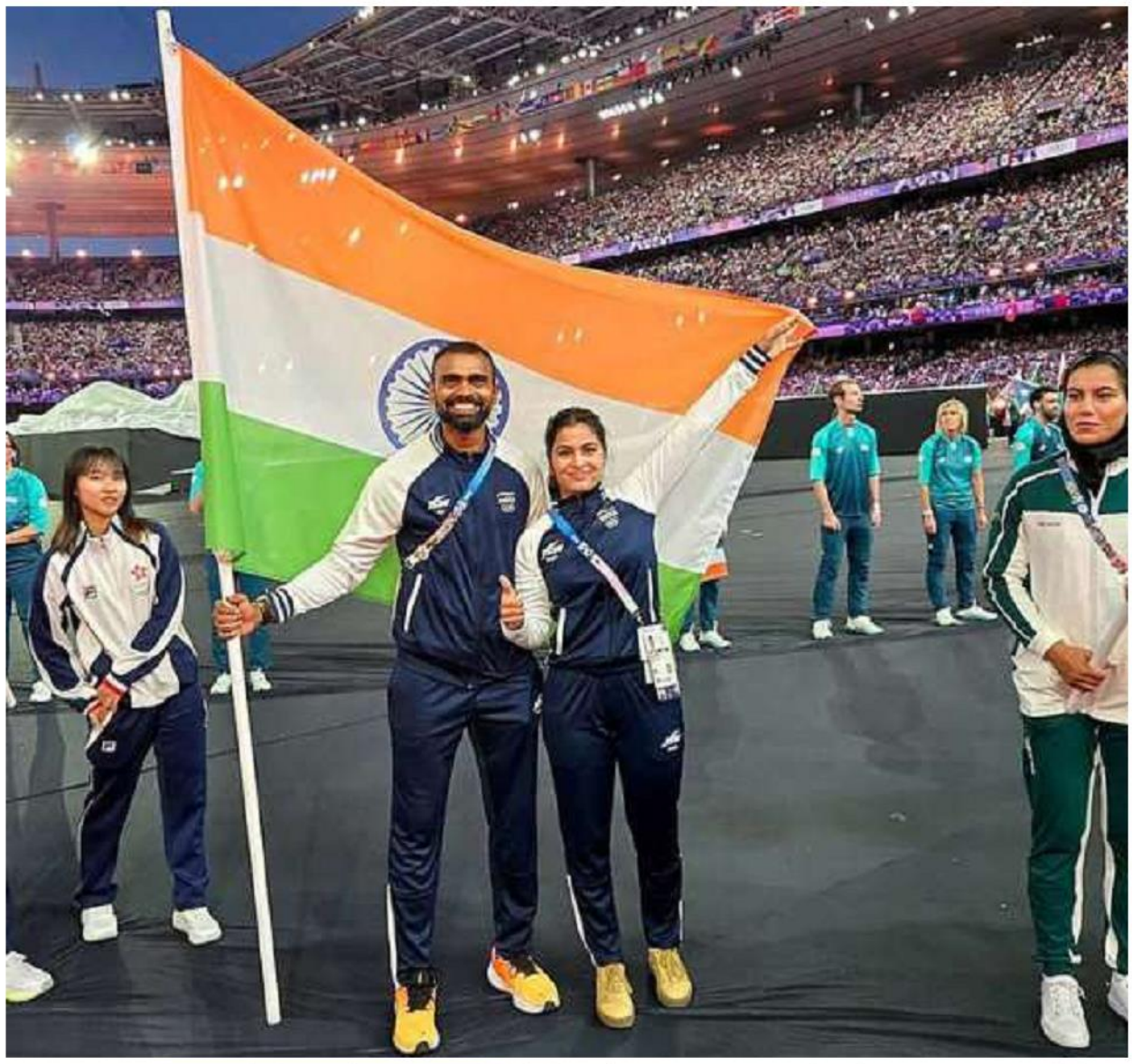
DAILY CURRENT AFFAIRS (13 August 2024)

TOPICS COVERED

1. Statistical effects pulled inflation to 59-month low of 3.54% in July
2. ‘Women can be tried for penetrative sexual assault on children’ (GS Paper-II: Vulnerable Section of Society)
3. Teachers’ federation issues appeal not to come to school drunk after one case too many
4. Tungabhadra repairs on, water diverted to canals (GS Paper-I: Geography)
5. 20 Sikhs from Afghanistan granted citizenship certificate under CAA (GS Paper-II: Citizenship)
6. Suspected case of Chandipura virus found in M.P.’s Indore (GS paper-III: Basic Science)
7. Manipur CM calls for survey to reorganise districts (GS Paper-II: Reorganization of districts)
8. AYUSH to be included in AB PM-JAY, discussions on (GS Paper-II: Health Sector)
9. Take steps to reopen Shambhu border, SC tells Punjab, Haryana
10. Most security camps in Chhattisgarh, Jharkhand set up on tribal properties (GS Paper-II: Vulnerable Section of Society)
11. NCERT finds several shortfalls in functioning of Kasturba Gandhi Balika Vidyalayas (GS Paper-II: Education)
12. Disinformation, AI and ‘cyber chakravyuh’ (GS paper-III: S&T)
13. The top court as custodian of liberties
14. J&K needs a participatory democratic set-up to deal with people’s needs (GS paper-II: Participatory Democracy)
15. States must develop capacity to conducttesting and sequencing of viruse (GS paper-III: Basic Science)
16. Possible revival of Dalit politics today (GS paper-II: Polity)
17. Socio-economic differentials within SCs/STs (GS Paper-I: Society, GS paper-II: Reservation)
18. Socio-economic differentials within SCs/STs (GS Paper-III: Capital Market)
19. The tech that helps vehicles from bumping into each other (GS Paper-III: S&T)

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 16)

IIT-Madras retains top spot in NIRF ranking for sixth consecutive year

The Hindu Bureau
NEW DELHI

The Indian Institute of Technology, Madras is the best educational institution in the country for the sixth time since 2019, shows the overall ranking based on parameters identified and defined in the National Institutional Ranking Framework (NIRF).

In the 2024 rankings, released here by Union Education Minister Dharmendra Pradhan on Monday, the IIT-Madras also retained the first position in engineering for the ninth year since 2016. The Indian Institute of Science, Bengaluru is the top institution under both the universities and research categories, retaining both positions since 2016 and 2021, respectively.

The ranks were given in 16 categories this year, three more than last year. Open universities, skill universities and State public universities are the three new categories. Mr. Pradhan said the Ministry is considering "sustainability" as a criterion, probably from next year.

While the IIM-Ahmedabad continued to be the top management institute for the fifth consecutive year since 2020, the All India Institute of Medical Sciences (AIIMS), New Delhi is the best place to study medical sciences as it retained the top spot for the seventh consecutive year.

The IIT-Bombay is the best 'innovational institution' followed by the IIT-Madras, and IIT-Delhi.

Top institutions in India

The table shows the top 10 overall institutions and Central and State universities, according to India Rankings, 2024. IIT-Madras secured the top spot in overall category

Ranks	Overall	Top universities	State universities
1	IIT-Madras	IISc, Bengaluru	Anna University
2	IISc, Bengaluru	Jawaharlal Nehru University	Jadavpur University
3	IIT-Bombay	Jamia Millia Islamia	Savitribai Phule University
4	IIT-Delhi	MAHE, Manipal	Calcutta University
5	IIT-Kanpur	Banaras Hindu University	Punjab University
6	IIT-Kharagpur	University of Delhi	Osmania University
7	AIIMS, Delhi	Amrita Vishwa Vidyapeetham	Andhra University
8	IIT-Roorkee	Aligarh Muslim University	Bharathiar University
9	IIT-Guwahati	Jadavpur University	Kerala University
10	JNU	Vellore Institute of Technology	CUSAT

Jamia Hamdard, New Delhi is the best college for pharmacy, while Saveetha Institute of Medical and Technical Sciences, Chennai is the best college to pursue dental science.

Colleges from New Delhi remained at the top in the colleges category with Hindu College and Miranda House being the top two. The IIT-Roorkee retained its first position in architecture and planning for the fourth consecutive year. The National Law School of India University, Bengaluru was named the best law school, for the seventh year in a row.

The Indian Agricultural Research Institute, New Delhi is the best institution to study agriculture and allied sectors, according to the rankings. Anna University, Chennai tops the State public universities category and Indira Gandhi National Open University (IGNOU), New Delhi is the best open university. Symbiosis Skill and Professional University, Pune emerged the best in the skill universities category.

Jawaharlal Nehru University and Jamia Millia Islamia, both in New Delhi, have secured the second and third ranks in the university category. Jadavpur University, Kolkata and Savitribai Phule Pune University, Pune are the second and third best universities under State public universities category. St. Stephen's College, New Delhi and Ramakrishna Mission Vidyamandira, Howrah shared third place in colleges category. IITs in Madras and Delhi secured second and third places in research institution subject.

Increased participation

A total of 6,517 institutions participated in the ranking under overall, category-specific or domain-specific rankings. "In all, 10,845 applications for ranking were made by these 6,517 unique institutions under various categories/domains," the Ministry said in a release, highlighting a "noticeable increase" in institutional participation in the rankings exercise.

