Sleepy Classes
Free. Regular. Quality.

Weekly Editorial Analysis (WEA)

8th March 2021

Table of Contents

Click here to watch the following topics on Youtube

1. Iran Nuclear deal

Nuclear enrichment

- Mined uranium has less than 1 percent of the uranium-235 isotope used in fission reactions, and centrifuges increase that isotope's concentration. Uranium enriched 3-4 % percent is used in nuclear power plants
- 20 percent it can be used in research reactors or for medical purposes.
- High-enriched uranium, at some 90 percent, is used in nuclear weapons.

The vital but delicate task of reviving the Iran deal

Time is running out for the Joe Biden administration, but there is an opportunity for Brussels to take a lead role

RAKESH SOOD

Of all the foreign policy challenges facing the Joe Biden administration, none is more critical than salvaging the Joint Comprehensive Plan of Action (JCPOA, or the Iran nuclear deal) that has been unravelling over the last three years when Donald Trump unilaterally discarded

can Senate, Mr. Obama was unable to get the nuclear deal ratified but implemented it on the basis of periodic Executive Orders to keep sanction waivers going.

Mr. Trump had never hidden his dislike for the JCPOA calling it a "horrible, one sided deal that should have never, ever been made". After ranting about it for a year, he finally pulled the plug on it in May 2018 and embarked on a policy of 'maximum pressure' to coerce Iran back to the negotiating table. The U.S. decision was criticised by all other parties to the JCPOA (including the European al

GETTY IMAGES/ISTOCKPHOTO

sanctions, widening their scope to cover nearly all Iranian banks connected to the global financial system, industries related to metallurgy, energy and shipping, individuals related to the defence

of the special inspection provisions with the IAEA within two months if sanctions relief was not forthcoming.

No appetite for talks

Clearly, Mr. Trump's policy may have provided comfort to Israel's leader Benjamin Netanyahu and Saudi Crown Prince Mohammed bin Salman, but it failed to bring Iran back to the negotiating table and only strengthened the hardliners. Iran has suffered and there is no appetite for more negotiations. The E-3's promised relief instrument in support of trade

not be enough to overcome this impasse.

Overcoming the impasse

The Biden administration has made a good start by appointing Robert Malley as the U.S. Special Envoy for Iran but he will need help. Positive steps along multiple tracks are necessary for creating a conducive atmosphere. Release of European and American nationals currently in custody in Iran would help. Clearing Iran's applications to the International Monetary Fund for COVID-19 relief and for

About IAEA

- The IAEA is the international centre for cooperation in the nuclear/ atomic field. It is a UN agency. It works with its member countries and many partners to promote peaceful uses of nuclear technologies.

  ✓Set up as the world's "Atoms for Peace" organization in 1957 within the United Nations family.

  ✓Reports to both the United Nations General Assembly and Security Council.

  ✓Headquarters in Vienna, Austria

Non-Proliferation Treaty (NPT -1968)

- aimed at limiting the spread of nuclear weapons including three elements:

  ✓ non-proliferation,

  ✓disarmament,

  ✓peaceful use of nuclear energy.

Nuclear & Non-Nuclear Weapon States

- The Treaty defines nuclear weapon states (NWS) as those that had manufactured and detonated a nuclear explosive device prior to 1 January 1967.
- All the other states are therefore considered non-nuclear weapon states (NNWS). The five nuclear weapon states are China, France, Russia, the United Kingdom, and the United States.

Nonproliferation

- Nuclear weapon states are not to transfer to any recipient whatsoever nuclear weapons and not to assist, encourage, or induce any NNWS to mNon-nuclear weapons states are not to receive nuclear weapons from any transferor, and are not to manufacture or acquire them.
- NNWS must accept the International Atomic Energy Agency (IAEA) safeguards on all nuclear materials on their territories or under their control.

