PM IAS ACADEMY

CREATIVE THOUGHT AND ACTION

PMIAS
be inspired

MASTER CHECKUP

GS 3 INTERNAL SECURITY

PM IAS ACADEMY

Erode | Coimbatore

www.pmias.in | 7373799495 | 04223572299

MANAGING PERCEPTIONS

Why in news?

- Group of envoys on a guided tour of Jammu and Kashmir (J&K), has triggered the debate over sovereignty of India.
- Clearly, the government, which has been under considerable international pressure to lift restrictions in the former State, has managed to arrange these three visits without any incident.
- The delegations have been taken to meet with local groups, and shown a glimpse of 'normalcy' in the Kashmir Valley, with shops open, people out on the streets, and boating on the Dal Lake.
- The chimera of 'normalcy' seems patently fragile.
- The visit had to be postponed by a day due to a bandh call in the Valley; and just a day after the visit, the Internet was snapped once again due to security concerns.

TERROR AND PUNISHMENT

- The Pakistani government, which for years tried to protect Hafiz Saeed, the alleged mastermind of the 2008 Mumbai attacks, finally got a conviction and a jail term for the cleric in two terror financing cases
- The Jamaat-ud-Dawa chief and his close aide Malik Zafar Iqbal have been sentenced to five-and-a-half years by an anti-terrorism court, vindicating India's years-long position that Saeed had been using his organisations to finance terrorist activities.
- It started cracking down on Saeed's groups in 2018 only after it was threatened to be put on the "grey list" of the Financial Action Task Force (FATF), an inter-governmental body fighting money laundering and terror financing. The government endorsed the UN ban on these organisations in February 2018
- Unsurprisingly, the conviction of Saeed and Iqbal comes a few days ahead of another crucial FATF meeting. In the 2019 October meeting, the organisation had warned Islamabad to take "extra measures" for the "complete" elimination of terror financing and money laundering.
- If the FATF is not satisfied with Pakistan's actions, the country faces the risk of being downgraded to the "black list", which could bring tough sanctions on its financial system
- The fundamental problem is Pakistan's policy of exporting terrorism to its neighbours for geopolitical leverage. Historically, Pakistan has adopted a dual policy towards terrorism — fight it at home but export it through proxies to its neighbours.

SWISS CHEESE MODEL AND DEFENCE REFORMS

Understanding Swiss Cheese model in simple terms

The Swiss cheese model is associated with accident investigation in an organisation or a system

- A system consists of multiple domains or layers, each having some shortcomings.
- These layers are visualised in the model as slices of Swiss cheese, with the holes in them being the imperfections.
- Normally, weaknesses get "nullified" because of the holes being unaligned. So, when there is a hole in a spot on one layer, the next layer does not have a hole and it is covered.
- At some point, the holes in every slice align to let a hazard pass through and cause an accident – this is because weaknesses are not covered.

Three slices in defence set-up

In a nation's defence preparedness, Swiss Cheese model works in the reverse way: The slices represent the major constituents in a nation's war-making potential, while the holes are pathways through which the domains interact.

At the macro level, there are only three slices with holes in each. These must align to ensure that a nation's defence posture is in tune with its political objectives.

In the Indian defence set-up, the three slices are:

1. The policymaking apparatus comprising the Department of Military Affairs (DMA) and Ministry of Defence (MoD)
2. The defence research and development (R&D) establishment and domestic manufacturing industry
3. The three services – Indian Army, Indian Navy and Indian Air Force.

Access to the right equipment

- India's security managers have to factor in the increasingly belligerent posture of the country's two adversaries – Pakistan and China.
- Such a security environment (with Terrorist activities in Jammu and Kashmir and ongoing incidents along the northern border with China) demands that the capability accretion of the three services be increased.
- Enter the well-meaning government diktat for buying indigenous only, but for that, in-house R&D and manufacturing entities have to play ball.

Way Forward: To work on the slices of Swiss Cheese

- So, the Swiss cheese slice representing indigenous R&D and a manufacturing supply chain that ensures quality war-fighting equipment, at the right time and in required quantities, still needs some work.
- The forthcoming reform of creating theatre commands is the most talked about result of jointness expected from the Swiss cheese slice in which lie the DMA and a restructured MoD.
- The three services that constitute the third Swiss cheese slice have to contend with the other two slices being in a state of flux for some time to come.

DEFENCE ACQUISITION COUNCIL (DAC)

Why in news?

Defence Acquisition Council (DAC) accorded approval for capital acquisition of various platforms and equipment required by the Indian Armed Forces.

Details

- Focused on indigenous design and development these approvals include acquisitions from Indian industry of Rs 31,130 crore.
- The equipments are going to be manufactured in India involving Indian defence industry with participation of several MSMEs as prime tier vendors.
- The indigenous content in some of these projects is up to 80 per cent of the project cost.
- A large number of these projects have been made possible due to Transfer of Technology (ToT) by Defence Research and Development Organisation (DRDO) to the indigenous industry.

Defence Acquisition Council (DAC)

- As an overarching structure, the Defence Acquisition Council (DAC), under the Defence Minister is constituted for overall guidance of the defence procurement planning process.
- DAC is the highest decision-making body in the Defence Ministry for deciding on new policies and capital acquisitions for the three services (Army, Navy and Air Force) and the Indian Coast Guard.
- The objective of the Defence Acquisition Council is to ensure expeditious procurement of the approved requirements of the Armed Forces in terms of capabilities sought, and time frame prescribed, by optimally utilizing the allocated budgetary resources.
- It was formed, after the Group of Ministers recommendations on 'Reforming the National Security System', in 2001, post Kargil War (1999).

Composition of Defence Acquisition Council

1. Defence Minister: Chairman
2. Minister of State for Defence: Member
3. Chief of Army Staff: Member
4. Chief of Naval Staff: Member
5. Chief of Air Staff: Member
6. Defence Secretary: Member
7. Secretary Defence Research & Development: Member
8. Secretary Defence Production: Member
9. Chief of Integrated Staff Committees HQ IDS: Member
10. Director General (Acquisition): Member
11. Dy. Chief of Integrated Defence: Staff Member Secretary

What is Defence Procurement Process (DPP)?

DPP is a national policy to purchase defence equipment.

The Defence Procurement Procedure mainly contains processes that needs to be followed to streamline and simplify defence procurement procedures and ultimately achieve the objective of self-reliance in meeting all the security needs of the Indian Armed Forces by promoting indigenous design, development and manufacture of Defence weapon systems and, platforms in a time-bound manner without any delays.

DAC APPROVES PURCHASE OF JETS AND UPGRADES

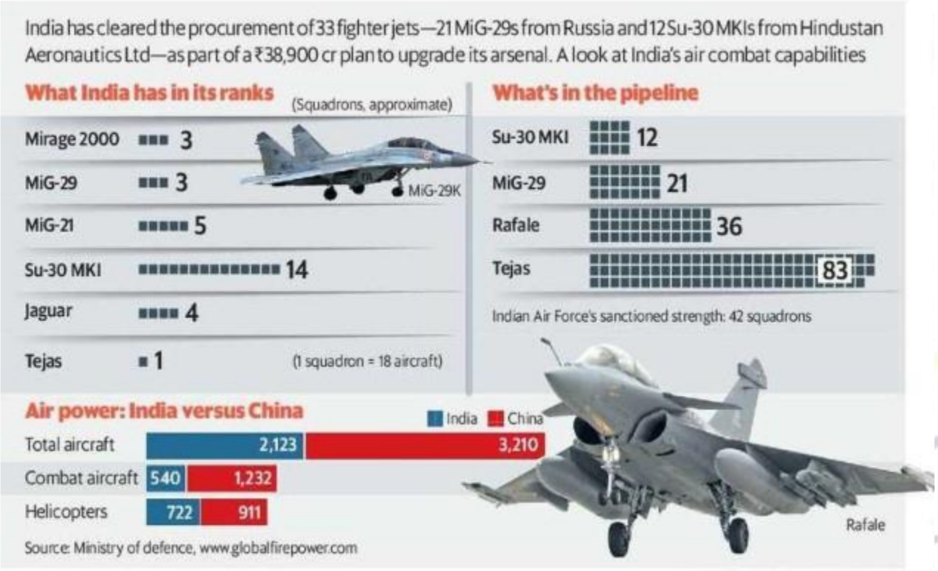
Why in news?

The defence ministry approved several capital procurement projects that include more than 30 new fighter jets, 300 long-range land-attack cruise missiles and 250 air-to-air missiles.

Details

- The projects will take at least two to three years, if not more, to translate into actual inductions into the armed forces but they signal the government's renewed thrust on building military capabilities for the two active borders with China and Pakistan despite budgetary constraints.
- The defence acquisitions council (DAC), chaired by defence minister approved procurement of more MiG-29s and Sukhoi-30 MKIs from Russia.
- HAL to license-produce additional Sukhois which will be licensed produced by defence PSU Hindustan Aeronautics, along with upgraded electronic warfare suites and additional supplies and spares for the fleet.

- Among the projects approved by the DAC are:
- Induction of the Astra beyond-visual-range air-to-air missiles,
- Induction of over 300 land-attack cruise missiles (advanced version of the Nirbhay (fearless) missile),
- Induction of Astra, software-defined radio, Pinaka munitions and the land-attack cruise missiles.



India has cleared the procurement of 33 fighter jets—21 MiG-29s from Russia and 12 Su-30 MKIs from Hindustan Aeronautics Ltd—as part of a ₹38,900 cr plan to upgrade its arsenal. A look at India's air combat capabilities

Source: Ministry of defence, www.globalfirepower.com

OPIUM SEIZURES

Why in news?

The fourth highest seizure of opium in 2018 was reported from India, after Iran, Afghanistan and Pakistan, according to the latest World Drug Report of the United Nations Office on Drugs and Crime (UNODC)

More about news

- The maximum of 644 tonnes of opium was seized in Iran, followed by 27 tonnes in Afghanistan and 19 tonnes in Pakistan. In India, the figure stood at four tonnes in 2018

- Again, Iran reported the highest seizure of heroin (25 tonnes), followed by Turkey, United States, China, Pakistan and Afghanistan.

- Myanmar, which accounts for 7% of the global opium production, and Laos, where 1% of the opium is produced, it is supplied to east and southeast Asia and Oceania

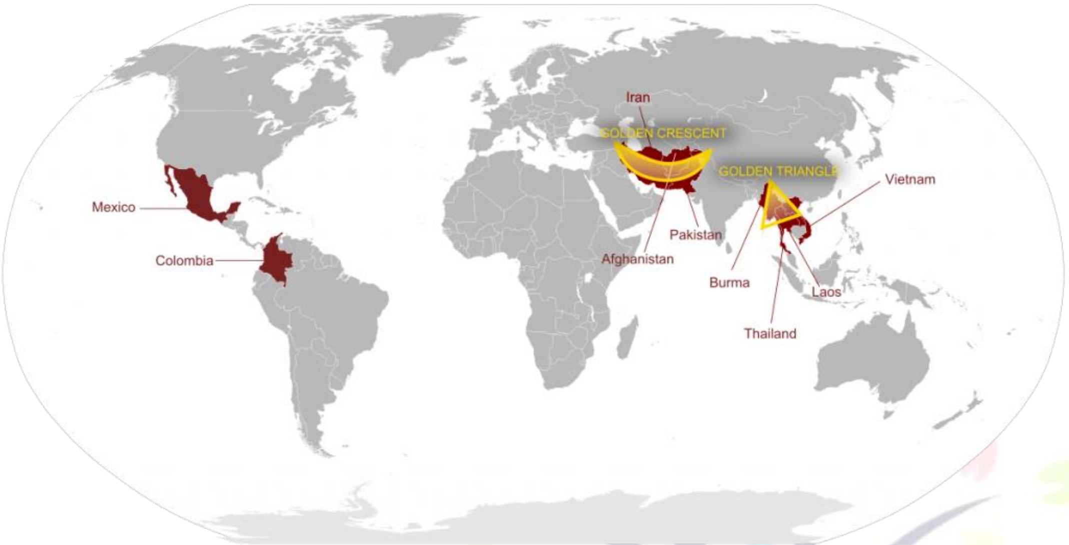
How is Heroin manufactured

Heroin is manufactured from the morphine extracted from the seed pod of opium poppy plants.