Mr. Pradhan said the Centre is considering inclusion of institutions in the neighbouring countries in the ranking to make it more comprehensive.

NIRF Ranking (National Institutional Ranking Framework)

- The National Institutional Ranking Framework (NIRF) is an initiative launched by the Ministry of Education, Government of India, in 2015.
- Its primary aim is to rank higher education institutions in India based on various parameters, promoting healthy competition and enhancing the quality of education in the country.
- NIRF serves as a benchmark for evaluating institutions in the context of global standards.

The NIRF ranking framework assesses institutions using five main parameters:

1. **Teaching, Learning & Resources (TLR)**:
    - This parameter evaluates the quality of teaching and the resources available in institutions. It includes factors like the student-faculty ratio, faculty qualifications, and the availability of academic resources and infrastructure.
2. **Research and Professional Practices (RPP)**:
    - This focuses on the research output of institutions, including the number of publications, patents, and funded research projects. It highlights the institution's commitment to innovation and professional development.
3. **Graduation Outcomes (GO)**:
    - This measures the success rate of students from the institutions, assessing metrics such as graduation rates, employability, and the number of students pursuing higher education after graduation.
4. **Outreach and Inclusivity (OI)**:
    - This parameter evaluates the institution's efforts to promote inclusivity and outreach, analyzing aspects such as the representation of marginalized groups and the institution’s initiatives to enhance student diversity.
5. **Perception (PR)**:
    - This comprises survey-based evaluations of institutions from different stakeholders, including students, faculty, employers, and alumni. It reflects the reputation of the institution in the academic and professional fields.

‘Women can be tried for penetrative sexual assault on children’

Vulnerable section of Society

The Hindu Bureau
NEW DELHI

Criminal proceedings can be initiated against a woman for committing the offence of “penetrative sexual assault” on a child, the Delhi High Court has said noting that the offence is not restricted to only men.

The court made the observation on August 9 while hearing a plea by an accused in a case lodged under the Protection of Children from Sexual Offences (POCSO) Act. The accused had argued that since she was a woman, the offences of “penetrative sexual assault’” and “aggravated penetrative sexual assault” could not be made out against her.

The public prosecutor had contended that the POCSO Act is a gender-neutral legislation and holds perpetrators, regardless of their gender, accountable for sexual offences against minors.

Agreeing with it, the Bench of Justice Anup Jairam Bhambhani said the POCSO Act was enacted to protect children from sexual offences “regardless of whether an offence is committed upon a child by a man or a woman”.

“There is no reason why the word person appearing in Section 3 of the POCSO Act should be read as referring only to a male,” the court said.

The court held that the word “he” appearing in the POCSO Act cannot be given a restrictive meaning, to say that it refers only to a “male”. “It must be given its intended meaning, namely that it includes within its ambit any offender irrespective of their gender,” it said, adding that the petitioner can be put to trial for the offences as charged.

‘Women can be tried for penetrative sexual assault on children’ (13 August)

- **Court Ruling**:
    - The Delhi High Court ruled on August 9 that criminal proceedings can be initiated against a woman for "penetrative sexual assault" on a child.
    - The court's decision was based on the fact that the offence is not restricted to men.
- **Case Context**:
    - The ruling came during a hearing of a plea by a woman accused under the Protection of Children from Sexual Offences (POCSO) Act.
    - The accused argued that, as a woman, she could not be charged with "penetrative sexual assault" or "aggravated penetrative sexual assault."
- **POCSO Act**:
    - The public prosecutor argued that the POCSO Act is gender-neutral and holds any perpetrator, regardless of gender, accountable for sexual offences against minors.
    - The court agreed, stating the POCSO Act is designed to protect children from sexual offences committed by anyone, irrespective of their gender.
- **Court’s Interpretation**:
    - The court held that the term "person" in the POCSO Act should not be interpreted to refer only to males.
    - The term "he" in the Act should be understood to include any offender, regardless of gender.
- **Outcome**:
    - The court decided that the woman can be put on trial for the charges as filed.

Chandipura Virus

- Chandipura virus is an arbovirus that belongs to the **genus Rhabdoviridae**, primarily transmitted by sand flies. It is notable for causing neurological diseases in humans, particularly in the Indian subcontinent.
- The virus was first isolated in 1965 from the blood of a child suffering from encephalitis in the **Chandipura area of Maharashtra**, and has since been linked to multiple outbreaks in various parts of India.

Transmission:

- **Vector:** The primary vectors for the Chandipura virus are sand flies, particularly species belonging to the genus **Phlebotomus**. These flies are usually active during dusk and dawn and are found in tropical and subtropical regions.
- **Hosts:** The virus primarily circulates among **rodent and other animal hosts**, which serve as reservoirs for the virus. Humans usually become infected through bites from infected sand flies.

Clinical Features:

- Chandipura virus infection can lead to severe clinical manifestations, most notably viral encephalitis. Symptoms typically begin 4 to 14 days after exposure and include fever, headache, seizures, and signs of neurological dysfunction. Severe cases can result in coma and death.
- Children are particularly vulnerable to severe outcomes from Chandipura virus infection, and outbreaks often lead to significant morbidity and mortality in pediatric populations.

Diagnosis:

- Diagnosis of Chandipura virus infection is primarily based on clinical presentation, supported by laboratory tests. Laboratory methods include serological testing to detect antibodies, polymerase chain reaction (PCR) to identify viral RNA, and isolation of the virus in cell cultures.

AYUSH to be included in AB PM-JAY, discussions on

GS Paper II: Health Sector

The Union government is working on inclusion of an AYUSH (Ayurveda, Yoga & Naturopathy, Unani, Siddha and Homeopathy) package under the Ayushman Bharat Pradhan Mantri-Jan Arogya Yojana (AB PM-JAY).

AB PM-JAY aims to provide health cover of ₹5 lakh per family per year for secondary and tertiary care hospitalisation to approximately 55 crore beneficiaries corresponding to 12.34 crore families constituting the bottom 40% of the population.

Aspects of the AYUSH package – such as design and cost, AYUSH hospital onboarding, standard treatment guidelines, objectively defined treatment outcomes and financial implications among others – are under discussion.

Wider stakeholder consultations involving States and Union Territories have been held, said Minister of State for AYUSH Prataprao Jadhav in the Lok Sabha. He said public health is a State subject and the responsibility to ensure availability of AYUSH treatment is with the State and Union Territory governments.

Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB PM-JAY)

- The scheme covers over 50 crore beneficiaries, representing approximately 40% of India's population.
- **Financial Protection:** Offers a health cover of up to Rs. 5 lakh per family per year for secondary and tertiary care hospitalization.
- **Cashless and Paperless:** Beneficiaries can avail cashless treatment at empanelled public and private hospitals across the country.
- **Comprehensive Coverage:** Includes pre-hospitalization, post-hospitalization expenses, and covers all pre-existing diseases.
- **Portability:** Benefits can be availed at any empanelled hospital across India.

AYUSH (Ayurveda, Yoga & Naturopathy, Unani, Siddha and Homeopathy)

AYUSH is an acronym for **Ayurveda, Yoga & Naturopathy, Unani, Siddha, and Homeopathy**. It represents the diverse and ancient systems of medicine that have been practiced in India for millennia.

- These systems have a holistic approach to health, emphasizing prevention, cure, and overall well-being.

The Five Systems Under AYUSH

1. **Ayurveda:** Considered one of the world's oldest medical systems, Ayurveda focuses on balancing the body, mind, and spirit.
   - It emphasizes the use of herbs, diet, lifestyle changes, and panchakarma (detoxification) treatments.
2. **Yoga & Naturopathy:** Yoga is a physical, mental, and spiritual practice that aims to unite the body and mind.
   - Naturopathy focuses on natural healing methods, including diet, exercise, and hydrotherapy.
3. **Unani:** Originating from Greece, Unani medicine was introduced to India by Arab scholars.
   - It emphasizes the importance of **humorism (balance of bodily fluids)** and uses herbal remedies, diet, and physiotherapy.
4. **Siddha: Originating in Tamil Nadu, Siddha medicine focuses on the body's five elements (earth, water, fire, air, and ether).**
   - It uses herbs, minerals, and animal products for treatment.
5. **Homeopathy:** A German system of medicine, Homeopathy uses highly diluted substances to stimulate the body's healing response.
   - It is based on the principle of "like cures like."

NCERT finds several shortfalls in functioning of Kasturba Gandhi Balika Vidyalayas

GS Paper II: Education

Contract and outsourced employees protest in Vijayawada for minimum time scale and job security on Friday. GIRI KVS

Lack of transparency in the utilisation of funds, weak infrastructure, shortage of teachers, low salary of teachers, and concerns about safety are among the challenges identified in an evaluation of 254 Kasturba Gandhi Balika Vidyalayas (KGBV) by the National Council of Educational Research and Training (NCERT). The NCERT has submitted the report to the Education Ministry.

This is the third such evaluation carried out since 2007. The second evaluation was carried out in 2013.

Of the 5,639 approved KGBVs, 4,260 are fully functional, 799 partially functional, and 580 completely non-functional as on June 30, 2023, according to the report.

A greater percentage of non-functional KGBVs are in the States of Bihar (132), Andhra Pradesh (88), Jammu & Kashmir (84), Uttar Pradesh (78), and Odisha (76). Bihar and Andhra Pradesh, along with J&K, account for more than half of the number of non-functional schools.