Disarmament

- All Parties must pursue negotiations in good faith on effective measures relating to the cessation of the nuclear arms race and to nuclear disarmament, and on a treaty on general and complete disarmament under strict and effective international control.

NPT

Peaceful Use

- All state parties undertake to facilitate, and have a right to participate, in the exchange of equipment, materials, and scientific and technological information for the peaceful uses of nuclear energy

Members

- South Sudan, India, Israel, and Pakistan remaining outside the treaty
- North Korea announced January 10, 2003, that it was withdrawing from the treaty, effective the next day. Although Article X of the NPT requires that a country give three months' notice in advance of withdrawing, North Korea argued that it satisfied this requirement because it originally announced its decision to withdraw March 12, 1993, and suspended the decision one day before it was to become legally binding. There is not yet a definitive legal opinion as to whether North Korea is still a party to the NPT.

About

- Iran's interest in nuclear technology dates to the 1950s, when the Shah of Iran received technical assistance under the U.S. Atoms for Peace program

Atom for peace

- A U.S. program announced by President Dwight D. Eisenhower at the United Nations on 8 December 1953 to share nuclear materials and technology for peaceful purposes with other countries

Increase enrichment

- Negotiations from 2013 and 2015 between Iran and P5+1 (China, France, Germany, Russia, the United Kingdom, the United States, and the European Union, or the EU).

Iran Nuclear Program and JCPOA

- In 2015, Iran with the P5+1 group of world powers - the USA, UK, France, China, Russia, and Germany agreed on a long-term deal on its nuclear programme.
- The deal was named as Joint Comprehensive Plan of Action (JCPOA) and in common parlance as Iran Nuclear Deal.
- Under the deal, Iran agreed to curb its nuclear activity in return for the lifting of sanctions and access to global trade.
- Iran's uranium stockpile was reduced by 98% to 300kg (660lbs), a figure that must not be exceeded until 2031. It must also keep the stockpile's level of enrichment at 3.67%.
- No enrichment will be permitted at Fordo until 2031, and the underground facility will be converted into a nuclear, physics and technology centre. The 1,044 centrifuges at the site will produce radioisotopes for use in medicine, agriculture, industry and science
- US experts estimated then that if Iran had decided to rush to make a bomb, it would take two to three months until it had enough 90%- enriched uranium to build a nuclear weapon - the so-called "break-out time"

About

- For the first year after the U.S. withdrawal, Iran's response was muted as the E-3 (France, Germany, the U.K.) and the EU promised to find ways to mitigate the U.S. decision. The E-3's promised relief Instrument in Support of Trade Exchanges (INSTEX), created in 2019 to facilitate limited trade with Iran
- INSTEX-to circumvent U.S. sanctions against trade with Iran by avoiding the use of the dollar.
- However, by May 2019, Iran's strategic patience ran out as the anticipated economic relief from the E-3/EU failed to materialize. As the sanctions began to hurt, Tehran shifted to a strategy of 'maximum resistance'.

Iran's Policy of 'Maximum Resistance'.

- Beginning in May 2019, Iran began to move away from JCPOA's constraints incrementally: exceeding the ceilings of 300kg on low- enriched uranium and 130 MT on heavy-water; raising enrichment levels from 3.67% to 4.5%; stepping up research and development on advanced centrifuges; resuming enrichment at Fordow, and violating limits on the number of centrifuges in use.

Roadblocks in Restoration of Deal

- Regional Cold War Between Iran & Saudi Arabia:
- The traditional Shia vs Sunni conflict precipitated into a regional cold war between Iran & Suadi Arabia.
- Thus, a major challenge for the US to restore the nuclear deal is to maintain peace between the two regional rivals.

Iran Gone too Far

- The challenge in resuming the agreement in its present form is that Iran is currently in violation of several of its important commitments, such as the limits on stockpiles of enriched uranium.