Golden crescent

- The **Golden Crescent** is the name given to one of Asia's two principal areas of illicit Opium production , located at the crossroads of central, south and western asia.

- This space overlaps three nations, Afghanistan, Iran and Pakistan whose mountainous peripheries define the crescent.



Golden triangle

The Golden Triangle is located in the area where the borders of Thailand, Myanmar and Laos meet at the confluence of the Ruak and Mekong Rivers. Along with the Golden Crescent, it is regarded as one of the largest producers of opium in the world since the 1950s until it was overtaken by the Golden Crescent in the early 21st century.

AIRCRAFT CARRIERS TO GET INDIAN JETS BY 2032

Why in news?

- The Navy is expected to get the Hindustan Aeronautics Ltd. (HAL)-built twin-engine carrier aircraft by 2032. It will replace the MiG-29Ks in service which are scheduled to start going out by 2034.
- The Navy currently operates Russian-origin carrier INS Vikramaditya and expects to have the first Indigenous Aircraft Carrier (IAC-I) Vikrant operational by 2022. With a second carrier to come in, the Navy is already evaluating a global tender for 57 carrier-based twin-engine fighter aircraft.
- The Navy currently has 45 Russian MiG-29K aircraft and its officials had stated that there will not be enough aircraft to operate from both carriers.

Points for prelims

- The Indian Navy currently operates one aircraft carrier, INS Vikramaditya (Procured from Russia and later modified)
- The second, INS Vikrant (Also called as Indigenous Aircraft Carrier (IAC-I)), is under construction by Cochin Shipyard in Kochi, due for commissioning in 2022.

China currently has two aircraft carriers, with a third in early construction, and a fourth planned for some time in the mid 2020 or 2030s.

PERMANENT COMMISSION TO WOMEN OFFICERS IN ARMY

Why in news?

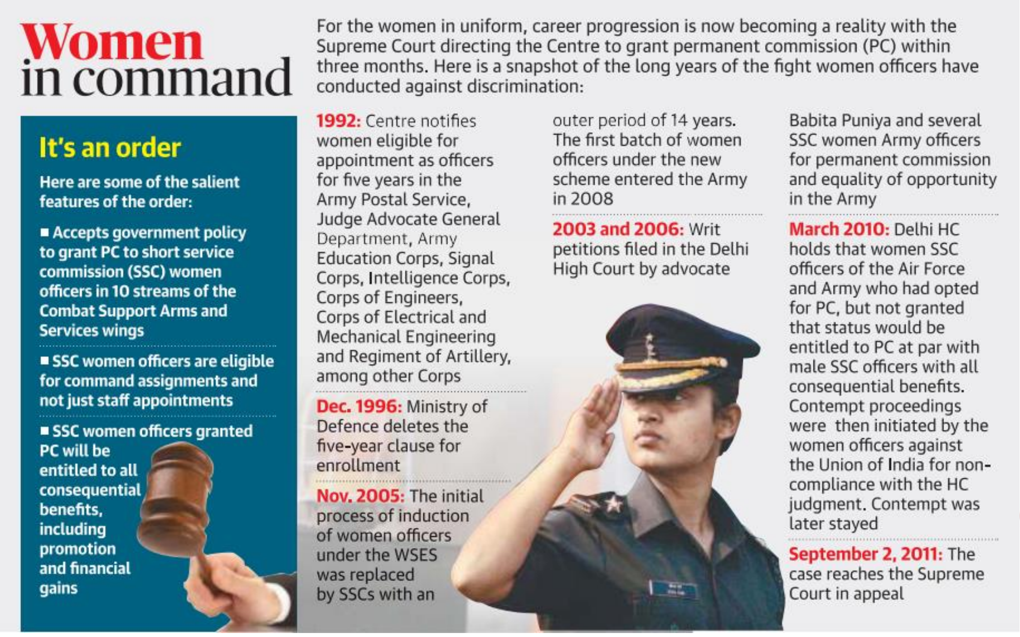
Ministry of Defence has issued the formal Government Sanction Letter for grant of Permanent Commission (PC) to Women Officers in the Indian Army, paving the way for empowering Women Officers to shoulder larger roles in the organisation.

Details

- The order specifies grant of PC to Short Service Commissioned (SSC) Women Officers in all ten streams of the Indian Army.
- In anticipation, the Army Headquarters had set in motion a series of preparatory actions for conduct of the Permanent Commission Selection Board for affected Women Officers.

Recently in news: Supreme Court Eligibility for Permanent Commission

- The Supreme Court **dismissed the Union government's submissions that women are physiologically weaker than men as a "sex stereotype"**.
- The Supreme Court declared that Short Service Commission (SSC) women officers are eligible for permanent commission and command posts in the Army irrespective of their years of service
- The court dismissed the government's stand that only women officers with less than 14 years of service ought to be considered for permanent commission, and those with over 20 years of service should be pensioned immediately.
- The court has done away with all discrimination on the basis of years of service for grant of PC in 10 streams of combat support arms and services, bringing them on a par with male officers.



Women in command

For the women in uniform, career progression is now becoming a reality with the Supreme Court directing the Centre to grant permanent commission (PC) within three months. Here is a snapshot of the long years of the fight women officers have conducted against discrimination:

It's an order

Here are some of the salient features of the order:

- Accepts government policy to grant PC to short service commission (SSC) women officers in 10 streams of the Combat Support Arms and Services wings
- SSC women officers are eligible for command assignments and not just staff appointments
- SSC women officers granted PC will be entitled to all consequential benefits, including promotion and financial gains

1992: Centre notifies women eligible for appointment as officers for five years in the Army Postal Service, Judge Advocate General Department, Army Education Corps, Signal Corps, Intelligence Corps, Corps of Engineers, Corps of Electrical and Mechanical Engineering and Regiment of Artillery, among other Corps

Dec. 1996: Ministry of Defence deletes the five-year clause for enrollment

Nov. 2005: The initial process of induction of women officers under the WSES was replaced by SSCs with an outer period of 14 years. The first batch of women officers under the new scheme entered the Army in 2008

2003 and 2006: Writ petitions filed in the Delhi High Court by advocate Babita Puniya and several SSC women Army officers for permanent commission and equality of opportunity in the Army

March 2010: Delhi HC holds that women SSC officers of the Air Force and Army who had opted for PC, but not granted that status would be entitled to PC at par with male SSC officers with all consequential benefits. Contempt proceedings were then initiated by the women officers against the Union of India for non-compliance with the HC judgment. Contempt was later stayed

September 2, 2011: The case reaches the Supreme Court in appeal

Women in the Indian Defence Forces

Year wise induction details of women officers in the three armed forces during the past three years and current year, given in a written reply is as follows:

	2017	2018	2019	2020
Indian Army	949	819	364	01
Indian Air Force	59	59	51	00
Indian Navy	57	38	54	18 (in progress)

% of women officers is more in Indian air force than army and navy.

SECURITY AGENCIES RED-FLAG FIRMS WITH CONNECTION TO CHINESE GOVT.

Why in news?

Faced with a belligerent People's Liberation Army (PLA) in East Ladakh, Indian security agencies have red-flagged the penetration of companies believed to have ties with the Chinese government in critical sectors, particularly telecommunications, higher education, and power supply and distribution.

Details

- It is understood that the recent senior-most bureaucrats of the critical ministries met on directions from the top leadership to understand the extent of this penetration.
- Senior officials of security agencies sensitized the officers on the issue, and the government has since issued verbal instructions to various departments to prevent this intrusion.

Concerns in Education

- In education, under the garb of cultural promotion, Indian universities and colleges have tied up with their Chinese counterparts through Memorandums of Understanding (MoUs), often without the requisite clearance of the designated authority — in this case, the Ministry of External Affairs or the Human Resource Development ministry.
- A classic example in this are the Chinese-government funded Confucius Institutes to promote Han Chinese language and culture — typicality set up in association with a local partner institution.

Concerns in Telecommunications

- Private sector companies have preferred cheaper Chinese infrastructure for mobile and internet telephony.
- There have been allegations that large tenders are sometimes designed to suit the Chinese companies.

Other Directions given

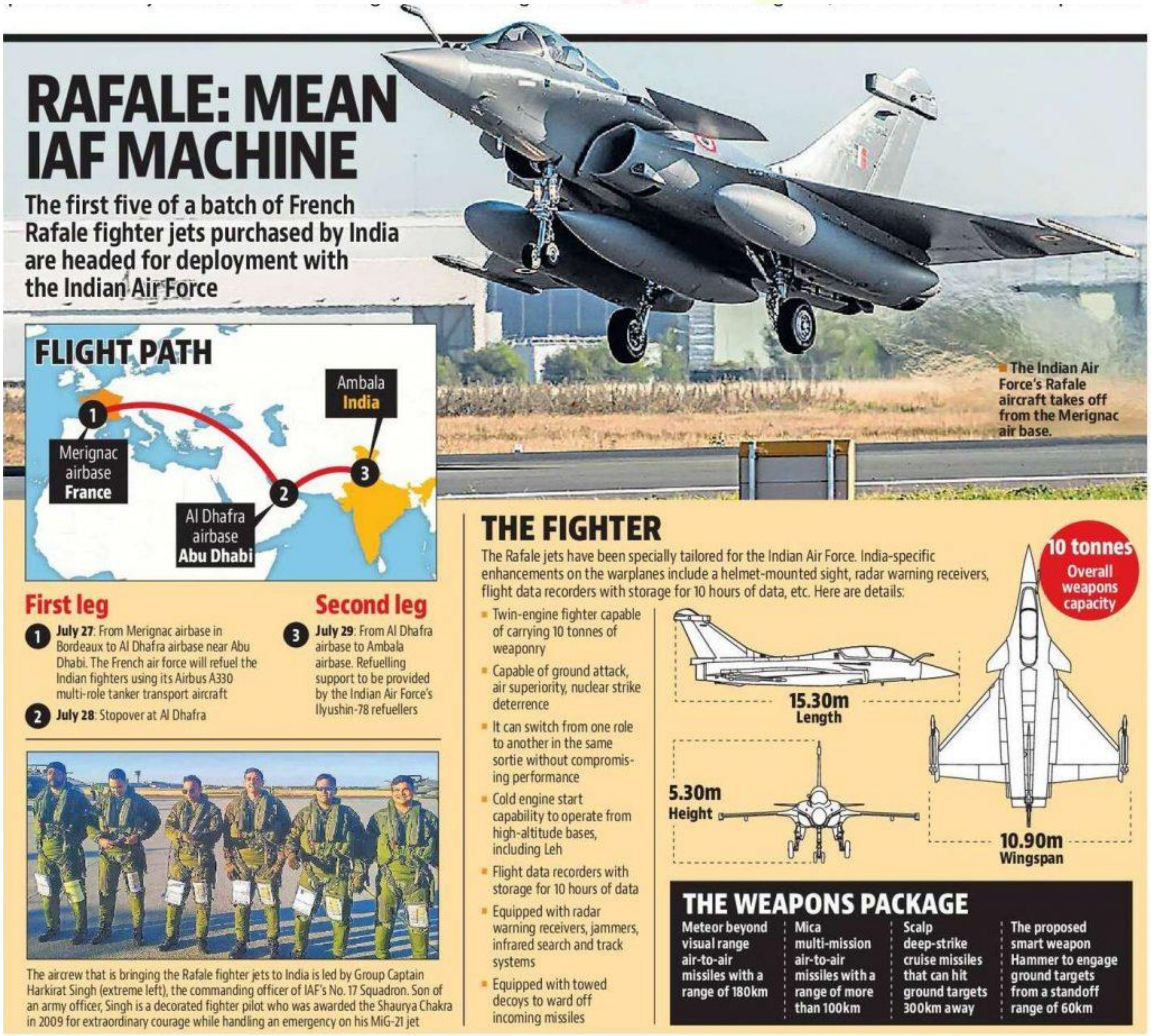
- The Department of Telecommunications asked BSNL to tweak its tender to exclude Chinese equipment makers from a large 4G upgrade project.
- The power ministry issued a detailed order where all equipment, components and parts imported for use in the power supply system and network will be tested in the country to check for any kind of embedded malware/trojans/cyber threat and adherence to Indian standards.