"Non-completion of construction work, land issues with other departments, delays in process of selection of sites, approval of funds, delays in seeking approval of posts of teachers and other staff are some reasons for non-functionality," the report says.

Low staff retention

In all, 6,88,013 girls are enrolled from Classes 6 to 12 in 5,035 KGBVs. The study of an indicative sample of 254 KGBVs showed there is a shortage of regular and full-time teaching and administrative staff.

"Retention of staff is a major challenge due to low wages, insecurity of job, remote and isolated locations of KGBVs," the report says.

Of the 5,035 KGBVs, 2,735 are functional schools with hostels, and 2,300 are standalone hostels. Currently, there are KGBV hostels where schooling facility is not available.

Students and parents have said schooling should be provided within hostels for Classes 6 to 12. However, the report disagrees. "It is recommended that slowly and gradually there should be only KGBVs with stand-alone hostels and students must go to nearby State school for studies in inclusive environment," the report recommends.

Around 44% of the teachers said they had less than five years experience in KGBVs, indicating low retention of teachers.

Approximately one-fourth of the teachers have six to 10 years of experience in KGBVs, and another fourth have 10 to 15 years of experience.

Only 3% of teachers have more than 15 years of experience in KGBVs, suggesting that the more experienced teachers quit KGBVs to find jobs elsewhere.

Despite being residential schools, the report says almost 58% of teachers are not staying on campus and commute long distances to far-flung locations, while 38% teachers said they lived on campus.

Two-thirds of the girls (65.6%) did not respond to the question on safety and security, one-third responded that they are not safe, and less than 1% said they are safe. "8.1 per cent said that they are stressed, 10.6 per cent sad, 6.1 per cent anxious, 14.6 per cent felt mood swings, depression, 2.4 per cent and 3.7 per cent felt fearful," according to the report.

Kasturba Gandhi Balika Vidyalayas (KGBV)

- Kasturba Gandhi Balika Vidyalayas (KGBVs) aimed at promoting girls' education, in rural and disadvantaged areas.
- Established in 2004, the program seeks to provide education to girls from marginalized communities who are unable to access schooling due to socio-economic barriers.

Objectives:

1. **Enhancing Education Access**: KGBVs are designed to provide quality education to girls, especially from Scheduled Castes, Scheduled Tribes, and other underprivileged backgrounds, ensuring that they have equal opportunities for schooling.
2. **Empowering Girls**: The initiative aims to empower girls through education, enabling them to contribute positively to their communities and breaking the cycle of poverty.

Key Features:

- **Residential Schools**: KGBVs serve as residential schools for girls in the **class 6 to 12 class**, providing a secure and supportive environment for them to study.
- **Curriculum and Subjects**: The schools follow the curriculum **prescribed by the National Council of Educational Research and Training (NCERT),** with a focus on promoting overall development, including academics, life skills, and vocational training.
- **Counseling and Support Services**: Alongside education, KGBVs offer counseling and other support services to help girls navigate personal and academic challenges.
- **Community Involvement**: The program encourages community participation in school management, fostering a sense of ownership among local stakeholders.

Implementation: KGBVs are implemented under the **Sarva Shiksha Abhiyan (SSA),** which is an initiative to achieve **universal elementary education** in India. The schools are established in areas where the female literacy rate is low and infrastructure for girls' education is lacking.

Disinformation, AI and 'cyber chakravyuh'

GS Paper III: S&T

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.

> This year may well be the one when the world confronts a cornucopia of security threats

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.

Disinformation, AI and 'cyber chakravyuh' (13 August)

- In 2024, there were growing concerns about new security threats, especially related to Artificial Intelligence (AI) and its various forms like Generative AI and Artificial General Intelligence (AGI).
- Security experts were particularly worried about the potential for cyber attacks and disinformation campaigns, which seemed to be increasing in scope and impact.
- The 33rd Summer Olympic Games in France (July-August 2024) were considered a major target for digital attacks by criminals and terror groups.
- Despite these concerns, the Games concluded without any significant security incidents, much to the relief of experts.
- However, the absence of major attacks does not mean that the threat has disappeared; security agencies must remain vigilant.
- The successful security during the Games is a positive outcome, but continuous vigilance is necessary to counter emerging digital threats.

The year so far

- In 2024, the year began with expectations of various security threats, including disinformation.

- Disinformation was a significant issue before the Taiwan elections in January 2024, with fake posts and videos spreading confusion, reportedly linked to China.
- The rise of AI has made it easier to create and spread disinformation that appears real, with deep fakes (digitally manipulated videos, audio, or images) becoming more common.
- These deep fakes cause confusion, and the truth often emerges only after the damage is done.
- Despite the seriousness of these threats, there is still limited understanding of the dangers posed by AI-generated deep fakes.
- The combination of cyber attacks and AI-enabled disinformation represents a new and serious threat to national security.
- This issue is evident in the ongoing conflict in Ukraine, where these tactics have caused significant harm.
- Ukraine is an example of how both sides in a conflict can use disinformation, including AI-enabled methods, to harm each other.
- Cyber attacks in Ukraine have caused major disruptions to critical infrastructure, such as telecommunications and power grids.
- Recently, a software update glitch in Microsoft Windows caused a significant outage, affecting the U.S. and other countries like India.
- This outage disrupted flight operations, air traffic, stock exchanges, and more, showing what could happen in a large-scale cyber attack.
- Though this was not a cyberattack, it highlighted the potential for massive global disruption.
- Past cyberattacks, like the 2017 WannaCry ransomware attack, caused widespread damage, infecting over 230,000 computers in 150 countries and costing billions of dollars.
- Other notable attacks include the Shamoon virus, which targeted oil companies like Saudi Aramco and was considered the "biggest hack in history" at the time, and the Petya malware, which severely impacted banks, electricity grids, and other institutions across Europe, the U.K., U.S., and Australia.
- The Stuxnet cyberattack in 2010 had a devastating impact, affecting over 200,000 computers and causing physical damage.
- Stuxnet was a malicious worm that targeted Iran's nuclear program, leading to the belief that it was state-sponsored.
- Stuxnet's design is versatile and can be adapted to attack various modern systems, not just those specific to its original target.
- While AI disinformation is a growing global threat, cyber threats are already a significant issue for individuals.
- Cyber fraud and hacking have increased rapidly, with people being tricked into giving away personal information, often by fraudsters posing as delivery agents.
- There is a rise in false credit card transactions and email compromise, leading to financial losses.
- Phishing is a common cyber fraud where personal information like customer IDs, credit card numbers, and PINs are stolen.
- Other cyber threats include spamming (unsolicited messages) and identity theft, which is becoming more widespread and dangerous.
- Governments in democratic countries are working to address digital threats, but industries and private institutions are often lagging behind.
- Private companies are particularly vulnerable to digital attacks, and basic security measures like firewalls, anti-virus software, and backup systems are not enough.
- Many CEOs are not well-prepared to handle digital threats, so having a Chief Information and Security Officer could help them manage these risks better.
- Raising awareness about digital threats is the first step in combating cyber and AI-driven dangers.
- Unauthorised use of Generative AI content is becoming common in digital bullying, and preventing this requires significant effort and funding in both private and public sectors.
- Dangerous digital technologies need more focused attention from those in charge, especially in democracies.
- Awareness about digital bullying and manipulation is essential to prevent escalation.
- There is a need for coordinated action to combat digital threats, recognizing that democracies are under attack from new sources.
- It is crucial to counter digital surveillance, disinformation, bullying, and manipulation for the sake of survival.

2024_08_13 MAINS PRACTICE QUESTION

GS Paper III: Cyber Security

Question: Analyze the role of cybersecurity in mitigating emerging threats related to AI-generated disinformation and cyberattacks. **(250 Words/15 Marks)**

ANSWER APPROACH

- Begin by introducing the significance of cybersecurity in the context of emerging threats from AI and cyberattacks, highlighting its impact on national security and societal stability.
- Discuss specific examples of AI-generated disinformation, such as during the Taiwan elections, to illustrate the growing vulnerabilities.
- Next, outline the critical roles of cybersecurity measures, emphasizing detection systems, awareness training, collaboration, regulatory frameworks, and investment in R&D.
- Conclude by stressing the necessity for a comprehensive and coordinated approach to safeguard against these threats, referencing recent incidents that underscore the urgency of robust cybersecurity strategies.

ANSWER:

The advent of Artificial Intelligence (AI) and its various manifestations, particularly Generative AI and Artificial General Intelligence (AGI), poses significant security challenges globally. As highlighted in recent analyses, the increasing sophistication of cyberattacks and the proliferation of AI-enabled disinformation underscore the urgent need for robust cybersecurity measures to mitigate these threats. Cybersecurity is not just a technical issue; it has profound implications for national security, individual privacy, and societal stability.

Emerging Threats Posed by AI

- AI technologies make **disinformation campaigns** more effective, as they enable the creation of **deep fakes and other manipulated media** that can spread rapidly across digital platforms.
- For instance, during the Taiwan elections in January 2024, the rise of AI-assisted disinformation posed a challenge as the environment became saturated with fake posts and videos, leading to confusion and distrust.
- Such developments highlight the ease with which disinformation can be disseminated, potentially destabilizing democratic processes and social cohesion.

