Kerala

Even at the regional level, rainfall showed large variations. **Northwest and central parts of the country received more than 100 per cent rains during the season, while eastern and North-Eastern regions got barely 80 per cent. The southern part of the country also had large deficits for most of the monsoon season**. The region finally ended with 92 per cent rains for the season.

The **deficiency in east and North-East India strengthens a long-term trend of below normal rainfall in the region**. As pointed out by the Climate Trends analysis, the **region has received less than 100 per cent rains in nine out of 10 previous years. On five of those occasions, the deficiency has been larger than 10 per cent.** This region, at least the North-East, traditionally gets a lot of rain.

This year, the states of Bihar, Jharkhand and West Bengal received particularly poor rainfall, each ending with a deficiency of more than 20 per cent. Nagaland, Manipur, Mizoram and Tripura also had more than 20 per cent deficit.

Kerala is one of the rainiest states in the country, but this year it finished with the largest deficit, 34 per cent. Rainfall over Kerala has been showing a declining trend in recent years, not just during the monsoon, a phenomenon that is not very well explained. But this year's monsoon rainfall, 132.7 cm in total, was the least that the state has received in the past 12 years.

CHART-2

KERALA MONSOON RAINS

Year	Seasonal Rainfall (in mm)
2012	1547.8
2013	2561.2
2014	2164.9
2015	1515.6
2016	1352.3
2017	1856.4
2018	2516
2019	2309.8
2020	2227.6
2021	1719
2022	1736.7
2023	1327.5

Climate change

The increasingly erratic behaviour of monsoon rainfall is usually blamed on climate change, but it is not that simple. There are many other factors at play. This year's monsoon, for example, was expected to be hit by the prevailing El Nino in the eastern Pacific Ocean. In previous years, El Nino events have resulted in large rainfall deficits during monsoon. But it did not have a similar impact on the rainfall this year, at least in overall quantitative terms.

An extended cyclone on the western coast in June, and a prolonged bout of extremely heavy rainfall in the northern states in July, helped nullify the rain-suppressing impact of El Nino. August was the only month that seemed to have been under the influence of El Nino. In fact, it happened to be the driest August ever, producing just 64 per cent rainfall. But September once again brought good rainfall, despite El Nino gaining in strength.

Climate change has introduced a greater degree of uncertainty in weather events. The unpredictability in monsoon rainfall is likely to continue even if some drastic measures are

taken to immediately bring down greenhouse gas emissions, known to be the cause of global warming and climate change.

The only coping mechanism right now seems to be better preparedness to face the unpredictable events. Increased emphasis on disaster preparedness, steps to remove the bottlenecks that worsen the impacts of extreme weather events —urban flooding, for example — and strengthening of climate resilience in new and old infrastructure are some of the things that are expected to attract greater attention.

What is Apple's 'state-sponsored attackers' alert, received by multiple Opposition leaders?

#StateSponsoredAttackers #AppleNotification #LockDownMode #Pegasus #Spyware #Cybercrime #InternalSecurity #GS3

Several top opposition leaders and a few journalists have reported receiving a notification from Apple about **"state-sponsored attackers who are remotely trying to compromise" their iPhones.**

The notification says the attackers are likely targeting these individuals because of who they are or what they do, and **advises them on how to protect themselves, including activating the 'Lockdown Mode' feature on their iPhones.**

Apple has been sending out these automated notifications since late 2021, whenever it suspects some activity resembles a state-sponsored attack. It has so far notified individuals in 150 countries.

Who are these "state-sponsored attackers" that Apple refers to?

Following the allegations, Apple said in a statement on Tuesday that it **"does not attribute the threat notifications to any specific state-sponsored attacker".**

In a note issued earlier, the tech giant had said**: "State-sponsored attackers are very well-funded and sophisticated, and their attacks evolve over time. Detecting such attacks relies on threat intelligence signals that are often imperfect and incomplete. It's possible that some Apple threat notifications may be false alarms, or that some attacks are not detected."**

Attackers backed by governments go after specific individuals and their devices, based on their identity or activities. **Such attacks are very different from the ones carried out by regular cybercriminals, who usually target a large number of users for financial gain.**

According to Apple, **state-sponsored attacks are often short-lived, and are designed to evade detection and exploit vulnerabilities that may not be known to the public.**

So, what is this threat notification that Apple issues?