- The order states that power is a strategic and critical sector that supports not only India's national defence, vital emergency services and critical national infrastructure but also the entire economy and the day to day life.

5 RAFALES HEAD TO INDIA

Why in news?

Five Rafale fighter jets of the 36 ordered by the Indian Air Force (IAF) took off from France and are homebound to India.



RAFALE: MEAN IAF MACHINE

The first five of a batch of French Rafale fighter jets purchased by India are headed for deployment with the Indian Air Force

The Indian Air Force's Rafale aircraft takes off from the Merignac air base.

FLIGHT PATH

First leg

1 **July 27**: From Merignac airbase in Bordeaux to Al Dhafra airbase near Abu Dhabi. The French air force will refuel the Indian fighters using its Airbus A330 multi-role tanker transport aircraft

2 **July 28**: Stopover at Al Dhafra

Second leg

3 **July 29**: From Al Dhafra airbase to Ambala airbase. Refuelling support to be provided by the Indian Air Force's Ilyushin-78 refuellers

The aircrew that is bringing the Rafale fighter jets to India is led by Group Captain Harkirat Singh (extreme left), the commanding officer of IAF's No. 17 Squadron. Son of an army officer, Singh is a decorated fighter pilot who was awarded the Shaurya Chakra in 2009 for extraordinary courage while handling an emergency on his MiG-21 jet

THE FIGHTER

The Rafale jets have been specially tailored for the Indian Air Force. India-specific enhancements on the warplanes include a helmet-mounted sight, radar warning receivers, flight data recorders with storage for 10 hours of data, etc. Here are details:

- Twin-engine fighter capable of carrying 10 tonnes of weaponry
- Capable of ground attack, air superiority, nuclear strike deterrence
- It can switch from one role to another in the same sortie without compromising performance
- Cold engine start capability to operate from high-altitude bases, including Leh
- Flight data recorders with storage for 10 hours of data
- Equipped with radar warning receivers, jammers, infrared search and track systems
- Equipped with towed decoys to ward off incoming missiles

THE WEAPONS PACKAGE

Meteor beyond visual range air-to-air missiles with a range of 180km	Mica multi-mission air-to-air missiles with a range of more than 100km	Scalp deep-strike cruise missiles that can hit ground targets 300km away	The proposed smart weapon Hammer to engage ground targets from a standoff range of 60km

Benefits

- This move of inducting Rafales to the IAF will boost rapid deployment of the jets to upgrade India's ageing air power amid tensions with neighbouring China and Pakistan.
- This also marks a new milestone in the strong and growing India-France defence cooperation.

- The new fighters — the first imported jets to be inducted into the IAF in 23 years after the Russian Sukhoi-30 jets entered service in June 1997 — will significantly enhance the offensive capabilities of IAF.
- The new fighters — the first imported jets to be inducted into the IAF in 23 years after the Russian Sukhoi-30 jets entered service in June 1997 — will significantly enhance the offensive capabilities of IAF
- The twin-engine jet is capable of carrying out a variety of missions – ground and sea attack, air defence and air superiority, reconnaissance and nuclear strike deterrence

INDIAN NAVY DEEPENS WATCH TO CHECK CHINA AMBITIONS

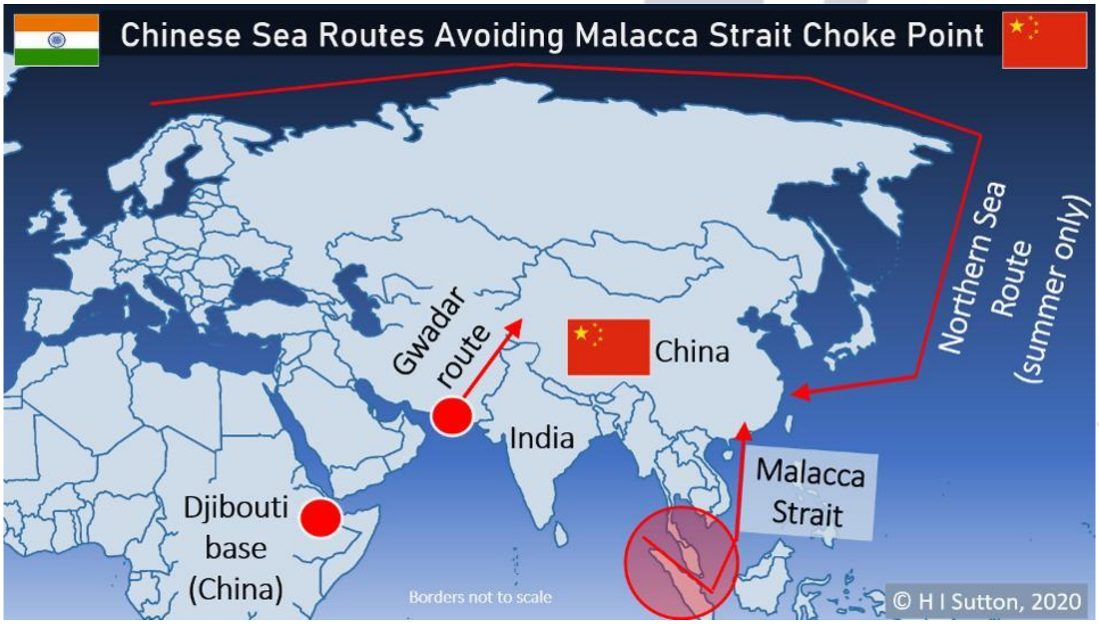
Why in news?

The Indian Navy has stepped up surveillance and activities in the Indian Ocean Region (IOR), which, it believes, China will “inevitably” try to enter in its quest to become a global power, just as it has laid claim to large portions of the disputed South China Sea.

Details and developments

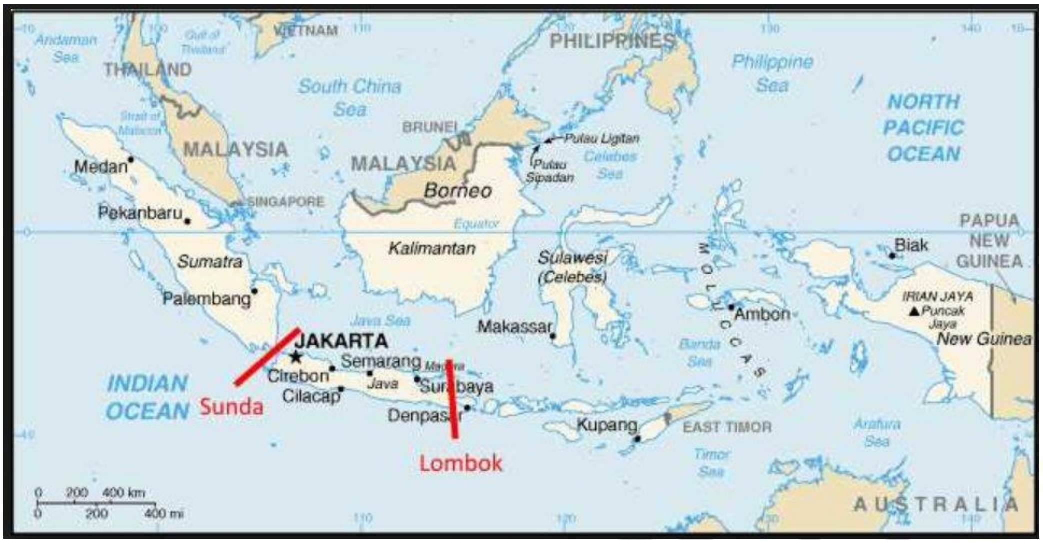
- It is to deal with this scenario of China trying to enter IOR that India reached out to neighbours in IOR — Maldives, Mauritius, Seychelles and Madagascar, to prevent China from expanding its footprint in the region by creating more bases — and like-minded navies, such as those of the United States and Japan
- Chinese are opening multiple routes to the Indian Ocean to overcome the Malacca Dilemma (China’s strategic weakness).

Malacca Dilemma



- The Malacca Dilemma refers to China’s apprehension of major naval powers controlling the Malacca Strait between Malaysia and Indonesia and interdicting vital supply lines.
- A significant volume (more than 80%) of China’s oil imports pass through the strait connecting the Indian Ocean and the South China Sea.

The multiple routes that China could be looking at to enter the Indian Ocean are further south of Malacca and include the Sunda, Lombok, Ombai and Wetar straits.



Recently in news:

- The Indian navy has conducted joint drills with a US Navy carrier strike group, led by USS Nimitz, and Indian and Japanese warships have carried out exercises in the Indian Ocean, against the backdrop of the India-China border standoff in Ladakh.
- The stage is also set for Australia to be part of the next Malabar naval exercise conducted by India with the US and Japan.
- From carrying out naval drills with like-minded countries to reaching out to states in the Indian Ocean region, the Indian Navy is focusing on checking China's rising ambitions in the region and sending out a strong message that Beijing's power play in South China Sea cannot be replicated in the Indian Ocean.
- China's step-by-step inroads into "territorialising" the South China Sea find echoes in some parts of IOR, not by trumped up claims because that would be blatant neo-colonialism but with more sophistication.
- Indian warships are deployed from as far as the Persian Gulf to the Malacca strait and northern Bay of Bengal to the southeast coast of Africa.

DEFENCE PRODUCTION AND EXPORT PROMOTION POLICY 2020

Why in news?

Ministry of Defence (MoD) has formulated a draft Defence Production and Export Promotion Policy 2020 (DPEPP 2020).

Defence Production and Export Promotion Policy 2020 (DPEPP 2020)

The DPEPP 2020 is envisaged as overarching guiding document of MoD to provide a focused, structured and significant thrust to defence production capabilities of the country for self-reliance and exports.