- The International Atomic Energy Agency noted that Iran now had more than 2,440 kilograms, which is more than eight times the limit set by the 2015 nuclear deal.
- Further, Iran says it wants the US to pay for the billions of dollars in economic losses it incurred when it pulled the United States out of the Iran deal in 2018 and reinstituted sanctions that it had lifted.

Impacts on India For Restoration of JCPOA

- May ease many restrictions over the Iranian regime, which may directly or indirectly help India.

- Boost to Regional Connectivity: Removing sanctions may revive India's interest in the Chabahar option,
  - ✓This would further help India to neutralize the Chinese presence in Gwadar port, Pakistan.
  - ✓Revival of International North-South Transit Corridor (INSTC), which runs through Iran, which will improve connectivity with five Central Asian republics, may also get a boost.
- Energy Security: Due to the pressure linked to the US' Countering America's Adversaries Through Sanctions Act (CAATSA), India has to bring down oil imports to zero.
- Restoration of ties between the US and Iran will help India to procure cheap Iranian oil and aid in energy security.

2. Financial action task force (FATF)

- Inter-governmental body established in 1989 during the G7 Summit in Paris.
- Its Secretariat is located at the Organisation for Economic Cooperation and Development (OECD) headquarters in Paris.
- FATF currently comprises 37 member jurisdictions and 2 regional organisations
- Argentina, Australia, Austria, Belgium,Brazil, Canada, China., Denmark.,European Commission, Finland, France, Germany,Greece, Gulf Co-operation Council,Hong Kong, China, Iceland, India, Ireland, Israel,Italy,Japan.Republic of Korea, Luxembourg, Malaysia Mexico, Netherlands, New Zealand, Norway, Portugal, Russian Federation, Saudi Arabia , Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, US.

G7 Countries

- intergovernmental organisation (1975)
- Meets annually to discuss issues of common interest like global economic governance, international security and energy policy.
- No formal constitution or a fixed headquarters.

- The decisions non-binding.

- G-7 is a bloc of industrialized democracies i.e. France, Germany, Italy, the United Kingdom, Japan, the United States, and Canada.
- The G7 was known as the 'G8' for several years after the original seven were joined by Russia in 1997.
- Russia was expelled as a member in 2014 following the latter's annexation of the Crimea region of Ukraine.

40+9 Recommendation

- 1990-40 recommendation on ML
- 2004 – 9 Special recc on Terrorist financing

Grey and Black list

- Grey List:
  - ✓Countries that are considered safe haven for supporting terror funding and money laundering are put in the FATF grey list. This inclusion serves as a warning to the country that it may enter the blacklist.
  - ✓officially referred to as Jurisdictions Under Increased Monitoring
  - ✓countries on the FATF grey list represent a much higher risk of money laundering and terrorism financing but have formally committed to working with the FATF to develop action plans that will address their AML/CFT deficiencies.
  - ✓Albania, the Bahamas, Barbados, Botswana, Cambodia, Ghana, Iceland, Jamaica, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen and Zimbabwe.
- Black List
  - ✓Countries known as Non-Cooperative Countries or Territories (NCCTs) are put in the blacklist. These countries support terror funding and money laundering activities. The FATF revises the blacklist regularly, adding or deleting entries.
  - ✓Iran & North korea

Pakistan

- Pakistan was put back on it in June 2018, and handed a 27-point action list to fulfil.
- It had three remaining points of the 27 that were only partially addressed, notably all in the area of curbing terror financing.
- Remaining tasks: demonstrating terror-funding prosecution is accurate, effective and dissuasive, and thoroughly implementing financial sanctions against all terrorists designated by the UN Security Council, which include LeT founder Hafiz Saeed, JeM chief Masood Azhar, other leaders of terror groups in Pakistan, and those belonging to al Qaeda.

UNSC

- Established by the UN Charter in 1945. It is one of the six principal organs of the United Nations.