Role of Cybersecurity

- Cybersecurity plays a crucial role in defending against the new landscape of threats posed by AI. Effective cybersecurity frameworks can mitigate risks related to data breaches, unauthorized access to sensitive information, and infiltration of critical infrastructure.

Governments and organizations must invest in advanced cybersecurity measures that include:

1. **Robust Detection and Response Systems:** Implementing AI-driven cybersecurity solutions can enhance the detection of unusual patterns indicative of cyber threats, enabling quicker responses. Real-time monitoring systems can alert organizations to potential breaches or disinformation campaigns before they escalate.
2. **Awareness and Training Programs:** Raising awareness about the nature of AI-generated disinformation and cyber threats is vital for organizations and individuals. Training programs focused **on digital literacy** can help users identify and report suspicious activities, such as **phishing** attempts or deep fake content.
3. **Collaboration and Information Sharing**: Governments and private sectors need to establish collaborative frameworks for information sharing regarding cyber threats. Organizations such as **CERT-IN (Indian Computer Emergency Response Team)** play a critical role in providing guidance and resources for cybersecurity practices and threat mitigation.
4. **Regulatory Measures and Standards:** Governments must implement effective regulations that hold organizations accountable for cybersecurity breaches. Moreover, creating standardized practices for the use of AI in commercial applications can help in mitigating risks related to disinformation.
5. **Investing in Research and Development:** Ongoing research into new cybersecurity technologies and techniques is essential to stay ahead of evolving threats. By allocating budgetary resources to cybersecurity research, organizations can fortify their defenses against increasingly sophisticated cyberattacks.

Thus, as the threat landscape continues to evolve with the advancement of AI and technology, comprehensive cybersecurity strategies are imperative. The responsibility extends beyond technical measures to include public awareness and effective governance. The incidents such as the CrowdStrike outage and historical cyberattacks like WannaCry, remind us of our vulnerability. Therefore, a coordinated approach, involving multi-stakeholder engagement and proactive measures, is essential to safeguard national security against the dual threats of AI-generated disinformation and cyberattacks.

The top court as custodian of liberties (13 August)

- The Supreme Court of India granted bail to former Delhi Deputy Chief Minister Manish Sisodia after a long period of incarceration.
- This decision by the Court is seen as a reaffirmation of its role as the protector of individual liberties.
- The Court emphasized the importance of constitutionalism and the rule of law, stating that liberty is an intrinsic part of these principles.
- The Court cited its 2020 judgment in the Arnab Goswami case, reaffirming that liberty is a fundamental right.
- The Court reiterated the principle that "bail is the rule, and jail is the exception," originally expounded by Justice V.R. Krishna Iyer in 1977.
- The right to a fair and speedy trial is implicit in the right to life under Article 21 of the Constitution, and the Court concluded that this right was denied to Manish Sisodia.
- The Court referred to its earlier observations from October 30, 2023, highlighting the extensive documents and witnesses involved in the case, which could cause significant delays in the trial.

- The Court also relied on previous judgments that emphasized the right to a speedy trial, including cases like Kashmira Singh (1977), P. Chidambaram (2020), Satender Kumar Antil (2022), and Sheikh Javed Iqbal (2024).
- The Supreme Court ruled that the right to bail in cases of delay, combined with long periods of incarceration, should be considered under Section 439 of the Criminal Procedure Code (Cr.PC) and Section 45 of the Prevention of Money Laundering Act (PMLA).
- The judgment is encouraging for those who value individual freedoms, especially given concerns about the misuse of strict penal laws and the oppressive application of the Prevention of Money Laundering Act (PMLA).
- The Supreme Court noted that out of over 5,000 cases brought under the PMLA in the last 10 years, only 40 resulted in convictions.
- Information presented to Parliament showed that the Enforcement Directorate (ED) filed several cases each year, but convictions were rare, with only one reported in 2020.
- The Court recognized that the criminal justice system's lengthy processes are oppressive, where the legal procedure itself becomes a form of punishment.
- Previous judgments have acknowledged that legal technicalities can prevent justice, a concept described as "the mortality of justice at the hands of law."
- Despite the judgment's strong constitutional basis, it raises a concerning question: Was it appropriate for the Court to accept the prosecution's statement that the trial would be completed within six to eight months?
- The Court also extended the accused's detention based on the prosecution's assurance that the charge sheet would be filed by a specific date.
- This situation suggests that the prosecution might be acting as both prosecutor and judge, which could undermine the principles of natural justice and fair trial.
- In the Indian constitutional system, individual liberty should not depend solely on the fairness of the prosecutor.
- Liberty must be based on justice and inalienable rights that people possess from birth until death.
- Rights are fundamental to the law, and unjust legal processes or laws that do not provide justice must be changed.
- Denying freedom is equivalent to denying humanity, so protecting it from executive overreach is a primary duty of the Supreme Court.
- While people's faith and action are the ultimate safeguards of civil liberties, courts play a crucial role in protecting human rights, which is vital for a healthy democracy.
- By eventually granting Manish Sisodia bail, the Supreme Court corrected its previous hesitation, ensuring that justice was upheld.
- The judgment aims to prevent undertrials from being held in custody indefinitely, losing their freedom, reputation, privacy, and dignity without any accountability.
- The nation should move away from politics driven by personal animosities and focus on justice and dignity for all, strengthening democracy.

Kashmir file (13 August)

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

- A team from the Election Commission of India (ECI), led by Chief Election Commissioner Rajiv Kumar, visited Jammu and Kashmir (J&K) recently.
- This was the ECI's second visit since March, meeting with political party representatives and local administration officials.
- Regional parties in J&K are increasingly demanding elections for the 90-seat Assembly of the Union Territory (UT).
- The Supreme Court's December 2023 judgment on Article 370 stated that legislative assembly elections in J&K should not be delayed until statehood is restored.
- The Court directed the ECI to conduct elections in J&K by September 30, 2024.
- J&K was split into two UTs, and its special status was removed in 2019.
- The last Assembly election in J&K was held in 2014, and the region has not had a representative government since the Peoples' Democratic Party-Bharatiya Janata Party (BJP) coalition government collapsed in 2018.
- The Central government may be encouraged by the high voter turnout of 58% in the April-May 2024 Lok Sabha elections, particularly in the Kashmir Valley, where election boycotts had been common since 1990.
- Holding Assembly elections in Jammu and Kashmir (J&K) would show confidence from the Central government.
- It would also be a positive response to the high voter turnout in the recent elections.
- The Central government has been criticized by rights groups for limiting democratic processes in J&K since its special status was removed in 2019.
- Allowing people to elect their representatives would be a significant step toward restoring and building political processes in J&K.
- Despite ongoing militant attacks, delaying elections due to security concerns could give terrorists more power.

- The government needs to continue its efforts to combat militancy while also initiating political processes.
- Assembly elections could help prevent the feeling of alienation from being exploited by enemies of the country.
- J&K needs a democratic system to address issues like unemployment, electricity shortages, and poor health infrastructure.
- These elections could help heal a region that has suffered from over three decades of conflict.

More and better (13 August)

States must develop capacity to conduct testing and sequencing of viruses

- The Zika outbreak began on June 20, with the first case reported in Pune.
- By the first week of August, Maharashtra had 88 confirmed Zika cases.
- Pune city, the main area affected, has 73 cases, while six are from Pune rural.
- Pregnant women make up half of the confirmed cases.
- Zika can cause Guillain-Barré syndrome, a neurological disorder where the immune system attacks the nerves.
- Pregnant women with Zika risk having babies with microcephaly (smaller than average head size) and other neurological issues.
- A January 2023 study in The Lancet found:
    - 6.6% of babies born to Zika-infected mothers had microcephaly.
    - 18.7% had functional neurological abnormalities.
    - Risks also included premature birth (10.5%), low birth weight, and small size for gestational age (16.2%).
- There is a lesser-known risk of sexual transmission of Zika by infected men, as the virus can remain in semen for at least two months.
- Infected men should be aware of this risk and take measures to prevent transmission to women, following U.S. CDC guidelines.
- It is concerning that the Pune-based ICMR lab only increased testing efforts after news broke about delays in testing by the Pune Municipal Corporation.
- Kerala's recent Nipah virus outbreak and Gujarat's Chandipura virus and acute encephalitis syndrome outbreaks highlight the need for states to improve their testing and virus sequencing capabilities.
- Quick testing is crucial for effective public health responses to limit virus spread and control outbreaks.
- The COVID-19 pandemic showed the benefits of decentralized testing and sequencing.
- This approach should be adopted for all deadly pathogens to improve outbreak management.