Regarding Domestic Production and Defence Exports

- The share of domestic procurement in overall defence procurement is about 60% now, and in order to enhance procurement from domestic industry, it is incumbent that procurement is doubled to RS. 1.4 Lakh crores by 2025 – according to DPEPP 2020's aims.
- The policy says that Defence Attachés have been mandated and are supported to promote export of indigenous defence equipment abroad, with the efforts in this direction supplemented by selected Defence Public Sector Undertakings (DPSU).
- Subject to strategic considerations, domestically manufactured defence products will also be promoted through Government to Government agreements and Lines of Credit/Funding.
- In addition, with the aim to move away from licensed production to design, develop and produce indigenously and own the design rights and Intellectual Property (IP) of the systems projected in Long Term Integrated Perspective Plan (LTIPP) of the Services a Technology Assessment Cell (TAC) would be created.

Aims / Objectives of the DPEPP 2020 Policy

- To achieve a turnover of Rs 1.75 Lakh Crores, including export of Rs 35 Thousand Crores in Aerospace and Defence goods and services by 2025.
- To develop a dynamic, robust and competitive Defence industry, including Aerospace and Naval Shipbuilding industry to cater to the needs of Armed forces with quality products.
- To reduce dependence on imports and take forward "Make in India" initiatives through domestic design and development.
- To promote export of defence products and become part of the global defence value chains.
- To create an environment that encourages R&D, rewards innovation, creates Indian IP ownership and promotes a robust and self-reliant defence industry.

In Aerospace

The policy has identified the opportunities in the aerospace industry in the following segments:

1. Aircraft build work,
2. Aircraft Maintenance,
3. Repair and Overhaul (MRO),
4. Helicopters, engine manufacturing and MRO work,
5. Line replaceable units,
6. Unmanned Aerial Vehicles and upgrades and retrofits.

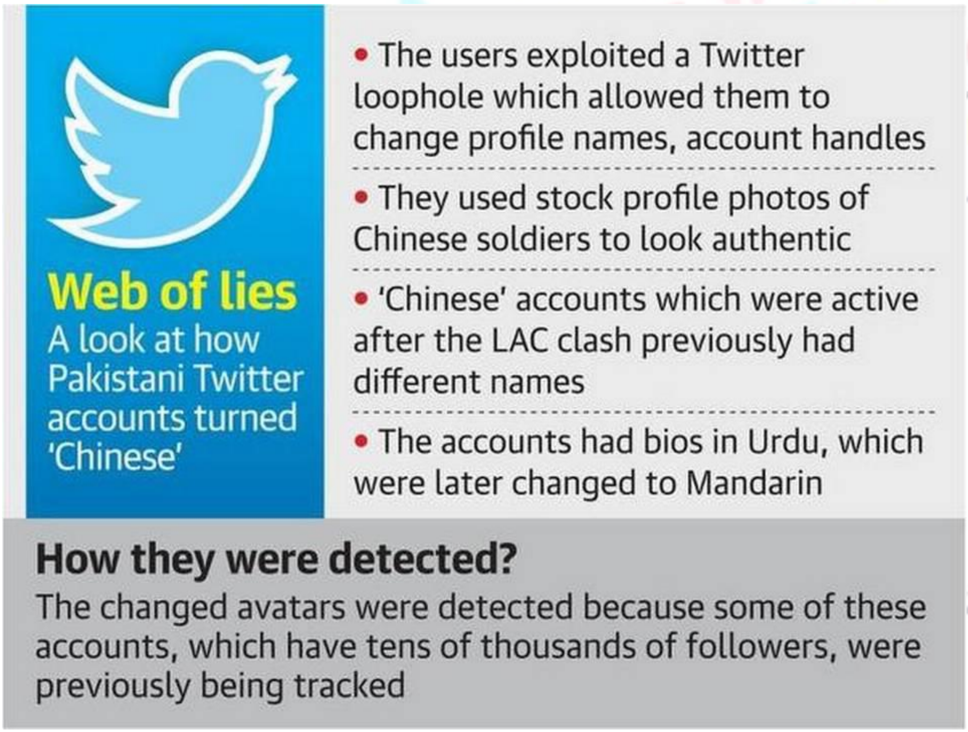
PAKISTANIS BEHIND 'CHINESE' INFO WAR

Why in news?

Many of the 'Chinese' accounts that appeared on social media and spread false information about the border clash with India have been traced to Pakistan, in what is believed to be a coordinated disinformation campaign aimed at India.

Details

- The recent India-China border tensions sparked a first-of-its-kind information war on social media, where Indian and Chinese accounts on Twitter, Facebook and YouTube traded images and videos in an effort to both capture the narrative and the attention of the media.
- Many of the 'Chinese' social media accounts that posed as China-based users were actually Pakistani accounts.
- It is also useful to note that Twitter is banned in China, although it can be accessed using virtual private networks.
- These accounts have used a loophole on Twitter that allows users to not only change their profile names, but their Twitter handles as well.
- These accounts have shared false information about casualties from the clash, unrelated images of injured soldiers, and videos of troops' confrontations that were from previous border incidents.
- This strategy has not been limited to adopting Chinese identities. Pakistani accounts have also recently adopted Nepali and Sri Lankan avatars, all with the same motivation: posting information aimed at creating an unfavourable narrative about India.



Web of lies

A look at how Pakistani Twitter accounts turned 'Chinese'

- The users exploited a Twitter loophole which allowed them to change profile names, account handles
- They used stock profile photos of Chinese soldiers to look authentic
- 'Chinese' accounts which were active after the LAC clash previously had different names
- The accounts had bios in Urdu, which were later changed to Mandarin

How they were detected?

The changed avatars were detected because some of these accounts, which have tens of thousands of followers, were previously being tracked

What is Fake News?

- Fake news is news, stories or hoaxes created to deliberately misinform or deceive readers.
- Usually, these stories are created to either influence people's views, push a political agenda or cause confusion and can often be a profitable business for online publishers.
- Combating fake news is a growing narrative of the technology platforms like Facebook, Google, the news media, the government and an informed citizenry.
- **Fake news affects free speech and informed choices of the subjects of the country, leading to the hijacking of democracy.**
- The advent of social media has decentralized the creation and propagation of fake news.

How to deal with fake news?

The current response to fake news primarily revolves around three prongs — rebuttal, removal of the fake news item and educating the public.

- **Rebuttal**: It is a form of fact-checking wherein the fake news is debunked by pointing out errors like mismatch, malicious editing and misattribution.
- **Removal of Fake news**: Technical companies like Facebook and YouTube uses algorithms to proactively remove fake news from their platforms.
- It is impossible to completely 'remove' fake news even after rebuttal, given the decentralised nature of dissemination.
- It may be possible to rebut fake news but the 'fake news factory' inspired by political agenda, will keep churning out similar stories to advance its chosen narrative.

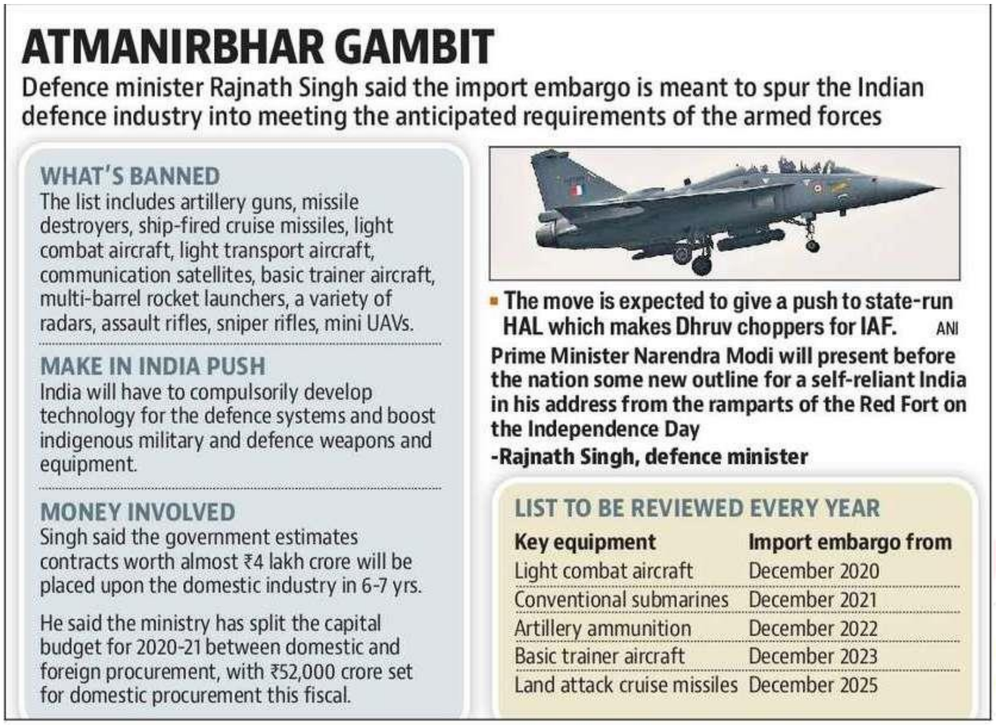
DEFENCE MINISTRY TO IMPOSE IMPORT EMBARGO

Why in news?

The Defence Ministry will "introduce import embargo on 101 items beyond given timeline to boost indigenisation of defence production".

Details

- The Ministry of Defence has prepared a list of 101 items for which there would be an embargo on the import beyond the timeline indicated against them.
- The government intends to reach a turnover of $25 billion through indigenously manufactured defence products and also expects to export products worth $5 billion.
- Government has also decided that in any government contract over ₹200 crore, no foreign company can participate in the tendering process, to help Indian Manufacturers.
- The embargo on imports is planned to be progressively implemented between 2020 to 2024.
- The aim is to apprise the Indian defence industry about the anticipated requirements of the Armed Forces so that they are better prepared to realise the goal of indigenisation.



ATMANIRBHAR GAMBIT

Defence minister Rajnath Singh said the import embargo is meant to spur the Indian defence industry into meeting the anticipated requirements of the armed forces

WHAT'S BANNED
The list includes artillery guns, missile destroyers, ship-fired cruise missiles, light combat aircraft, light transport aircraft, communication satellites, basic trainer aircraft, multi-barrel rocket launchers, a variety of radars, assault rifles, sniper rifles, mini UAVs.

MAKE IN INDIA PUSH
India will have to compulsorily develop technology for the defence systems and boost indigenous military and defence weapons and equipment.

MONEY INVOLVED
Singh said the government estimates contracts worth almost ₹4 lakh crore will be placed upon the domestic industry in 6-7 yrs.

He said the ministry has split the capital budget for 2020-21 between domestic and foreign procurement, with ₹52,000 crore set for domestic procurement this fiscal.

▪ The move is expected to give a push to state-run HAL which makes Dhruv choppers for IAF. ANI

Prime Minister Narendra Modi will present before the nation some new outline for a self-reliant India in his address from the ramparts of the Red Fort on the Independence Day
-Rajnath Singh, defence minister

LIST TO BE REVIEWED EVERY YEAR

Key equipment	Import embargo from
Light combat aircraft	December 2020
Conventional submarines	December 2021
Artillery ammunition	December 2022
Basic trainer aircraft	December 2023
Land attack cruise missiles	December 2025

GOVT. PLANS CYBER SECURITY SYSTEM FOR FINANCIAL SECTOR

Why in news?

The government is in the process of setting up a system to secure the country's financial sector from cyber-attacks after agencies pointed to its vulnerability due to the increase in number of digital transactions over the past few months on account of Covid-19, and threats from hostile countries such as China and Pakistan.