- The other 5 organs of the United Nations are—the General Assembly, the Trusteeship Council, the Economic and Social Council, the International Court of Justice, and the Secretariat.
- Its primary responsibility is to work to maintain international peace and security
- A total of 15 members are there in the Council, out of which 5 are permanent and 10 are not permanent.
- The five permanent members include China, France, the Russian Federation, the United Kingdom and the United States.

UNSC Members

- The non-permanent members are elected for two-year terms by the United Nations General Assembly (UNGA).
- Five members of the UNSC are replaced every year.
- Originally, there were 11 members of the Security Council: 5 permanent and 6 non-permanent members. In 1963, the General Assembly recommended an amendment to the Charter to increase the membership of the Security Counci
- Set the pattern for geographic representation as follows:
  - ✓5 from African and Asian States (three are for Africa and two for Asia.)
  - ✓1 from Eastern European States
  - ✓2 from Latin American States
  - ✓2 from Western European and other States
- In June 2020, India was elected to the UNSC as a non-permanent member, winning 184 out of the 193 votes at the UNGA.
- This membership is for 2021-22.
- India was the only candidate from the Asia-Pacific category for the year 2021-22. Previously, India had been a member in the years 1950-1951, 1967-1968, 1972-1973, 1977-1978, 1984-1985, 1991-1992 and 2011-12.

Pakistan

- Pakistan to complete the remaining tasks by June 2021, when the FATF will meet again to vote on the issue
- Pakistan's next steps on the FATF directive to successfully prosecute terrorists and terror financers identified by the grouping are in its own interests

Grey list impact

- Economic sanction (IMF, WB)
- Trade reduction
- Loan restriction
- Financial downgrade & difficult loan

- Sign
- Like all pol parties, terrorist gp require money
- Sequeezing money more efficacious way of dealing than army

Pakistan case

- 2012-15- raised $5 billion from international bond market - Import- Export remain stable
- Recent report that calculated Pakistan has lost $38 billion because of its time on the grey list (2008-2015 and 2018-the present).

3. Cybersecurity

Cyberspace

- refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyber security

- techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation
- Specops Software analyzed the latest data from Center for Strategic and International Studies (CSIS) to discover which countries across the world have experienced the most "significant" cyber-attacks between May 2006 and June 2020.
- Significant" cyber-attacks are defined as cyber-attacks on a country's government agencies, defense and high-tech companies, or economic crimes with losses equating to more than a million dollars.

Lack of Umbrella organization

- India has 36 different central bodies to look after cyber issues. Each organization has its own reporting structure and CERT (Indian Computer Emergency Response Team). On the other hand countries like the US, Singapore etc. have a national organization that deals with cyber threats.

Digital economy

- India's digital economy comprises of 14-15% of its total economy and is expected to rise up to 20% by 2024. Thus, there is an urgent need for India to upgrade its cybersecurity strategy

Attacks

- In the year 2016, banks announced that details of 3.2 million debit cards were leaked. In 2018, Cosmos Bank, based in Pune lost Rs 94 Crore in a malware attack. In September 2019, the Kudankulam nuclear plant was attacked via malware.

The Techniques Most Commonly Used to Cause Significant Cyber Attacks

- Denial of Service Attack (DoS): A DoS attack occurs when a cybercriminal makes a machine or network resource unavailable to its intended
- SQL Injection Attack: An SQL injection is a malicious SQL code inserted by cyber criminals into a database to access sensitive information that was never intended to be displayed.
- A man-in-the-middle (MitM): A MitM attack happens when a cybercriminal intercepts communication between two parties through a range of online avenues such as email, social media and web browsing. The purpose of a MitM attack may involve hijacking password credentials, spying on victims, or modifying traffic between parties.
- Phishing Attack: Phishing is a cyber-attack practice where cyber criminals send emails that appear to be from trusted entities, but are in fact a fraudulent attempt to gain authentication details from victims such as login credentials, payment information, and personal address.