Possible revival of Dalit politics today (13 August)

- In the 2024 general election, Dalit political parties like the Bahujan Samaj Party (BSP) in Uttar Pradesh and the Vanchit Bahujan Aghadi (VBA) in Maharashtra have seen a decline, reducing the prominence of Dalit politics.
- However, Dalit parties such as the Lok Janshakti Party (LJP) in Bihar and Viduthalai Chiruthaigal Katchi (VCK) in Tamil Nadu show that Dalit politics can remain relevant if they form alliances with larger national political groups.
- The current trend shows a decrease in commitment to Ambedkarite values, as Dalit parties are seeking various ways to remain significant.
- This diversity in approach indicates a lack of a unified, grand political vision among Dalit parties to challenge traditional ruling elites on a national scale.
- Dr. B.R. Ambedkar hoped that modern democracy would empower marginalized groups, like Dalits, to challenge the dominance of social elites.
- With the decline of major Dalit parties, there are fewer supporters of this transformative vision.
- Dalit politics, based on social justice, has recently become less influential and more passive.
- There’s no clear agreement among Dalit political parties on their core beliefs or goals.
- Dalit leaders are seen as lacking both a clear political vision and impactful social initiatives.
- Unlike other parties that form alliances to protect their interests, Dalit parties haven’t tried to unite different Dalit groups nationally.
- They often focus on regional issues and lack a strong national agenda.
- Other marginalized groups, like Adivasis and Muslims, are cautious about engaging with Dalit parties due to doubts about their commitment and beliefs.
- National parties, like Congress, have been successful by addressing the concerns of marginalized groups and promoting constitutional values.
- Chandrashekhar Azad’s win in Nagina, Uttar Pradesh, highlights the potential for revitalizing independent Dalit politics.
- Azad successfully engaged with marginalized groups, including Muslims, and challenged both right-wing and secular-socialist parties.
- His approach shows that a new, radical perspective in Dalit politics could revive and strengthen the movement.

Unified political bloc

- A unified political bloc of Dalit parties like BSP, VCK, and VBA could revitalize the social justice movement and drive significant political change.
- This bloc should form at the national level and work with other regional and national alliances focused on social justice and constitutional ideals.
- Dalit leaders need to see themselves as key players against right-wing politics and work together more effectively.
- Recent decisions by BSP and VBA have often isolated Dalits from secular, progressive groups and inadvertently supported BJP.
- For success, Dalit parties must unite to create a new social justice agenda that addresses issues like neo-liberalism and Hindutva.
- This unity requires overcoming personal egos, resolving internal conflicts, and ending ideological divisions.
- Dalit leaders should offer strong intellectual and visionary leadership to challenge current political passivity.
- Intellectuals, activists, and civil society should discuss forming a federal Dalit front to push for a radical agenda and transform economic and political systems.

Socio-economic differentials within SCs/STs (13 August)

Disparities among SC/ST sub-groups have led the Court to endorse sub-classification, aiming at ensuring a fairer distribution of reservation benefits

- A critique of group-based affirmative action policies is that they treat entire groups as homogeneous, while in reality, there are significant differences within these groups.
- Even among disadvantaged groups, families can have vastly different access to resources, leading to benefits primarily for the more advantaged within these groups.
- This can increase inequality within the group, contrary to the goal of affirmative action, which is to promote greater equality.
- In India, reservations for SCs and STs in education, employment, and politics are constitutionally mandated, but there are many subgroups within these categories with varying levels of disadvantage.
- There has been dissatisfaction because benefits often go to a few subgroups within SCs/STs, prompting calls for sub-classification to ensure a fairer distribution of benefits.
- The Supreme Court previously ruled in 2004 that SCs and STs should not be further subdivided, treating them as a single, homogeneous class.
- However, a recent ruling on August 1, 2024, allows for sub-classification within SC/ST quotas, acknowledging socio-economic differences within these groups.
- Despite this, detailed analysis of these intra-group inequalities is limited, even though census data is available on socio-economic indicators for SCs and STs.
- The analysis focuses on socio-economic disparities within SCs/STs in a few large states by comparing two significant sub-groups (one better-off and one more deprived) to illustrate these disparities.
- Census data show that different sub-groups within SCs and STs experience varying levels of urbanization.
- Some sub-groups are more urbanized and therefore have better educational opportunities and less precarious employment.
- For example, Musahars in Bihar and Uttar Pradesh are among the most disadvantaged, with very low levels of educational attainment. In contrast, Pasis in Bihar and Chamars in Uttar Pradesh are slightly better off.
- In Maharashtra, Bhambis are more advantaged compared to Mangs in terms of education and job opportunities.
- Similarly, Chamars in Punjab have higher educational attainment and urban exposure compared to Mazhabis.
- In West Bengal, Namsudras and Bagdis show significant differences in urbanization, education, and livelihood.
- Among STs, Halba tribes in Chhattisgarh are more urbanized and better educated than Baiga tribes, who also work more in agriculture.
- Oraons in Jharkhand are more educated and better off than Mal Paharia tribes, and the same pattern is seen between Oraons and Bhumia in Odisha.
- In Rajasthan, Meenas are highly educated and economically advanced, whereas Garasias have seen less development.
- The analysis highlights persistent socio-economic disparities within SCs and STs, suggesting that the benefits of undifferentiated reservations may have primarily gone to the more advantaged sub-groups.
- Sub-classification and sub-quotas within SC/ST reservations could help distribute benefits more equitably among different sub-groups.

On the allegations against the SEBI chief

What are the accusations brought forth by New York-based Hindenburg Research against SEBI Chairman Madhabi Puri Buch and her husband Dhaval Buch? How is Blackstone involved? What is the status of the ongoing investigation by SEBI into the Adani Group's actions?

GS Paper III: Capital Market

Saptaparno Ghosh

The story so far:

New York-based Hindenburg Research has released a new set of documents to substantiate its accusation that the ongoing investigation into insider trading and other stock market violations by the Adani Group by India's financial regulator – the Securities and Exchange Board of India (SEBI) – is compromised. In its latest tranche, Hindenburg has included emails and publicly available records of stakes held by SEBI Chairman Madhabi Puri Buch and her husband Dhaval Buch in Adani Group-related entities through offshore investment funds to allege a conflict of interest that aided the Adani Group to "syphon monies". The short seller attempts to establish a correlation between the alleged use of two offshore funds, the couple's investments and varied professional engagements to accuse Ms. Buch of being biased toward the Adani Group. Both Ms. Buch and the Adani Group have denied the charge.

What is short selling about?

Short selling entails profiting from a fall in the prices of a scrip. Although short selling can serve many purposes, such as mitigating demand-supply imbalances in scrips and ensuring price efficiency, it has also been used as a means of manipulation – or what the U.S Securities and Exchange Commission (SEC) has described as a "bear raid". Thus, prompting concerns about intent and credibility. As a practice, it entails selling a borrowed scrip in anticipation of a downward price movement and buying it back when the lower price level is realised. Let us say, anticipating a downward movement, an individual sells 10 shares at ₹100 apiece. The total sale value is ₹1,000. The price of the share decreases to ₹85 apiece and they opt to buy the quantity back. This time it will cost them ₹850 – a direct profit of ₹150.

The short seller in discussion had shorted electric truck maker Nikola Corp in 2020 placing concerns about their functionality. In October 2022, the Nikola's founder Trevor Milton was convicted by a U.S. jury of fraud for lying to investors about the technology.

What is the SEBI chief accused of?

At the centre of the allegations are the Buchs' alleged "hidden stakes" in certain offshore funds in Bermuda and Mauritius, two tax havens, and their professional engagements during and before Ms. Buch's tenure at SEBI. Hindenburg asserts concern on two fronts, a conflict of interest and an ensuing collusion.

About personal investments: gathering from investigations by the Organized Crime and Corruption Reporting Project (OCCRP), the short seller points to Vinod Adani, brother of Adani Group Chairman Gautam Adani, who invested in the Bermuda-based 'Global Dynamic Opportunities Fund' (GDOF), which then invested in the Mauritius-based IPE Plus Fund 1. A separate investigation by the *Financial Times* said that the parent fund of GDOF, that is, the Global Opportunities Fund (GOF) were used by two Adani associates, Nasser Ali Shaban Ahli from UAE and Chang Chung-Ling from Taiwan, to amass and acquire large positions in scrips of the conglomerate, amounting to stock manipulation. Additionally, as per the Hindenburg report, the founder and Chief Investment Officer (CIO) of the IPE Plus Fund was Anil Ahuja, director at Adani Enterprises for nine years until 2017.

REUTERS

The Buchs opened an account with the Mauritius-based fund in 2015. The short seller places that SEBI's alleged unwillingness to take "meaningful action" (in the ongoing investigation) could stem from the chairperson's "complicity" in using the exact same funds as Mr. Adani.

The other set of accusations relate to their professional engagements. In 2013, Ms. Buch had set up a consulting firm Agora Partners in India and Singapore respectively. Important to note that she became a whole-time member with SEBI in April 2017 before being elevated as the chairperson in March 2022. SEBI's Code on Conflict of Interests for Members of Board stipulates that whole-time members can neither hold any office of profit nor engage in any professional activity that involves receiving any fees or payment. However, the short seller accuses her of transferring only the 100% stake in the Singapore unit (not the Indian one) after her appointment to the top post, and that too only in 2022. In an X post responding to the Buchs statement Hindenburg says: "Buch remained a 100% shareholder of Agora Partners Singapore until March 16th, 2022, per Singaporean records, owning it during her entire time as a SEBI Whole Time Member. She only transferred her shares into her husband's name 2 weeks after her appointment as SEBI Chairperson."