Present scenario

- At present, the Indian Computer Emergency Response Team (CERT-In) deals with all types of cyber security threats but officials in the administration have been discussing the need for a specialised agency, which could be called Cert-Fin, the officials said, asking not to be identified.
- Several rounds of discussions have been held at the Financial Stability and Development Council (FSDC) on the matter of securing the financial sector from cyber-attacks.
- CERT-In functions under the ministry of electronics and information technology (MeitY).

Financial Stability and Development Council (FSDC)

- FSDC is an apex body for coordination between the various regulators of the financial sector, and is chaired by the finance minister.
- Its members include top bureaucrats and heads of financial sector regulators such as the Reserve Bank of India (RBI), the Securities and Exchange Board of India (Sebi), the Pension Fund Regulatory and Development Authority of India (PFRDA), the Insurance Regulatory and Development Authority (IRDA) and the Forward Markets Commission (FMC).

Critical issues

- Banking and ATM networks have been the target of cyber criminals for several years, with attackers often disrupting operations and attempting to steal sensitive data.
- In one of the biggest attacks of this kind, the data of 3.2 million debit cards used in India was stolen after a malware was injected in a back-end banking system in 2016.
- RBI's latest Financial Stability Report also flagged the issue of cyber threats to the financial sector.
- A report said that hackers from various countries attempted over 40,000 cyber-attacks on India's Information Technology infrastructure and banking sector over five days in the last week of June.
- Cyber-attacks against banks and financial institutions globally have increased 238% amid the Covid-19 crisis (lockdown period) and Ransomware attacks increased by nine times during the same period.

DRDO IDENTIFIES 108 SUBSYSTEMS FOR PRIVATE SECTOR

Why in news?

Defence Research and Development Organisation (DRDO) provided a list of 108 systems and sub-systems to Defence Minister which have been identified for indigenous development only.

Details

- DRDO will also provide its support to industries in this development process.
- This will pave the way for Indian Defence industry to develop many technologies towards building an AtmaNirbhar Bharat.
- The systems and sub-systems in the list of 108 items include mini and micro UAVs, ROVs, uncooled NV-IR sights for weapons (short-range), mountain footbridge, floating bridge (both metallic), mines laying and marking equipment.

Recently in news

Recently Light Combat Aircraft (LCA) MK I A, Land-Attack Cruise Missiles (Long-Range),155 mm Artillery Ammunition were put among the list of the 101 items that have been put under an import embargo by the Ministry of Defence.

INDIA, RUSSIA TO HOLD NAVAL DRILLS IN ANDAMAN SEA

Why in news?

Amid high operational alert by the Indian Navy in the Indian Ocean Region (IOR) due to the ongoing standoff with China in Ladakh, India and Russia are scheduled to hold the bilateral naval exercise, Indra 2020, in the Andaman Sea, close to the strategic Strait of Malacca.

Details

- This is the first bilateral naval exercise since all such engagements were suspended due to COVID-19.
- The timing of the exercise coincides with Indian Defence Minister's visit to Russia for the Shanghai Cooperation organisation (SCO) defence ministers meet and also comes just after India withdrew from the Kavkaz-2020 multinational exercise in Russia.

- While the stated reason for the withdrawal was the COVID-19 pandemic, defence sources had said that it due to the participation of Chinese troops.

Exercise "Indra"

- It is a joint, tri-services exercise between India and Russia
- This series of exercise began in 2003 and the First joint Tri-Services Exercise was conducted in 2017.
- Company sized mechanized contingents, fighter and transport aircraft, as well as ships of respective Army, Air Force and Navy, participate in this exercise of ten days duration.

Recently in news: Exercise with USS Nimitz

- In July, frontline warships of the Indian Navy conducted a Passage Exercise (PASSEX) with the U.S. aircraft carrier with USS Nimitz strike group in the same area near the Andaman and Nicobar (A&N) islands as it was transiting the Indian Ocean.
- The USS Nimitz was returning from the South China Sea through the Malacca Strait where it undertook freedom of navigation operations.
- With ongoing tensions, Indian Navy is keeping a close watch on movement in the IOR of Chinese Naval ships whose presence has gone up considerably over the years in the name of Anti-Piracy patrols.

Recently in news: Major Infrastructure plans in Andaman and Nicobar

- In 2017, China opened its first overseas military base in Djibouti in the Horn of Africa.
- Given their strategic location, India has embarked on a major infrastructure expansion plan on the A&N island chain.

DEFENCE EXPORTS INCREASED 700% IN 3 YEARS

Why in news?

- In the last three years, the country witnessed a "staggering" 700% growth in defence exports which is an all-time high and 19th in the list of defence exporters in 2019, according to Chief of Defence Staff (CDS).
- India is the third largest spender on defence around the world – the only net importer in the category and account for 9.2% of global arms imports.

Details on what was done

- With the aim to achieve a manufacturing turnover of $25 bn including exports of $5 bn in aerospace and defence goods and services by 2025, the Defence Ministry issued a draft 'Defence Production & Export Promotion Policy (DPEPP) 2020'.
- A series of measures had been taken since 2014 to boost exports, including simplified defence industrial licensing, relaxation of export control and grant of No Objection Certificates (NOC).
- Specific incentives were introduced under the foreign trade policy. The Ministry of External Affairs (MEA) has facilitated a Line of Credit for foreign countries to import defence products.
- Defence Attaches in Indian missions were empowered to promote defence exports which would also strengthen defence diplomacy.

Way Forward suggested by the CDS

- We must move out of the constant threat of sanctions of dependency on individual nations for military requirements.
- We must carry out a realistic analysis and have a hard look at the distribution of our budget expenditure.
- Where feasible, defence exports can also be financed through the Exim Bank.

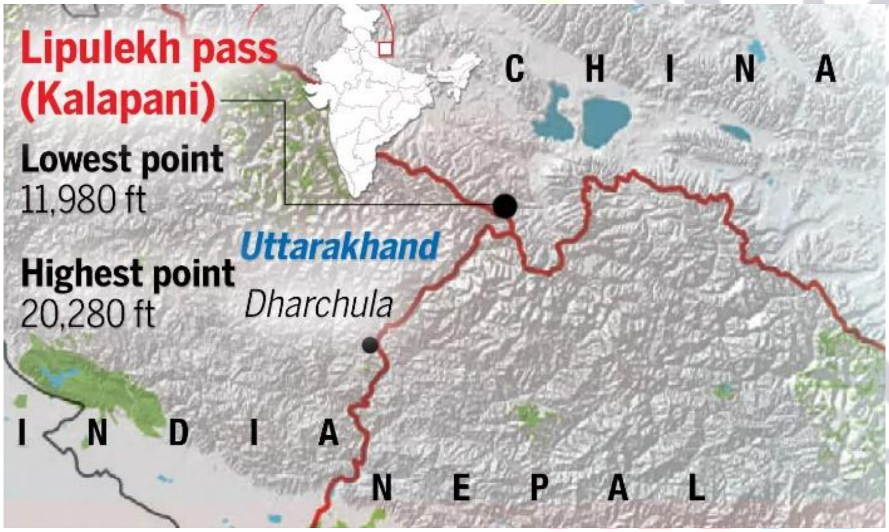
UTTARAKHAND IS UPGRADING DEFENCE

Introduction

In the context of ongoing tensions and territory issues with China and Nepal, the Uttarakhand government, along with the defence forces, has taken measures to strengthen infrastructure along its international border.

Why Uttarakhand matters?

- Uttarakhand shares a 350-km border with China and a 275-km boundary with Nepal. Five of the state's 13 districts are border districts.
- Pithoragarh is strategically very sensitive as it has boundaries with both China and Nepal.



Radar and tactical airfields

- In the recent development, the Uttarakhand government has agreed to provide land to the Indian Air Force (IAF) to set up air defence radars in three districts bordering China – Chamoli, Pithoragarh, and Uttarkashi.
- The IAF has also proposed to develop a new Advanced Landing Ground to facilitate its activities in the hill areas.

Filling gaps in telecom infra

- The Uttarakhand cabinet has approved an amendment in the state's information technology (IT) policy to provide incentives to facilitate private telecom companies to install towers in "dark villages" in which telecommunication facilities are unavailable at present.
- More than 400 "dark villages" have been identified in Uttarakhand, where no telecom service provider (TSP) or Internet service provider (ISP) extends services. These villages are mostly located along the state's border of China and Nepal, government sources said.

- Also, villagers in border areas have traditionally acted as the eyes and ears of the defence forces, and telecommunications are a force multiplier in this regard.

EIGHTEEN MORE INDIVIDUALS DECLARED AS TERRORISTS UNDER THE UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967.

Why in News?

Under the strong and iron-willed leadership of the Prime Minister, Shri Narendra Modi, the Central Government had amended the Unlawful Activities (Prevention) Act, 1967 in August 2019, to include the provision of designating an individual as a terrorist. Prior to this amendment, only organizations could be designated as terrorist organizations.

The Union Home Minister, Shri Amit Shah has unequivocally reaffirmed the nation's resolve to fight terrorism. By invoking the said amended provision, the Central Government designated four individuals in September, 2019 and nine individuals in July, 2020 as terrorists.

About The Unlawful Activities (Prevention) Act, 1967;-

The UAPA, an upgrade on the Terrorist and Disruptive Activities (Prevention) Act TADA (lapsed in 1995) and the Prevention of Terrorism Act – POTA (repealed in 2004) was originally passed in the year 1967.

Till the year 2004, "unlawful" activities referred to actions related to secession and cession of territory. Following the 2004 amendment, **"terrorist act" was added** to the list of offences.

The Act assigns absolute power to the central government, by way of which if the Centre deems an activity as unlawful then it may, by way of an Official Gazette, declare it so.

Unlawful Activities
(prevention) Act
UAPA

About The Unlawful Activities (Prevention) Amendment Bill 2019;-

The Unlawful Activities (Prevention) Amendment Bill, 2019 was introduced in Lok Sabha by the Minister of Home Affairs, Mr. Amit Shah, on July 8, 2019. The Bill amends the Unlawful Activities (Prevention) Act, 1967.

The Act provides special procedures to deal with terrorist activities, among other things.

Who may commit terrorism:-

Under the Act, the central government may designate an organization as a terrorist organization if it:

(i) commits or participates in acts of terrorism,

(ii) prepares for terrorism,

(iii) promotes terrorism, or

(iv) is otherwise involved in terrorism.

The Bill additionally empowers the government to designate individuals as terrorists on the same grounds.

Approval for seizure of property by NIA:-

Under the Act, an investigating officer is required to obtain the prior approval of the Director General of Police to seize properties that may be connected with terrorism.

The Bill adds that if the investigation is conducted by an officer of the National Investigation Agency (NIA), the approval of the Director General of NIA would be required for seizure of such property.

Investigation by NIA:-

Under the Act, investigation of cases may be conducted by officers of the rank of Deputy Superintendent or Assistant Commissioner of Police or above.

The Bill additionally empowers the officers of the NIA, of the rank of Inspector or above, to investigate cases.

Insertion to schedule of treaties:-

The Act defines terrorist acts to include acts committed within the scope of any of the treaties listed in a schedule to the Act.

The Schedule lists nine treaties, including the Convention for the Suppression of Terrorist Bombings (1997), and the Convention against Taking of Hostages (1979). The Bill adds another treaty to the list. This is the International Convention for Suppression of Acts of Nuclear Terrorism (2005).

COUNTERING DEEPFAKES, THE MOST SERIOUS AI THREAT

Context: The debate around "deepfakes" has been rekindled recently with the popularity of applications such as FaceApp (for photo-editing) and DeepNude (that produces fake nudes of women).