Recent Cyber Attacks

- There has been a steep rise in the use of resources like malware by a Chinese group called Red Echo to target “a large swathe” of India’s power sector.Red Echo used malware called ShadowPad, which involves the use of a backdoor to access servers.
- Chinese hacker group known as Stone Panda had “identified gaps and vulnerabilities in the IT infrastructure and supply chain software of Bharat Biotech and the Serum Institute of India.
- SolarWinds hack, impacted national critical infrastructure in the USA.

Cyber crimes

- National Cyber Security Coordinator Lt Gen (Dr) Rajesh Pant recently made the following observations on Cyber Crimes in India:
- Cyber crimes in India caused Rs 1.25 trillion loss in 2019.
- Cyber threats will continue to increase as the country starts developing smart cities and rolling out 5G network, among other initiatives.
- There are only a few Indian companies who are making some of the cyber security products and there is a big vacuum in the sector.

Recommendation

- A dedicated industry forum for cyber security should be set up to develop trusted indigenous solutions to check cyber attacks

National Cyber Security Policy, 2013

- With primary aim to monitor and protect information and strengthen defences from cyber-attacks, the National Cyber Security Policy, 2013 was released by the Government of India.
- It aims to achieve through:
  - ✓Creating workforce of 5, 00,000 professionals skilled in next five years through capacity building, skill development and training.
  - ✓Developing suitable indigenous technologies in ICT sector.
  - ✓Providing fiscal benefits to corporate sector for adoption of cyber security.
  - ✓Safeguarding the privacy of citizens' data.
  - ✓Enabling effective prevention, detection and investigation of cybercrimes.
  - ✓Creating and promote the culture of cyber security.
  - ✓Enhancing global cooperation in cyber security.

issues

- India was one of the first few countries to propound a futuristic National Cyber Security Policy 2013. However, since its adoption, not much has changed in terms of a coordinated cyber approach. The current cyber threat poses significant challenges due to rapid technological advancements such as Cloud Computing, Artificial Intelligence, 5G, etc.
- The new cyber challenges include a long list-- data protection or privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms and much more. Thus, the existing structures must be revamped or revitalised.

National Cyber Security Strategy 2020: (4th March)

- To improve cyber awareness and cybersecurity through more stringent audits. Empanelled cyber auditors will look more carefully at the security features of organisations than are legally necessary now.

Key points

- There will be table-top cyber crisis management exercises regularly to reinforce the idea that cyber attacks can take place regularly.
- It does call for an index of cyber preparedness, and attendant monitoring of performance.
- A separate budget for cybersecurity is suggested, as also to synergise the role and functions of various agencies with the requisite domain knowledge.
- Online cybercrime reporting portal to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content.
- Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

- National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.
- CERT-In-to report cyber security incidents
- Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) for providing detection of malicious programmes and free tools to remove such programmes.

Need

- Citizen awareness
- Focus upon Artificial Intelligence, Robotics, Virtual reality & augmented reality, Internet of things (IOT) which would be the backbone of the country in future.
- CERT-In should engage academic institutions and follow an aggressive strategy.
- There should be increased partnership of government and private sector since the majority of the country's cyber resources are controlled by entities outside of the government.
- More investment in this field in terms of finance, skill training and manpower is required. There is a need to increase the number of cyber security experts and IT security auditors, in which the nation is facing a crisis at present.
- Explicit privacy laws in the country must be enacted addressing the concerns regarding encroachment on citizens' privacy and civil- liberties.

4. Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021.

Who is an Intermediary?