The last set of accusations concern her husband, Dhaval Buch. The short seller stated that Mr. Buch notwithstanding a lack of prior experience in either real estate nor fund management, was appointed senior advisor at the investment management firm Blackstone in 2019. With Ms. Buch employed at SEBI and later at the helm of affairs, the report accuses, that SEBI "proposed, approved and facilitated" major changes to real-estate investment trusts' (REITs) policies and rules on listing and other stock market related activities. Thus, enabling Blackstone – "one of the largest REIT sponsors in India" – to benefit from the changes, Hindenburg alleged.

What has been the recent exchange about their investments?

In a detailed statement, the Buchs said the investments referred to in Hindenburg's report were made two years before Ms. Buch joined SEBI. While addressing concerns about collusion, the Buchs stated the investment was undertaken considering Mr. Ahuja's "strong investing career" and that he was also Mr. Buch's "childhood friend" and a batchmate at IIT Delhi. Re-emphasising their argument, they pointed to redeeming their investment in the fund when Mr. Ahuja stepped down as its CIO in 2018. The joint statement further affirms that at no point the fund invested in any bond, equity or derivative of the Adani conglomerate.

However, Hindenburg in its response on 'X', said the response only confirmed the investment in the offshore fund. Mr. Ahuja also served as a director at the Adani Group until 2017, something the conglomerate has also mentioned in their response to the short-seller's allegations. Hindenburg emphasised the Buchs' investments in the offshore fund was first made in 2015, when Mr. Ahuja was still a director at the Adani Group. The short seller also pointed to Ms. Buch's communications in 2017 and 2018. In 2017, Mr. Buch had sought that the ownership be transferred entirely to him. However, in 2018, during her tenure as a whole-time SEBI member, Ms. Buch sought to redeem the units in the fund – prompting concerns about continued engagement.

What about the consulting firm?

The statement from the Buchs also stated that two consulting companies in discussion had become "immediately dormant on her appointment with SEBI". This was also disclosed to SEBI. It further informs that Dhaval Buch in 2019, started his own consultancy practice with "prominent clients in the Indian industry" enabled by his deep expertise in "supply chain" management.

In their 'X' post however, Hindenburg accused the SEBI chief of still holding a 99% stake in the Indian consulting entity, and not her husband. The entity, it said, was active and generated revenues to the tune of $3,12,000 between financial years 2022-2024, when Ms. Buch was the SEBI chief. About the Singapore unit, the short seller said Ms. Buch only transferred the stake in 2022, after becoming the chairperson and held it during her entire tenure as a whole-time member.

Hindenburg further alluded to more conflict of interest concerns based on the firm's clientele (if they are regulated by SEBI) and its revenue. The short seller expresses its inability to trace the same (about the Singapore unit) citing the local legislation exempting the firm from making disclosures. However, it deems the information as necessary to assess the "probity of the chairperson's external business".

What of the Blackstone appointment?

About Mr. Buch's appointment at Blackstone, the couple stated that the appointment was on account of Mr. Buch's expertise in supply chain management. It furthers states that at no point was Dhaval Buch associated with the real-estate side of Blackstone.

In fact, it also informs about Blackstone Group being immediately added to the incumbent SEBI chief's recusal list. The markets regulator in its standalone statement also described Hindenburg's accusations as "inappropriate". The statement other than explaining the mandatory exhaustive consultation process, also pointed to having underscored the potential of REITs, SM REITs, InvITs and Municipal Bonds among other asset classes for democratisation of markets, financialisaton of household savings and for capital formation through markets.

Where do we stand now?

The Supreme Court in an order this January had, among other things, sought SEBI to also probe whether the losses suffered by Indian investors because of Hindenburg's erstwhile report involved any "infraction of the law". SEBI issued a show cause notice to the short seller this June. "It is unfortunate that instead of replying to the show cause notice, they have chosen to attack the credibility of SEBI and attempt character assassination of the Chairperson," SEBI said. In an order dated January 3, the SC had also asked SEBI to complete the investigation into the pending two allegations of the twenty-four overall ones within three months. It informed on Sunday about having completed one of them and the other being "close to completion".

In fact, the apex court in the same order had refused to transfer the investigation from SEBI to the Special Investigative Team (SIT) or the Central Bureau of Investigation (CBI). But it noted that it would exercise its powers in "extraordinary circumstances" if the competent authority displays a "glaring, wilful and deliberate" inaction in carrying out the investigation.

THE GIST

- New York-based Hindenburg Research has released a new set of documents to substantiate its accusation that the ongoing investigation into insider trading and other stock market violations by the Adani Group by India's financial regulator — the Securities and Exchange Board of India (SEBI) — is compromised.
- At the centre of the allegations are the Buchs' alleged "hidden stakes" in certain offshore funds in Bermuda and Mauritius, two tax havens, and their professional engagements during and before Ms. Buch's tenure at SEBI.
- The Supreme Court in an order this January had, among other things, sought SEBI to also probe whether the losses suffered by Indian investors because of Hindenburg's erstwhile report involved any "infraction of the law".

On the allegations against the SEBI chief (13 August)

What are the accusations brought forth by New York-based Hindenburg Research against SEBI Chairman Madhabi Puri Buch and her husband Dhaval Buch? How is Blackstone involved? What is the status of the ongoing investigation by SEBI into the Adani Group's actions?

- Hindenburg Research has released documents accusing India's financial regulator, SEBI, of being compromised in its investigation into the Adani Group for insider trading and stock market violations.
- The documents include emails and records showing investments by SEBI Chairman Madhabi Puri Buch and her husband Dhaval Buch in Adani Group-related entities through offshore funds.
- Hindenburg claims this constitutes a conflict of interest, suggesting it helped the Adani Group to "syphon monies."
- Both Ms. Buch and the Adani Group deny these allegations.
- Short selling is a trading strategy where investors profit from a decline in the price of a stock.
- It involves borrowing a stock, selling it at a high price, and buying it back later at a lower price to return it.
- For example, if you sell 10 shares at ₹100 each, making ₹1,000, and later buy them back at ₹85 each, costing ₹850, you make a profit of ₹150.
- Short selling can stabilize prices but can also be used for manipulation, leading to concerns about its intent.
- In 2020, a short seller raised concerns about Nikola Corp, an electric truck maker, and in 2022, Nikola's founder was convicted of fraud for deceiving investors about the technology.

What is the SEBI chief accused of?

- Allegations Against the Buchs:
    - Hindenburg Research accuses the Buchs of having "hidden stakes" in offshore funds in Bermuda and Mauritius, suggesting a conflict of interest and collusion.
- Personal Investments:
    - Investigations show Vinod Adani, brother of Gautam Adani, invested in the Bermuda-based Global Dynamic Opportunities Fund (GDOF), which then invested in the Mauritius-based IPE Plus Fund 1.
    - The Financial Times found that the parent fund of GDOF, the Global Opportunities Fund (GOF), was used by Adani associates to acquire large positions in Adani Group stocks, potentially manipulating the market.
    - The founder of IPE Plus Fund, Anil Ahuja, was a director at Adani Enterprises until 2017.
    - The Buchs opened an account with the Mauritius-based fund in 2015, and Hindenburg suggests SEBI's lack of action could be due to Ms. Buch's alleged connection to these funds.
- Professional Engagements:
    - Ms. Buch established a consulting firm, Agora Partners, in India and Singapore in 2013. She joined SEBI in April 2017 and became chairperson in March 2022.
    - SEBI's rules prohibit board members from holding other paid positions, but Hindenburg claims Ms. Buch transferred her stake in Agora Partners Singapore to her husband only after becoming SEBI chairperson.
    - Hindenburg argues that Ms. Buch owned Agora Partners Singapore until March 16, 2022, which is during her time at SEBI.
- Accusations Against Dhaval Buch:
    - Dhaval Buch, despite lacking experience in real estate and fund management, was appointed a senior advisor at Blackstone in 2019.
    - Hindenburg alleges that SEBI, under Ms. Buch's leadership, made changes to REIT policies and stock market rules that benefited Blackstone, a major REIT sponsor in India.

What has been the recent exchange about their investments?

- The Buchs explained that their investments in the offshore fund were made before Ms. Buch joined SEBI and were influenced by Mr. Ahuja's strong investment background and personal relationship with Mr. Buch.
- They redeemed their investment in 2018 after Mr. Ahuja left his position at the fund, and they claimed the fund did not invest in Adani Group shares.
- Hindenburg responded by confirming the Buchs' investments in the offshore fund and noted that Mr. Ahuja was still with Adani Group when the Buchs invested.
- Hindenburg also pointed out that Ms. Buch sought to redeem the fund units during her time at SEBI, raising concerns about potential ongoing involvement.

What about the consulting firm?

- The Buchs claimed their consulting companies became inactive when Ms. Buch joined SEBI, and this was disclosed to SEBI.
- Dhaval Buch started his own consultancy in 2019, focusing on supply chain management.

- Hindenburg accused Ms. Buch of still holding a 99% stake in her Indian consulting firm, which was active and earned $312,000 during her SEBI tenure.
- Hindenburg also claimed Ms. Buch transferred her stake in the Singapore unit only after becoming SEBI chairperson.
- The firm's clients and revenue raised concerns about potential conflicts of interest, but Hindenburg could not trace details due to local laws.
- The Buchs responded that Mr. Buch's Blackstone appointment was due to his expertise, not real estate, and noted that Blackstone was added to Ms. Buch's recusal list at SEBI.
- SEBI called Hindenburg's accusations inappropriate and noted its role in promoting market democratization and financial inclusion.
- The Supreme Court ordered SEBI to investigate whether Hindenburg's report led to legal violations and to complete the investigation into two out of twenty-four allegations within three months.
- The court also decided against moving the investigation to a Special Investigative Team or the CBI but reserved the right to act if SEBI shows significant inaction.