Apple's threat notifications are a way of alerting and helping users who may have been targeted by state-sponsored attackers.

As a response to these attacks, the company has developed a system that can spot activity that matches certain patterns. **When an attack is detected, a "Threat Notification" is sent by email and iMessage to the email addresses and phone numbers that are linked to the affected user's Apple ID.** The notification that some politicians and others received was likely triggered by this system.

In its note issued earlier, Apple had said: **"We are unable to provide information about what causes us to issue threat notifications, as that may help state-sponsored attackers adapt their behaviour to evade detection in the future."**

What does Apple advise users should do when an attack is detected?

The notifications are accompanied by advice on some extra steps that users can take to protect their devices and safeguard their privacy. **Some of the general security tips that Apple recommends are updating to the latest software versions, setting a passcode, enabling two-factor authentication, and using a strong password for the Apple ID.**

It also recommends that users should download apps only from the App Store, use a different password for each online account, and avoid clicking on links or attachments from unknown sources.

Apple also suggests that users activate the Lockdown Mode, which is a feature introduced in its latest software updates to specifically protect against rare and sophisticated cyber attacks such as these.

What exactly is the Lockdown Mode, and how can it be turned on?

When you activate Lockdown Mode, your device will enter into a state of high security, where many usual functions will be restricted or disabled. For example, you won't be able to send or receive attachments, links, or link previews in messages, to prevent attackers from accessing your personal information.

Lockdown Mode is only available on devices that run iOS 16 or later, iPadOS 16 or later, watchOS 10 or later and macOS Ventura or later. Apple says that such attacks are rare and target only specific individuals, but if you ever feel that your device or data are in danger, you can turn on Lockdown Mode by going to Settings, then Privacy & Security, then Lockdown Mode, and toggling it on.

Anyone who receives a threat notification from Apple should take it seriously and follow the steps that Apple recommends to secure their device and account.

Recalling Pegasus, the last time phones of Oppn leaders were allegedly targeted by spyware

What was the Pegasus spyware case?

In July 2021, a global collaborative investigative project reported that a **spyware called Pegasus, developed by an Israeli cybersecurity company called NSO Group, may have been used to target mobile phones of individuals in several countries, including India.**

The central government repeatedly rejected the conclusions of the global media investigation, and condemned what it claimed was the alleged undermining of national security by the opposition. However, it also refused to supply any facts in the matter — and also never explicitly denied the use of Pegasus.

On October 27, 2021, a three-judge Bench of the Supreme Court led by then Chief Justice of India (CJI) N V Ramana appointed an Expert Committee headed by Justice R V Raveendran (retd) to look into the allegations in the Pegasus spyware case, "taking into account the public importance and the alleged scope and nature of the large-scale violation of the fundamental rights of the citizens of the country".

What was this expert committee, and what was it tasked to do?

The court framed seven terms of reference for the committee, which were essentially facts that needed to be ascertained to decide the issue. These included determining **who procured Pegasus, whether the petitioners were indeed targeted by the use of the malware, and what laws justified the use of spyware such as Pegasus against Indian citizens.**

The court also asked the committee to make recommendations on a legal and policy framework on cyber security to ensure the right to privacy of citizens was protected. The committee was initially expected to submit its report in eight weeks.

Did the committee find Pegasus in the phones it examined?

On August 25, 2022, the top court recorded in its order that the expert committee found **no conclusive evidence for the use of the NSO Group's Pegasus spyware in the phones that it examined**. The **court also noted that the Centre "has not cooperated" with the panel.**

Following this, the court proceeded to examine the report and found that the committee had examined 29 phones but had not found conclusive evidence for the use of Pegasus in any of them. Malware was, indeed, found in five phones, the court noted, but this did not mean that the malware was Pegasus.

After this, the **court listed the case for further hearing after four weeks. However, no hearing has taken place since then.**

-------------------------X------------------------X------------------------X---------------------------------