- An 'intermediary' has been defined in Section 2(w) of the Act as "any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, web-housing service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes"

Intermediary Liability under the Information Technology Act, 2000

- Section 79 of the Act is a 'safe harbour' provision which grants conditional immunity to intermediaries from liability for third party acts.
- Section 79(1) of the Act grants intermediaries a conditional immunity with regard to any third party information, data or communication link made available or hosted by them. This immunity is subject to section 79 (2) and 79 (3) of the Act.
- 79(2) to be applicable, intermediaries are to have neither knowledge nor control over the information which is transmitted or stored.
- Furthermore, Section 79(3)(b) envisages a 'notice and take down' regime, wherein the intermediary is required to take down unlawful content upon receiving actual knowledge of its existence.
- Section 79 states that an intermediary (Digital media and OTTs) shall not be liable for any third party information, data, or communication.

2011 guidelines

- After the amendment to the IT Act in 2008, the Government of India introduced the Intermediary Guidelines, which were mandatory for all intermediaries to follow for claiming safe harbour protection.
- Intermediaries to publish rules and regulations, privacy policy and user agreement;
- Rules and regulations, terms and conditions or user agreement shall specify all prohibited acts, i.e. belonging to other persons, grossly harmful, harassing or unlawful, harms minors, infringes any intellectual property rights, violates any law, is deceiving or misleading, impersonates any person, contains virus, threatens India etc. and the intermediary should inform users that violation of same shall lead to termination of access.
- Intermediaries to disable such information within 36 hours and storage of same for 90 days for investigation purposes,
- Intermediaries to appointment and publish the details of a Grievance Officer on its website.

issues

- Ambiguity in prohibited content and forced decision by intermediaries.
- Further, any person could request the intermediaries to take down the unlawful content.

Shreya Singhal v Union of India (2015)

- In Shreya Singhal vs. UOI, the Supreme Court read down Section 79(3)(b) to mean that an "intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatebale to Article 19 (2) are going to be committed then fails to expeditiously remove or disable access to such material".
- Thus, an intermediary is only required to act upon receiving a court order or a notification from the appropriate government or its agency.
- The intermediary is not required to exercise its own discretion regarding the material which is to be removed or disabled.

New IT rules

Reason

Users

- Bigger user base over 44.8 Crore YouTube users, over 53 crore WhatsApp users, and 41 Crore Facebook users.

Existing loopholes

- Section 69 of the IT Act gives power to the government to issue directions "to intercept, decrypt or monitor...any information generated, transmitted, received or stored" in any digital equipment.
- The Intermediaries are required to preserve and retain specified information. Further, they have to obey the directions issued by the government from time to time.

Sec 79

- By adhering to government rules, they will get protected from legal action for any user-generated content under Section 79.
- Section 79 states that an intermediary (Digital media and OTTs) shall not be liable for any third party information, data, or communication.

New IT Rules related to Social Media

- Publishing unlawful information
  - ✓Social media companies are prohibited from hosting or publishing any unlawful information in relation to the interest of the sovereignty and integrity of India, public order, friendly relations with foreign countries, etc.
  - ✓Government role- the government can take down prohibited information within 24 hours. The user will be given a notice before his/her content is taken down.
- Monthly compliance report
  - ✓social media companies need to publish a monthly compliance report.
- Traceability
  - ✓The government can direct messaging platforms to tie the identity of the user with the message transmitted by him/her for strengthening traceability.
- Safe harbour provisions
  - ✓The safe harbour provisions have been defined under Section 79 of the IT Act, and protect social media intermediaries by giving them immunity from legal prosecution for any content posted on their platforms.
  - ✓In case, due diligence is not followed by the intermediary, safe harbour provisions will not apply to them
- Safety and Dignity of Users:
  - ✓Intermediaries shall remove or disable access within 24 hours of receipt of complaints of contents that exposes the private areas of individuals, show such individuals in full or partial nudity or in sexual act or is in the nature of impersonation including morphed images etc.
  - ✓Such a complaint can be filed either by the individual or by any other person on his/her behalf.
- Grievance Redressal Mechanism is Mandatory:
  - ✓Intermediaries shall appoint a Grievance Officer to deal with complaints and share the name and contact details of such officers.
  - ✓Grievance Officer shall acknowledge the complaint within twenty four hours and resolve it within fifteen days from its receipt.
- Categories of Social Media Intermediaries:
- Based on the number of users, on the social media platform intermediaries have been divided in two groups:
  - ✓Social media intermediaries.