Securities and Exchange Board of India (SEBI)

The Securities and Exchange Board of India (SEBI) is the regulatory authority responsible for overseeing and developing the securities market in India. It operates under the administrative control of the Ministry of Finance. Established as a non-statutory body in 1988, SEBI was granted statutory powers in 1992 through the Securities and Exchange Board of India Act, 1992.

- **Chairman: Madhabi Puri Buch, born in 1966, is the current chairperson of the Securities and Exchange Board of India (SEBI) and the first woman to hold this role. She is married to Dhawal Buch.**
- **Headquarters: Mumbai, Maharashtra**

Primary Objectives

SEBI's primary objectives are to:

- Protect the interests of investors in securities.
- Promote the development of, and regulate the securities market.
- Ensure fair practices in the securities market.

Key Functions

Market Regulation

- **Registration and Regulation of Intermediaries:** SEBI registers and regulates a wide range of market intermediaries, including stockbrokers, sub-brokers, investment advisers, mutual funds, depositories, and custodians.
- **Issue of Capital and Listing of Securities:** SEBI regulates the process of issuing securities to the public, including initial public offerings (IPOs), follow-on public offers (FPOs), and rights issues. It also oversees the listing of securities on stock exchanges.
- **Supervision of Stock Exchanges and Depositories:** SEBI monitors the activities of stock exchanges and depositories to ensure fair and efficient market practices.
- **Enforcement of Market Regulations:** SEBI takes strict action against entities and individuals involved in insider trading, market manipulation, and other fraudulent activities.

Investor Protection

- **Investor Education:** SEBI conducts investor awareness programs to educate the public about the securities market and the risks involved.
- **Redressal of Investor Grievances:** SEBI provides mechanisms for investors to lodge complaints against market intermediaries and takes steps to resolve them.
- **Promotion of Investor Interests:** SEBI works to create a conducive environment for investors by promoting transparency, disclosure, and good governance practices.

Market Development

- **Fostering Market Growth:** SEBI undertakes initiatives to promote the growth and development of the securities market, such as introducing new products and encouraging participation from various investor segments.
- **Market Efficiency and Transparency:** SEBI strives to enhance market efficiency by promoting fair pricing, reducing transaction costs, and improving information dissemination.
- **Internationalization:** SEBI takes steps to integrate the Indian securities market with global markets, facilitating cross-border investments.

The tech that helps vehicles from bumping into each other

Most collision avoidance systems require two pieces of information: the locations of all the other vehicles and the location of this vehicle relative to those vehicles

GS Paper III: S&T

Vehicular traffic is a mainstay of modern life. And therefore, the number of transport options people have invented and the number of places to deploy them in have increased. Today, we have traffic on the road, in the air, across various water bodies, and – in a dubitable sign of progress – in space. For better or for worse, we can't roll this traffic back very much, so we have collision avoidance systems instead.

What is a collision avoidance system?
In broad terms, a collision avoidance system (CAS) is a collection of technologies to help a vehicle steer clear of another vehicle or obstacle. For example, a CAS device fit on a train will be designed to help that train avoid colliding with another train. Most CAS devices require two pieces of information, preferably in real-time: the locations of all the other vehicles and the location of this vehicle relative to those vehicles. Over the years, scientists and engineers have developed instruments that collect this information and transmit it and other instruments that receive this information and aid in the navigation of the vehicle.

Such a vehicle can be driven by a human, in which case CAS's purpose would be to assist the driver, or be autonomous.

How does CAS help land-based vehicles?
Say two cars, called the Front Car and the Back Car, are moving in sequence and both are fit with CAS devices. Typically, the Back Car will be tracking the speed of the Front Car, the distance between the two cars, and the speed of the Back Car. If the separation between the two cars is expected to drop within a certain value in a stipulated time frame, the CAS may be empowered to deploy an automatic emergency brake – as required of cars in the European Union, for example – without the driver's intervention.

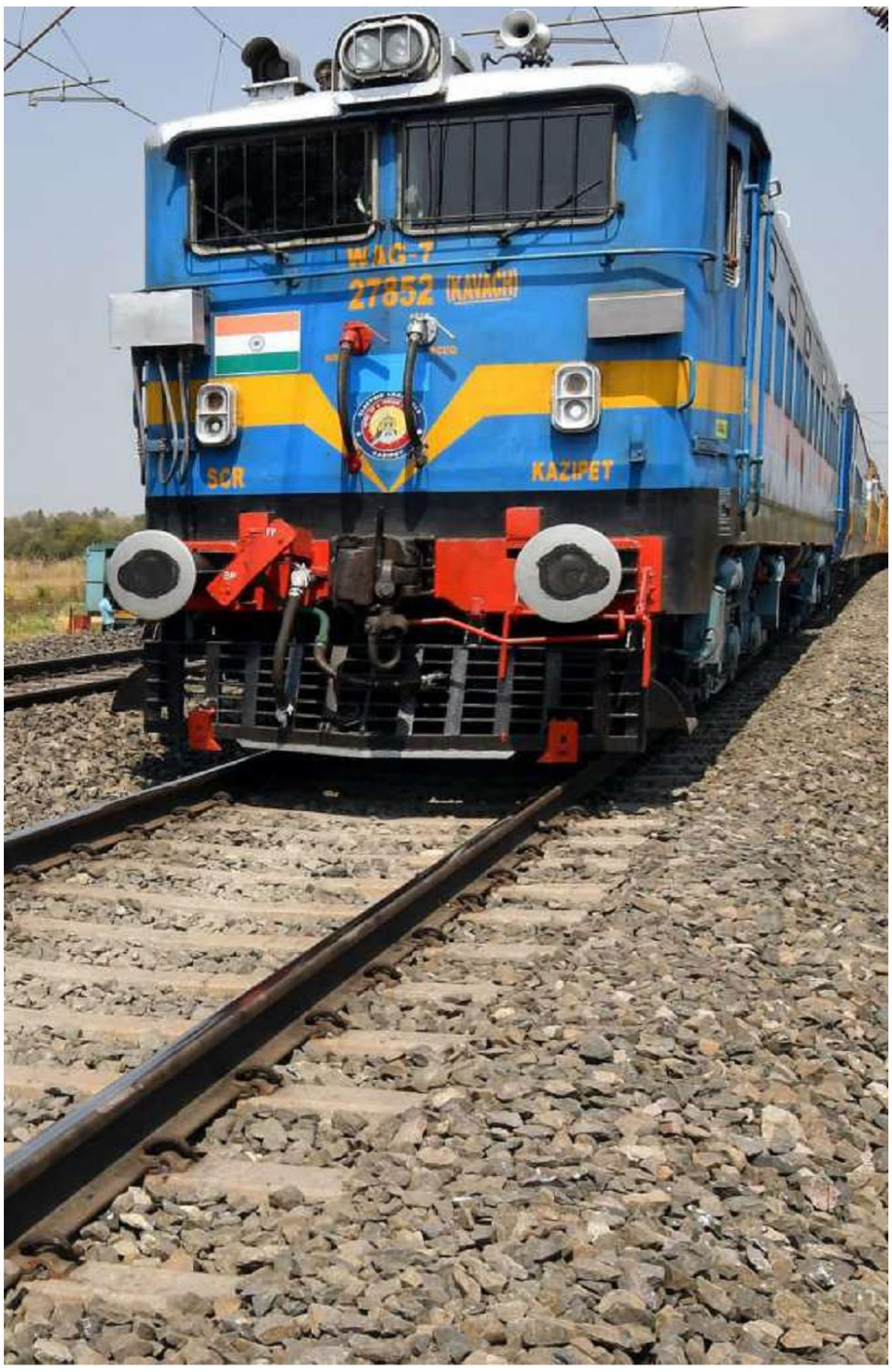
In order to achieve this, the CAS will have to be connected to the Back Car's braking system and be able to override the driver's instructions. It will also be connected to the Back Car's speed metre as well as equipped with a sensing technology to track the Front Car, like radar, lidar, and/or cameras with object recognition.

What is 'Kavach'?
Another important land-based mode of transport is the railway.

A spate of train accidents in India recently put the spotlight on the sluggish implementation of 'Kavach', the homegrown CAS for the Indian Railways. In their fundamentals, Kavach's components perform the same functions that CAS does in cars, but the railway system is more complicated.

Kavach has three main components: onboard, trackside, and communications. For the purpose of explanation, let's regroup them as computers, communications, and control.

Computers – there is a computer onboard the train plus two other computers for station masters. Of the latter, one is the master computer: it collates and processes information from signals and interlocking points and sends its output to the locomotive computer. The other is the remote interface unit, which also collates and processes information from various points on the railway network, and eventually transmits its data to the master computer; it doesn't communicate directly with the locomotive computer.