Relevance:

GS Paper 3: Basics of Cyber Security; Role of media and social-networking sites in internal security challenges; Internal security challenges through communication networks

Mains questions:

1. It is crucial to enhance media literacy, meaningful regulations and platform policies, and amplify authoritative sources. Discuss the statement in context of Deepfake. 15 marks
2. Disinformation and hoaxes have evolved from mere annoyance to high stake warfare for creating social discord, increasing polarisation, and in some cases, influencing an election outcome. Elaborate. 15 marks

Dimensions of the Article:

- What is Deepfakes?
- What are the threats related to Deepfakes?
- Measures to address the challenges related to Deepfakes
- Way forward

What is Deepfakes?

Deepfake is a portmanteau of **"deep learning" and "fake"**. It is **an Artificial Intelligence (AI) software** that superimposes a digital composite on to an existing video (or audio).The origin of the word "deepfake" can be traced back to 2017 when a Reddit user, with the username "deepfakes", posted explicit videos of celebrities.

Deepfakes are **the digital media (video, audio, and images) manipulated using Artificial Intelligence.** This synthetic media content is referred to as deepfakes.

What are the threats related to deepfakes?

A cyber Frankenstein: Frankenstein is **not a computer virus**, which is a program that can multiply and take over other machines. But, it could be **used in cyberwarfare** to provide cover for a virus or another type of malware, or malicious software. Therefore it has multiple challenges:

- **Deepfakes, hyper-realistic digital falsification**, can inflict damage to individuals, institutions, businesses and democracy. They make it possible to fabricate media — swap faces, lip-syncing, and puppeteer — mostly without consent and bring threat to **psychology, security, political stability, and business disruption.**
- **Nation-state actors** with **geopolitical aspirations, ideological believers, violent extremists, and economically motivated enterprise**s can manipulate media narratives using deepfakes, with easy and unprecedented reach and scale.

Targeting women:

- The very first use case of malicious use of a deepfake was seen in pornography**, inflicting emotional, reputational,** and in some cases, violence towards the individual.
- **Pornographic deepfakes** can threaten, intimidate, and inflict psychological harm and reduce women to sexual objects. Deepfake pornography exclusively targets women.

Damaging individual dignity:

- Deepfakes can depict a person indulging in **antisocial behaviour**s and saying vile things. These can have severe implications on their **reputation, sabotaging their professional and personal life.**
- **Malicious actors** can take advantage of unwitting individuals to defraud them for financial gains using audio and video deepfakes.
- Deepfakes can be deployed to **extract money, confidential information**, or exact favours from individuals.

Harming social fabric of society:

- **Deepfakes can cause short- and long-term social harm** and accelerate the already declining trust in news media. Such an erosion can contribute to a culture of **factual relativism, fraying the increasingly strained civil society fabric.**
- **The distrust in social institutions** is perpetuated by the democratising nature of information dissemination and social media platforms' financial incentives.
- **Falsity is profitable**, and goes viral more than the truth on social platforms. Combined with distrust, the existing biases and political disagreement can help create echo chambers and filter bubbles, creating discord in society.

Challenge to internal security:

- Imagine a deepfake of **a community leader denigrating a religious site of another community.** It will cause riots and, along with property damage, may also cause life and livelihood losses.
- A deepfake could act as a powerful tool by a nation-state to **undermine public safety** and create uncertainty and chaos in the target country.
- It can be used by **insurgent groups and terrorist organisations**, to represent their adversaries as making inflammatory speeches or engaging in provocative actions to stir up anti-state sentiments among people.

Undermining democracy:

- A deepfake can also aid in **altering the democratic discourse and undermine trust in institutions and impair diplomacy**. False information about **institutions, public policy, and politicians** powered by a deepfake can be exploited to spin the story and manipulate belief.
- **A deepfake of a political candidate** can sabotage their image and reputation. A well-executed one, a few days before polling, of a political candidate spewing out racial epithets or indulging in an unethical act can damage their campaign.
- **A high-quality deepfake** can inject compelling false information that can cast a shadow of illegitimacy over the voting process and election results.
- **Deepfakes contribute to factual relativism** and enable authoritarian leaders to thrive. For authoritarian regimes, it is a tool that can be used to justify oppression and disenfranchise citizens. Leaders can also use them to increase populism and consolidate power.

- Deepfakes can become a very effective tool to sow the seeds of **polarisation, amplifying division in society, and suppressing dissent.**

Measures to address the threats related to deepfakes:

Collaborative actions and collective techniques across **legislative regulations, platform policies, technology intervention, and media literacy** can provide effective and ethical countermeasures to mitigate the threat of malicious deepfakes.

Media literacy:

- Media literacy for consumers and journalists is the most effective tool to combat disinformation and deepfakes.
- Media literacy efforts must be enhanced to cultivate a discerning public. As consumers of media, we must have the ability to decipher, understand, translate, and use the information we encounter.
- Even a short intervention with media understanding, learning the motivations and context, can lessen the damage. Improving media literacy is a precursor to addressing the challenges presented by deepfakes

Legislative regulations:

- Meaningful regulations with a collaborative discussion with the technology industry, civil society, and policymakers can facilitate disincentivising the creation and distribution of malicious deepfakes.

Technological solutions:

- We also need easy-to-use and accessible technology solutions to detect deepfakes, authenticate media, and amplify authoritative sources.

Way forward:

Deepfakes can create possibilities for all people irrespective of their limitations by augmenting their agency. However, as **access to synthetic media technology** increases, so does the risk of exploitation. Deepfakes can be used **to damage reputations, fabricate evidence, defraud the public, and undermine trust in democratic institutions**. To counter the menace of deepfakes, we all must take the responsibility to be a critical consumer of media on the Internet, think and pause before we share on social media, and be part of the solution to this infodemic.

Background:

1: Types of cybercrime:

- **Cyber Warfare:** states attacking the information systems of other countries for espionage and for disrupting their critical infrastructure.
- **Phishing:** It is a kind of fraudulent attempt that is made through email, to capture personal and financial information.
- **Cyber Stalking**: repeated use of electronic communications to harass or frighten someone
- **Identity theft**: It is a type of fraud in which a person pretends to be someone else and does crime with the name of someone else

- **Denial of service (DoS)**: It attacks refers an attempt to make computer, server or network resources unavailable to its authorized users usually by using temporarily interruption or suspension of services.

MHA TELLS STATES TO REGISTER MORE FIRS FOR CYBERCRIME

Why in news?

The Ministry of Home Affairs (MHA) has written to all States to examine and register FIRs based on the complaints received on National Cybercrime Reporting Portal.

Details

- As per data available with the Ministry, only 2.5% of total complaints registered on the portal are converted into First Information Reports (FIRs).
- Through the portal, MHA also aims to raise a group of "cybercrime volunteers" to flag "unlawful content" on the Internet.
- The unlawful content is categorised as content against the sovereignty and integrity of India, against defence of India, against security of the State, against friendly relations with foreign States, content aimed at disturbing public order, disturbing communal harmony and child sex abuse material.

Low conversion

- Since its launch last year, the portal has received over 2 lakh complaints, but FIRs have been registered only in 5,000 cases.
- A senior government official said that on an average around 1,000 cybercrimes complaints from across the country are received. The rate of conversion of complaints to FIRs is very low.
- According to data compiled by the National Crime Records Bureau (NCRB), the number of registered cybercrimes increased by 63.5% in the year 2019 compared to the previous year.
- A total of 44,546 cases were registered under cybercrimes compared to 27,248 cases in 2018.
- In 2019, 60.4% of cybercrime cases registered were for the motive of fraud followed by sexual exploitation with 5.1% and causing disrepute with 4.2%.
- On receiving the complaint, the designated Police Officer after verifying the matter will report to concerned bank and financial intermediary or payment wallet, etc., for blocking the money involved in the cyber fraud.

THE FORGOTTEN FACT OF CHINA-OCCUPIED KASHMIR

Context:

On November 1, observed every year in Gilgit-Baltistan as "Independence Day", Pakistan Prime Minister Imran Khan announced that his government would give the region "provisional provincial status".

Relevance:

GS Paper 3: Border Areas (security challenges and management thereof); Security forces & agencies (mandate); Role of External State & Non-State actors in creating internal security challenges

Mains Questions

1. Cross-border movement of insurgents is only one of the several security challenges facing the policing of the border in North-West India. Examine the various challenges currently emanating across the India-Pakistan border. Also, discuss the steps to counter the challenges. 15 marks
2. The china Pakistan Economic Corridor passes through the Gilgit Baltistan region which undermines India's territorial claim over Gilgit Baltistan region and PoK. Elaborate. 15 marks

Dimensions of the article

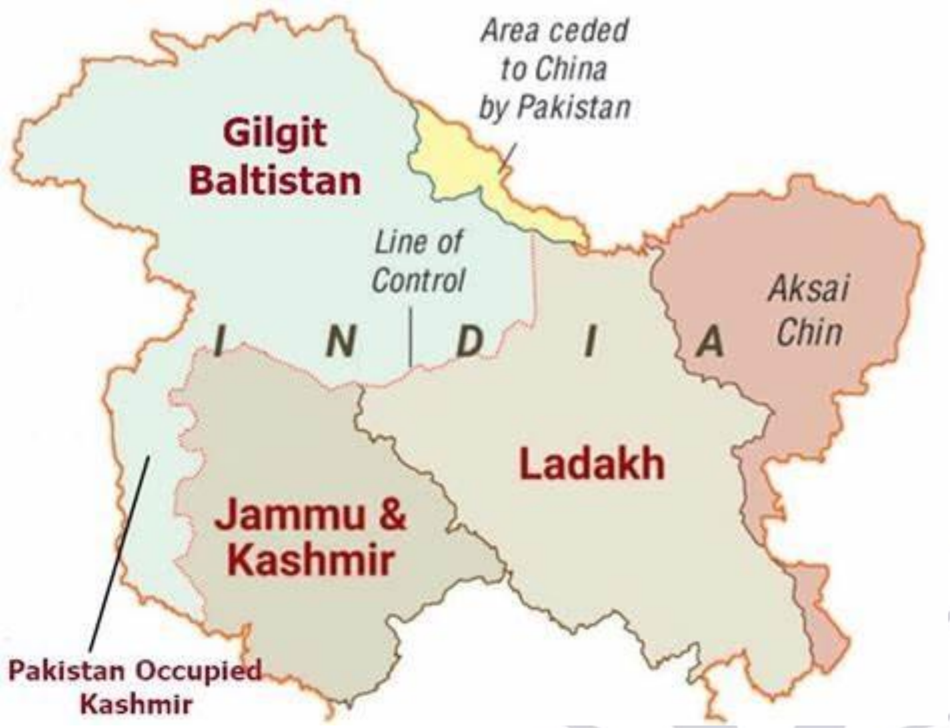
- Geographical location of Gilgit-Baltistan region.
- Historical background of Gilgit-Baltistan region.
- Strategic importance of Gilgit-Baltistan
- Challenges along the border with china and Pakistan
- India's initiatives to improve border management
- Way forward

Geographical location of Gilgit-Baltistan Region

Gilgit-Baltistan borders **Pakistan's Khyber Pakhtunkhwa** province to the west, a small portion of **the Wakhan Corridor of Afghanistan** to the north, **China's Xinjiang Uyghur Autonomous Region** to the northeast, the **Indian-administered Jammu and Kashmir** to the southeast, and the Pakistani-administered state of Azad Jammu and Kashmir to the south.