✓Significant social media intermediaries.

- Additional Due Diligence for the Significant Social Media Intermediaries:
- Appointments:
  - ✓Appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and Rules. Such a person should be a resident of India.
  - ✓Appoint a Nodal Contact Person for 24×7 coordination with law enforcement agencies. Such a person shall be a resident in India.
  - ✓Appoint a Resident Grievance Officer who shall perform the functions mentioned under the Grievance Redressal Mechanism. Such a person shall be a resident in India
- Identity of the Originator:
  - ✓Significant social media intermediaries providing services primarily in the nature of messaging shall enable identification of the first originator of the information.
  - ✓Required only for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, Or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material punishable with imprisonment for a term of not less than five years.
- Compliance report:
  - ✓Need to publish a monthly compliance report mentioning the details of complaints received and action taken on the complaints as well as details of contents removed proactively.

New IT Rules related to Digital media and OTT platforms:

- A Code of Ethics has been prescribed for OTT platforms and digital media entities.
- The streaming platforms (Like Netflix and Amazon Prime) will have to self-classify content on five age-based categories:
- U (universal), U/A 7+, U/A 13+, U/A 16+, and A (Adult).
- Parental lock
  - ✓Platforms would be required to implement parental locks for content classified as U/A 13+ or higher, and reliable age verification mechanisms for content classified as “A”.
- News publisher
  - ✓Publishers of news on digital media will have to observe the norms of journalistic conduct of the Press Council of India and the Programme Code under the Cable Television Networks Regulation Act.
  - ✓A three-level grievance redressal mechanism has also been established:

Grievance Redressal Mechanism

- A three-level grievance redressal mechanism has been established under the rules with different levels of self-regulation.

- Level-I: Self-regulation by the publishers
  - ✓ Publisher shall appoint a Grievance Redressal Officer based in India who shall be responsible for the redressal of grievances received by it.
  - ✓ The officer shall take decision on every grievance received by it within 15 days.
- Level-II: Self-regulation by the self-regulating bodies of the publishers;
- Self-Regulatory Body:
  - ✓ There may be one or more self-regulatory bodies of publishers.
  - ✓ Such a body shall be headed by a retired judge of the SC, a High Court or independent eminent person and have not more than six members.
  - ✓ Such a body will have to register with the Ministry of Information and Broadcasting.
  - ✓ This body will oversee the adherence by the publisher to the Code of Ethics and address grievances that have not been resolved by the publisher within 15 days.
- Level-III: Oversight mechanism
- Oversight Mechanism:
  - ✓ Ministry of Information and Broadcasting shall formulate an oversight mechanism.
  - ✓ It shall publish a charter for self-regulating bodies, including Codes of Practices. It shall establish an Inter-Departmental Committee for hearing grievances.
- Display Rating:
  - ✓ Shall prominently display the classification rating specific to each content or programme together with a content descriptor informing the user about the nature of the content, and advising on viewer description (if applicable) at the beginning of every programme enabling the user to make an informed decision, prior to watching the programme.

Issues

Traceability' and breaking encryption?

- Many platforms (Whatsapp, Telegram but even other platforms) retain minimal user data for electronic information exchange and also deploy end-to-end encryption to provide reliability, security and privacy to users
- Encryption becomes even more important now as more of our lives involve our personal data being aggregated and analysed at a scale that was never possible before.
- In the past, the Report of the Justice Srikrishna Committee on Data Protection has also criticised the government for mandating low encryption standards in license agreements with telecom service providers because "this poses a threat to safety and security of the personal data of data principals."