NAGARA GOPAL

The locomotive computer receives information from two other sources – (i) from the two Radio-Frequency Identification (RFID) readers mounted on its underside. The tracks will be fit with RFID cards at fixed intervals. When the locomotive passes over the cards, the readers will scan the cards and retrieve the train's location and a track ID number, and send them to the onboard computer; (ii) additionally, onboard computers can communicate with each other if their respective locomotives are nearby.

Taken together, the system facilitates communications between stations and locomotive pilots, facilitates pilots' decision-making (with or without having to visually spot another train), maintains speed, issues sounds and alarms when passing through areas with low visibility, and applies emergency brakes when a collision is expected.

Communication – the remote interface unit transmits data to the master computer via fibre-optic cables. The master computer communicates with the locomotive computer via ultra-high frequency radio. The onboard computer uses GSM-Railway to communicate with the overall network management system (the software system that animates the Kavach CAS), including to authenticate its communications with nearby master computers and locomotive computers.

Control – as with cars, the onboard computer is connected to various other parts of the locomotive, including its braking system and an alarm to alert pilots. While operating the locomotive, pilots will use a bespoke interface – like a digital screen – that relays information from the computer and receives inputs from the pilots. The station master will have a similar interface, with the ability to send SOS messages as well.

How does CAS work in ships and aircraft?
The Traffic Collision Avoidance System for aircraft also has a computer-communication-control setup as for trains. An important component is the transponder – a device that, when it receives a radio-frequency ping, produces a response. Using the transponders of various other aircraft, the host aircraft can build up a 3D view of the air traffic around itself.

Another salient component of aircraft CAS is the alerts. If another aircraft is within 48 seconds away on a potential collision course, the computer sounds a traffic advisory that requires the pilots to visually identify the other aircraft. If the aircraft is less than 30 seconds away, the computer requires the pilots to make a resolution: report the alert as soon as possible to air traffic control and manoeuvre the aircraft to a safer course, if required contrary to air traffic control's instructions; and revert to the original course once the resolution is complete.

Finally, aircraft may also have radar altimeters to sense the distance to the ground and another system to alert pilots to 'tall' features like towers and ground antennae.

Ships – akin to cars and aircraft – use a combination of visual sighting and radar to steer clear of each other, while these operations are similarly assisted with the use of additional systems. Two important ones are AIS and LRIT. In the AIS, or Automatic Identification System, base stations on land track data received from transceivers onboard ships to infer their location, speed, and bearing, and transmit the details to each vessel.

LRIT is short for 'Long Range Identification and Tracking'. According to the International Maritime Organisation, a ship on an international voyage is required to report its location, local time, and onboard equipment once every six hours to the authorities in the country under whose flag the ship is sailing. This data is distributed to contracting governments and to operators of search-and-rescue missions via the International LRIT Data Exchange.

How have satellites changed CAS?
An important alternative to the transponder-based system for aircraft is the Automatic Dependent Surveillance-Broadcast (ADS-B) system, which collects and processes information shared actively by each aircraft via satellites to understand the relative location, bearing, and speed of a group of aircraft. Similarly, the AIS for ships can be facilitated by satellites as well: such S-AIS systems are useful to track ships that are too far from AIS stations on land.

The advent of the U.S. Global Positioning System (GPS) had a transformative effect on navigation and collision avoidance worldwide, and which some countries have augmented with systems of their own to cater to specific national needs. For example, India already envisages the use of its NavIC constellation of navigational satellites to assist road and railway traffic.

Recall also the Front Car + Back Car scenario: if the country these cars are moving through also has a GPS-tagged database of its various traffic elements (stop signs, turns, signals, intersections, etc.), the CAS onboard the cars can also be assisted by GPS data. The spatial frequency of GPS for civilian applications is restricted to 10 metres, which is not good enough for CAS. But systems can overcome this limitation using differential GPS capabilities, which can improve the resolution to less than a metre.

The tech that helps vehicles from bumping into each other (13 August)

Most collision avoidance systems require two pieces of information: the locations of all the other vehicles and the location of this vehicle relative to those vehicles

- Collision avoidance systems (CAS) help vehicles avoid collisions with other vehicles or obstacles.
- CAS devices need real-time information on the locations of other vehicles and the vehicle using the system.
- CAS can assist human drivers or control autonomous vehicles.
- For land-based vehicles, like cars, CAS tracks the speed and distance between vehicles.
- If a collision risk is detected, CAS can automatically apply the brakes if necessary, as required in the EU.
- CAS is connected to the vehicle's braking system and speed meter, and uses sensors like radar, lidar, and cameras to monitor other vehicles.

What is 'Kavach'?

Kavach is a collision avoidance system for Indian Railways.

It includes:

- **Computers**:
  - Onboard computer in the train.
  - Master computer and remote interface unit at stations.
  - Locomotive computer gets data from RFID readers on tracks and nearby trains.
- **Communication**:
  - Data is sent from the remote unit to the master computer via fiber-optic cables.
  - Master computer communicates with the train via ultra-high frequency radio.
  - Onboard computer uses GSM-Railway for network communication.
- **Control**:
  - Onboard computer connects to braking system and alarm.
  - Pilots use a digital screen for information and controls.
  - Station masters have an interface to monitor and send SOS messages.

How does CAS work in ships and aircraft?

Aircraft Collision Avoidance System:

- **Transponders**: Respond to radio-frequency pings to help build a 3D view of surrounding air traffic.
- **Alerts**:
  - 48 seconds away: Pilots receive a traffic advisory to visually identify the other aircraft.
  - 30 seconds away: Pilots must report the situation to air traffic control, possibly maneuver the aircraft, and return to the original course afterward.
- **Radar Altimeters**: Measure distance to the ground and alert pilots to tall features like towers.

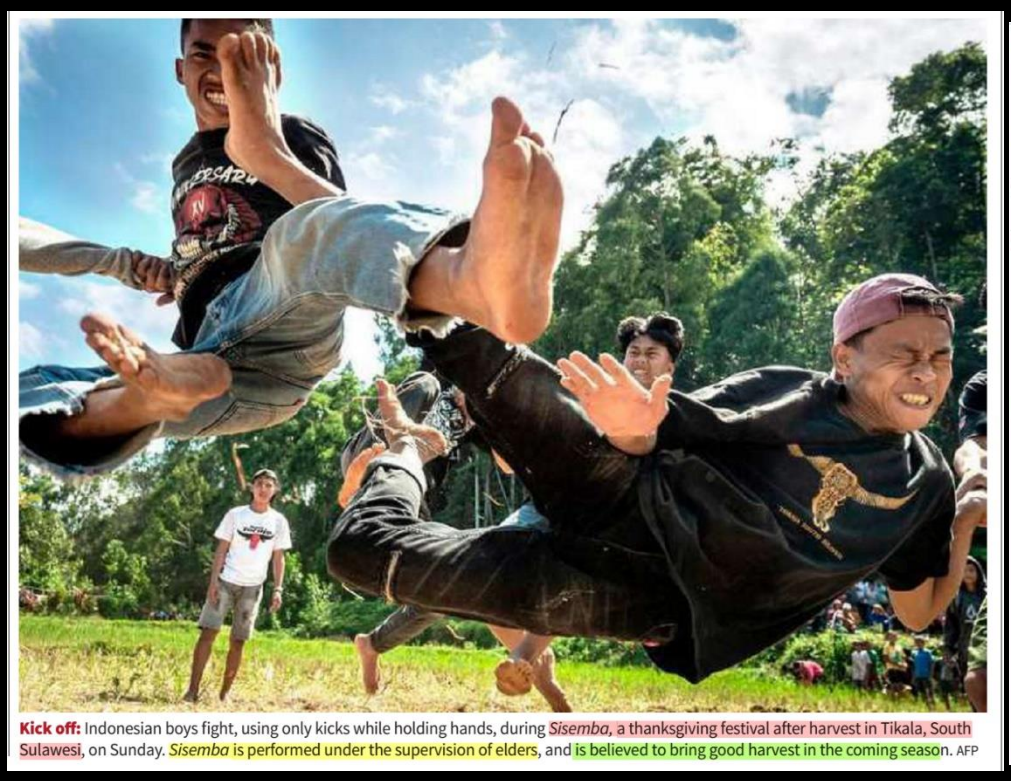
Ship Collision Avoidance System:

- **AIS (Automatic Identification System)**: Ships send data about their location, speed, and bearing to base stations, which track and share this information.
- **LRIT (Long Range Identification and Tracking)**: Ships report their location and details every six hours to authorities, with data shared for search-and-rescue operations.

Satellites in CAS:

- **ADS-B (Automatic Dependent Surveillance-Broadcast)**: Uses satellites to gather and share aircraft data for better tracking.
- **S-AIS**: Satellite-based AIS for tracking ships that are out of range of land-based stations.
- **GPS**: Revolutionized navigation and collision avoidance. Countries like India use GPS and its own systems (NavIC) for traffic management.

- **Differential GPS**: Enhances GPS accuracy from 10 meters to less than a meter for improved collision avoidance in vehicles.



Kick off: Indonesian boys fight, using only kicks while holding hands, during *Sisemba*, a thanksgiving festival after harvest in Tikala, South Sulawesi, on Sunday. *Sisemba* is performed under the supervision of elders, and is believed to bring good harvest in the coming season. AFP