The region is home to some of **the world's highest mountain ranges**. The main ranges are the **Karakoram** and the western Himalayas. **The Pamir Mountains** are to the north, and **the Hindu Kush** lies to the west. Amongst the highest mountains are **K2 (Mount Godwin-Austen)** and **Nanga Parbat**, the latter being one of the most feared mountains in the world.

Three of the **world's longest glaciers** outside the polar regions are found in Gilgit-Baltistan: the **Biafo Glacier**, **the Baltoro Glacier,** and **the Batura Glacier**.



Historical Background

The Soviet-British Great Game territory: The British wanted to protect their border from The Soviet's invasion so they took Gilgit as a leased from Hari Singh in 1935. The British returned it in August 1947.

On November 1 1947, after J&K ruler Hari Singh had signed **the Instrument of Accession** with India, and the Indian Army had landed in the Valley to drive out tribal invaders from Pakistan, there was a rebellion against Hari Singh in Gilgit.

Pakistan did not accept **Gilgit-Baltistan's accession** although it took administrative control of the territory. After India went to the UN and a series of resolutions were passed in **the Security Council** on the situation in Kashmir, Pakistan believed that neither **Gilgit-Baltistan nor PoK** should be annexed to Pakistan, as this could undermine the international case for a plebiscite in Kashmir.

Strategic importance of Gilgit-Baltistan

Gilgit-Baltistan is the northernmost territory administered by Pakistan, providing the country's only territorial frontier, and thus **a land route, with China**, where it meets **the Xinjiang Autonomous Region. The China Pakistan Economic Corridor** has made the region vital for both countries. In a recent analysis by **Andrew Small**, this ambitious project is seen to have been going slow for a combination of reasons. But given the strategic interests of both countries, CPEC will continue.

China occupies **5,180 square kilometres in the Shaksgam Valley** in addition to approximately **38,000 square kilometres in Aksai Chin.** China and Pakistan have colluded to obfuscate these facts, even as they brazenly promote the China-Pakistan Economic Corridor (CPEC) which runs through parts of **Indian territory under their respective occupation.**

Therefore, this region is strategically very important to India, moreover this region belongs to India as Instruments of accession.

Challenges along the border with china

- Border dispute at **Aksai Chin, Arunachal Pradesh, Doklam etc**. with sporadic aggression.
- **Large scale smuggling of Chinese electronic** and other consumer goods take place through these border points even after designated areas for border trade.
- **Inadequate infrastructure** due to difficult terrain. However, China has undertaken a large-scale effort to upgrade **air, roads and rail infrastructure,** as well as surveillance capabilities near to the border.
- **Multiple forces** along Indian border (for e.g.-ITBP, Assam rifles, Special frontier force) as opposed to single PLA commander on Chinese side.
- **Water-sharing issue as China** is building dams on its side reducing water flows on our side.

Challenges along the border with Pakistan

- **Border dispute** at Sir Creek and Kashmir.
- **River water sharing** issue at Indus river.
- **Infiltration and Cross-border terrorism** targeted to destabilise India. Recently BSF detected a fifth (since 2012) cross border tunnel in the forest area of Jammu.
- **Diverse terrain** including desert, marshes, snow-capped mountain and plains makes border guarding difficult. · Time & cost overruns in infrastructure projects due to unforeseen circumstances& natural calamities.
- Other issues include **drug smuggling, fake currency, arms trafficking.**

India's initiatives to improve border management

- **Creating infrastructure:** India is also constructing some critical bridges to cut down time for troop movement such as **Dhola-Sadiya bridge**.
- India has joined hands with Japan to aggressively develop **infrastructure projects** in North east to contain China.
- **Army infrastructure projects** within 100Km of LAC have been exempted from forest clearance.
- To expedite **border road construction, Ministry of Defence** has decided to delegate administrative and financial powers to the Border Roads Organisation (BRO)
- **MHA** sanctioned the implementation of **Comprehensive Integrated Border Management System (CIBMS)** to establish an integrated security system at borders providing all-round security even in adverse climatic conditions.
- The centre has decided to deploy **Indian special forces unit National Security Guard (NSG)** commandos in J&K to fortify counter terror operations by training J&K police and other paramilitary forces in room intervention, anti-terror skills, overseeing anti-hijack operations etc.

Way forward

- **Dispute resolution**– Government should resolve **pending border disputes** with the neighbouring countries, as they later become matters of national-security threat.
- **No diversion of security forces**– The border-guarding force should not be distracted from its principal task and deployed for other internal security duties. For e.g.-ITBP, a force specifically trained for India China border should not be used in the Naxalite-infested areas.

- **Involvement of army** – It is felt that the responsibility for unsettled and disputed borders, such as the LoC in J&K and the LAC on the Indo-Tibetan border, should be that of the Indian Army while the BSF should be responsible for all settled borders.
- **Follow one-force-one-border principle** to effectively manage borders as divided responsibilities never result in effective control.
- **Developing Infrastructure**-accelerated development of infrastructure along the border, especially to wean the border population from illegal activities.
- **Use of advanced technology** – The advances in surveillance technology, particularly satellite and aerial imagery, can help to maintain a constant vigil along the LAC and make it possible to reduce physical deployment.
- **Up-gradation of intelligence network** and co-ordination with sister agencies, conduct of special operations along the border.
- **Raising the issues of infiltration** from across the border during various meeting with counterpart countries.

MAOIST ATTACKS IN CHHATTISGARH'S SUKMA

Context:

A day after the encounter between central paramilitary forces and Maoists in Chhattisgarh's Sukma, bodies of 22 personnel were recovered, 31 were injured and one commando was still missing, according to Chattisgarh police.

Relevance:

GS-III: Internal Security Challenges (Linkages of Organized Crime with Terrorism, Left-Wing Extremism)

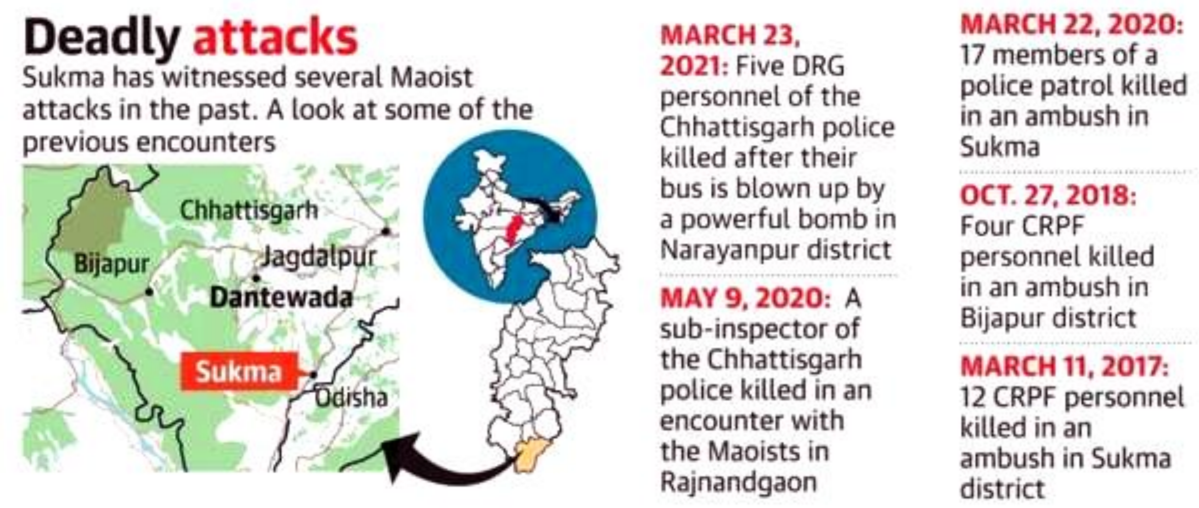
Dimensions of the Article:

1. Background to the recent attacks
2. Road Requirement Plan for Left Wing Extremism (LWE) Affected Areas
3. Left Wing Extremism (LWE)
4. What is Naxalism in India?
5. Government Initiatives to fight LWE

Background to the recent attacks

- With critical road projects to provide connectivity in Left Wing Extremism-affected areas often coming to a halt due to security reasons, Chhattisgarh has proposed a new plan to the Centre, suggesting that it divide the remaining contracts into small packets so that local contractors can take up the jobs.
- 90% of the Road Requirement Plan — for connectivity in hotspots of 34 districts worst-affected by Maoist insurgency in eight states — stands completed, but progress remains a problem in Chhattisgarh.
- A team of security forces was attacked by a People's Liberation Guerilla Army (PLGA) unit in the Tarrem area near the Sukma-Bijapur district border, Chhattisgarh. Several security personnel were killed and many were injured.
- PLGA was founded in 2000. It has been declared as a terrorist organisation and banned under the Unlawful Activities (Prevention) Act-1967 (UAPA).
- Sukma District located in the southern tip of the state of Chhattisgarh is covered with the semi-tropical forest and is a mainland of tribal community **Gond.**
- One major river that flows through the district is Sabari (a tributary of Godavari river).

- Over a few decades, this region has become a fostering ground for Left Wing Extremism (LWE) activities and the uneven terrains and the tricky geographic locations made this region a safer hideout for the LWE activists.


Deadly attacks

Sukma has witnessed several Maoist attacks in the past. A look at some of the previous encounters

MARCH 23, 2021: Five DRG personnel of the Chhattisgarh police killed after their bus is blown up by a powerful bomb in Narayanpur district

MAY 9, 2020: A sub-inspector of the Chhattisgarh police killed in an encounter with the Maoists in Rajnandgaon

MARCH 22, 2020: 17 members of a police patrol killed in an ambush in Sukma

OCT. 27, 2018: Four CRPF personnel killed in an ambush in Bijapur district

MARCH 11, 2017: 12 CRPF personnel killed in an ambush in Sukma district

Road Requirement Plan for Left Wing Extremism (LWE) Affected Areas

- Road Requirement Plan for Left Wing Extremism (LWE) Affected Areas Scheme is being implemented by the Ministry of Road Transport and Highways for improving road connectivity in 34 LWE affected districts of 8 States.
- 8 States are Andhra Pradesh, Bihar, Chhattisgarh, Jharkhand, Madhya Pradesh, Maharashtra, Odisha and Uttar Pradesh.
- This scheme envisaged construction of 5,422 km roads lengths in LWE affected States.

Left Wing Extremism (LWE)

- Left Wing Extremism (LWE) organizations are the groups that try to bring change through violent revolution. They are against democratic institutions and use violence to subvert the democratic processes at ground level.
- These groups prevent the developmental processes in the least developed regions of the country and try to misguide the people by keeping them ignorant of current happenings.
- Left Wing Extremists are popularly known as Maoists worldwide and as Naxalites in India.

PERSISTENT MINDLESSNESS: ON MAOIST ENCOUNTER

Context:

The deaths of over 20 paramilitary personnel in an encounter with the Maoists in the Tarrem area near Chhattisgarh's Sukma district once again puts the spotlight on the long-running conflict in this remote tribal region.