Development of AI to automate censorship

- Significant social media intermediary (such as WhatsApp, Signal, Twitter, Instagram or Facebook etc.) to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information like depicting rape, child sexual abuse or conduct.

- This will be a slippery slope where use of automated tools will be expanded beyond instances of sexual violence and child sexual abuse material.
- Underdeveloped and imperfect nature of AI in the current state-of- the-art. AI "learns" by examining vast amounts of data, and the development of a censorship
- AI is likely to require social media intermediaries to store and examine large amounts of user-generated content that does not in any way relate to the kind of content sought to be censored.
- AI seeks to control and monitor the exercise of a user's fundamental right to freedom of speech and expression. It is necessary to carefully consider whether AI ought to be allowed to regulate the fundamental rights of citizens.

OTT

- This oversight mechanism is being created without any clear legislative backing and will now increasingly perform functions similar to those played by the Ministry of Information and Broadcasting for TV regulation.
- Today, India is no longer a consumer but a producer of original high quality video content that provides employment and entertainment to audiences locally and globally. It competes actively with other countries such as South Korea and needs an environment that recognises that traditional cinema or television based regulation may irreparably harm the sector.
- Any such model of regulation will likely have a substantial impact on citizens' digital rights, result in economic harm, and also negatively impact India's growing cultural influence through the production of modern and contemporary video formats entertainment

Digital News Media

- With respect to regulation of news media, several concerns abound. The purview of the Information Technology Act, 2000 does not extend to news media, and so the guidelines do not have the legislative backing to regulate news media. Thus, these Rules are exercising powers far beyond the parent legislation
- The vague definition of "publisher of news and current affairs content" may also lead to further arbitrariness. The definition excludes replica e-papers of newspapers from its ambit
- Such a definition also privileges the established media houses, who may have a print newspaper as a significant component of their operations and could thus claim to be exempted from these guidelines.
- Smaller and independent media houses on the other hand may not have the luxury to do so, and instead rely on the internet to disseminate news and information. This discriminatory approach between online news media

Positive side

Balanced approach

- The ministry's announcement reveals an approach that is aligned with the thinking of today without imposing unreasonable boundaries on the innovation and expression that must continue to lead the country into the future. With this refreshing light-touch and empowering approach, the guidelines are clearly designed to carefully balance the many priorities and contexts of all stakeholders of these ecosystems while ensuring that the rule of law can be enforced objectively and in full alignment with the Constitution

Value generation

- Help in acceleration of value generation and inclusive empowerment of their local users, while global companies that have large user bases in the country can also align with a common framework that protects creators and consumers alike

Empowerment

- The proposal has clearly-defined grievance redressal mechanisms that empower every social and digital media intermediary to self- enforce effective mechanisms to address complaints from users

Safety and dignity

- With a special focus on protecting the online safety and dignity of users, especially women, the guidelines have prioritised affirmative addressal of the most serious issues that have affected India's digital population.
- They also ensure that the digital platform companies are empowered to report the first originator of the grievance-causing information, thus ensuring that liability is limited while the country's laws can be fully and effectively enforced on the actual perpetrators.
- Equally importantly, they provide users with an opportunity to be heard — a vital defence against the arbitrary censorship that several social media platforms are increasingly embracing globally

Regulate arbitrariness

- Twitter's recent move to " suspend" former US President Donald Trump's account for "violations of the Twitter Rules", while refusing to comply with the GOI's blocking orders on accounts that clearly violated Indian law, has demonstrated the comical arbitrariness in the interpretations that are made by some of these digital platform companies

Conclusion

- The need of the hour is for every country to have a body of clearly- defined policy that is consistent with the principles of their democracies.
- India has taken a leadership position and made these issues a matter of inclusive public debate through this announcement.
- The country's guidelines will ensure that unlawful information has clear boundary conditions, liability is defined, the process for enforcement of orders is transparent, and that all social and digital media companies can rely on a consistent definition of the ethics code that protects all participants in the digital ecosystem.