Relevance:

GS-III: Internal Security Challenges (Linkages of Organized Crime with Terrorism, Left-Wing Extremism)

Mains Questions:

Is lack of development the real cause for the spread of left-wing extremism (LWE)? Briefly explain the Government of India's approach to counter the challenges posed by LWE. (15 Marks)

Dimensions of the Article:

1. Background to the Maoist attack in Chhattisgarh
2. Trend in Maoist / Naxalite insurrection
3. Radicalization
4. Types of Radicalisation
5. Left Wing Extremism (LWE)
6. What is Naxalism in India?
7. Causes of Naxalism in India:
8. Government Initiatives to fight LWE
9. Way Forward

Background to the Maoist attack in Chhattisgarh

- Reports indicate a Maoist ambush of the paramilitary personnel from different units who had proceeded to perform combing operations in Maoist strongholds.
- The units had embarked upon their combing exercise at a time when Maoists were trying to disrupt the construction of a road near Silger-Jagargunda.
- The lack of road and telecommunications infrastructure in these remote areas has been one of the reasons for the Maoists being able to use the terrain to their advantage.

Trend in Maoist / Naxalite insurrection

- The Maoist insurrection which began first as the Naxalite movement in the 1970s and then intensified since 2004, following the merger of two prominent insurgent groups, remains a mindless guerrilla-driven militant movement that has failed to gain adherents beyond those living in remote tribal areas either untouched by welfare or are discontents due to state repression.
- The Maoists are now considerably weaker than a decade ago, with several senior leaders either dead or incarcerated, but their core insurgent force in south Bastar remains intact.
- The recourse to violence is now little more than a ploy to invite state repression which furthers their aim of gaining new adherents.
- While the Indian state has long since realised that there cannot only be a military end to the conflict, the Chhattisgarh government's inability to reach out to those living in the Maoist strongholds remains a major hurdle, which has resulted in a protracted but violent stalemate in the area.

Radicalization

- Radicalization is a process by which an individual or group comes to adopt increasingly extreme political, social, or religious ideals and aspirations that reject or undermine the status quo or contemporary ideas and expressions of the nation.
- The outcomes of radicalization are shaped by the ideas of the society at large; for example, radicalism can originate from a broad social consensus against progressive changes in society or from a broad desire for change in society.

- Radicalization can be both violent and nonviolent, although most academic literature focuses on radicalization into violent extremism (RVE).
- There are multiple pathways that constitute the process of radicalization, which can be independent but are usually mutually reinforcing.
- Radicalization that occurs across multiple reinforcing pathways greatly increases a group's resilience and lethality.
- Furthermore, by compromising its ability to blend in with non-radical society and participate in a modern, national economy, radicalization serves as a kind of sociological trap that gives individuals no other place to go to satisfy their material and spiritual needs

Types of Radicalisation

1. **Right-Wing Extremism –** It is characterized by the violent defence of a racial, ethnic or pseudo-national identity, and is also associated with radical hostility towards state authorities, minorities, immigrants and/or left-wing political groups.
2. **Politico-Religious Extremism –** It results from political interpretation of religion and the defence, by violent means, of a religious identity perceived to be under attack (via international conflicts, foreign policy, social debates, etc.). Any religion may spawn this type of violent radicalization.
3. **Left-Wing Extremism –** It focuses primarily on anti-capitalist demands and calls for the transformation of political systems considered responsible for producing social inequalities, and that may ultimately employ violent means to further its cause. It includes anarchist, maoist, Trotskyist and marxist–leninist groups that use violence to advocate for their cause.

Left Wing Extremism (LWE)

- Left Wing Extremism (LWE) organizations are the groups that try to bring change through violent revolution. They are against democratic institutions and use violence to subvert the democratic processes at ground level.
- These groups prevent the developmental processes in the least developed regions of the country and try to misguide the people by keeping them ignorant of current happenings.
- Left Wing Extremists are popularly known as Maoists worldwide and as Naxalites in India.

What is Naxalism in India?

- A Naxal or Naxalite is a member of any political organisation that claims the legacy of the Communist Party of India (Marxist–Leninist), founded in Calcutta in 1969. The term Naxal derives from the name of the village Naxalbari in West Bengal, where the Naxalite peasant revolt took place in 1967.
- It creates conditions for non-functioning of the government and actively seeks disruption of development activities as a means to achieve its objective of 'wresting control'. It spreads fear among the law-abiding citizens.
- Naxalism is considered to be one of the biggest internal security threats India faces.
- The conflict is concentrated the Eastern part of the country, particularly an area known as the Red Corridor spread across the states of Chhattisgarh, Odisha, Jharkhand, Bihar and Andhra Pradesh. o Some districts of Kerala, Telangana, Uttar Pradesh, Andhra Pradesh etc are impacted by Naxalism.
- Naxal violence is related to the intensity of the feeling of people of their deprivation and their commitment to take revenge against those who are believed to be responsible for such denial.
- Currently, the main supporters of the movement are marginalized groups of India including Dalits and Adivasis, who believe they have been neglected by the government.
- Further, Naxals support Maoist political sentiments and ideology.

Causes of Naxalism in India:

- **Mismanagement of Forests:** It is one of the main reasons for the spread of Naxalism. It started with the British government. The monopolization of the forest started with the enactment of various forest laws. The integration with the wider world led to an influx of a new class like moneylenders. The administrative machinery became more exploitative and extortionate at functional level.
- **Tribal policies not implemented well:** Even during the post-Independence era, the government was not able to stop the process of the tribal alienation and their displacement caused by large projects. Even the issues of food security were not fully sorted out. Consequently, Naxalism made inroads in Orissa and other states.
- **The Growing inter and intra-regional disparities:** Naxalism attract people who have poor livelihood like fishermen, farmers, daily labourers and bamboo cutters. The government policies have failed to stem the growing inter and intra-regional disparities. The poor people think that Naxalism can provide solutions to their problems.
- **Absence of proper Industrialization and lack of land reforms:** The half-hearted implementation of land reforms by the government has yielded negative results. The agrarian set up has not been defined in the absence of proper implementation of survey and settlement. This further damaged the agriculture production and the rural economy. Absence of proper industrialization has failed to generate employment for rural people leading to dissatisfaction with the government. It is also one of the causes behind Naxalism.
- **Geographical Terrain:** Naxalism thrives in areas covered with forests. It helps them fight against the police and the army by waging Guerrilla warfare.
- **Middle Class Youth:** The educated youths have been the largest supporters of the Naxalist movement as the maximum of the youths involved in the movement are medical and engineering graduates. Universities have turned up to be a pitch for the creation of radical ideologies.

Government Initiatives to fight LWE

1. **Greyhounds** was raised in 1989 as an elite anti-naxal force.
2. **Operation Green Hunt** was started in 2009-10 and massive deployment of security forces was done in the naxal-affected areas. It decreased Naxal affected areas from 223 to 90 districts in 9 years.
3. **LWE Mobile Tower Project** envisioned to improve mobile connectivity in the LWE areas, the Government in 2014, approved installation of mobile towers in LWE affected States.
4. **Aspirational Districts Programme** was launched in 2018, it aims to rapidly transform the districts that have shown relatively lesser progress in key social areas.
5. **Police Modernization** Scheme plus fortification of police station in areas affected by Naxal movements. Assistance in training of State Police through the Ministry of Defence.
6. **National Policy and Action Plan 2015** is a multi-pronged strategy in the areas of security, development, ensuring rights & entitlement of local communities etc
7. **Special Infrastructure Scheme** for funds to the States of Bihar, Chhattisgarh, Jharkhand and Odisha to raise Special Task Force to combat LWE.
8. **Security Related Expenditure (SRE) Scheme:** Under this the central Govt. reimburses security related expenditure to the LWE affected state Governments.
9. **Unlawful Activities (Prevention) Act, 1967** has been amended to strengthen the punitive measures.

SAMADHAN Doctrine

SAMADHAN doctrine is the one-stop solution for the LWE problem.

It encompasses the entire strategy of government from short-term policy to long-term policy formulated at different levels.

- S- Smart Leadership,
- Aggressive Strategy,
- M- Motivation and Training,
- Actionable Intelligence,
- D- Dashboard Based KPIs (Key Performance Indicators) and KRAs (Key Result Areas),
- H- Harnessing Technology,
- Action plan for each Theatre, and
- N- No access to Financing.

Way Forward

- **Good governance –** Analyzing the loopholes in the present strategy and developing a coherent national strategy to end the menace.
- **Dialogue –** Between the Naxal leaders, and the government officials can be a way to work out a solution.
- **Generate more employment and increase wages –** insecure livelihood and unemployment in the areas have left the people with little option but to join the Naxals.
- **Ending the political marginalization of weaker sections –** Weaker sections of the society, the schedule castes and schedule tribes still face discrimination from the upper class making them a soft target for the Naxals.
- **Remove disparity –** Economic disparity and the growing distance between rich and the poor is one of the main problems that has contributed to the growth of Naxalism.

WHY THE PERSONAL DATA PROTECTION BILL MATTERS?

Context:

The number of personal data breaches from major digital service providers has increased worryingly in the same period as the pandemic has forced more people to participate in the digital economy.

The Personal Data Protection Bill, 2019, now under scrutiny by a Joint Parliamentary Committee, could play a big role in providing robust protections to users and their personal data.

Relevance:

GS-III: Internal Security Challenges (Cyber Security, Government Policies & Interventions, Internal security challenges through communication networks)

Mains Questions:

What is need for India to have a robust data protection regime? To what extent does the Personal Data Protection Bill, 2019 address the issues? Critically examine. (15 Marks)

Dimensions of the Article:

1. Significance of Data
2. Personal Data Protection Bill 2019
3. Advantages of the changes
4. Issues with the bill

5. Data Protection Authority (DPA): The solution?
6. Broad Mandate of the DPA, a problem

Significance of Data

- Data is the large collection of information that is stored in a computer or on a network.
- Data is collected and handled by entities called data fiduciaries.
- While the fiduciary controls how and why data is processed, the processing itself may be by a third party, the data processor.
- This distinction is important to delineate responsibility as data moves from entity to entity. For example, in the US, Facebook (the data controller) fell into controversy for the actions of the data processor — Cambridge Analytica.
- The processing of this data (based on one's online habits and preferences, but without prior knowledge of the data subject) has become an important source of profits for big corporations.
- Apart from it, this has become a potential avenue for invasion of privacy, as it can reveal extremely personal aspects.
- Also, it is now clear that much of the future's economy and issues of national sovereignty will be predicated on the regulation of data.
- The physical attributes of data — where data is stored, where it is sent, where it is turned into something useful — are called data flows. Data localisation arguments are premised on the idea that data flows determine who has access to the data, who profits off it, who taxes and who "owns" it.

Personal Data Protection Bill 2019

- The Personal Data Protection Bill 2019 (PDP Bill 2019) is being analyzed by a Joint Parliamentary Committee (JPC) in consultation with experts and stakeholders.
- The Bill covers mechanisms for protection of personal data and proposes the setting up of a Data Protection Authority (DPA) of India for the same.
- Some key provisions the 2019 Bill provides for which the 2018 draft Bill did not, such as that the central government can exempt any government agency from the Bill and the Right to Be Forgotten, have been included.
- The Bill proposes "Purpose limitation" and "Collection limitation" clause, which limit the collection of data to what is needed for "clear, specific, and lawful" purposes.
- It also grants individuals the right to data portability and the ability to access and transfer one's own data. It also grants individuals the right to data portability, and the ability to access and transfer one's own data.
- Finally, it legislates on the right to be forgotten. With historical roots in European Union law, General Data Protection Regulation (GDPR), this right allows an individual to remove consent for data collection and disclosure.

The Bill trifurcates data as follows:

1. Personal data: Data from which an individual can be identified like name, address etc.
2. Sensitive personal data (SPD): Some types of personal data like as financial, health, sexual orientation, biometric, genetic, transgender status, caste, religious belief, and more.
3. Critical personal data: Anything that the government at any time can deem critical, such as military or national security data.

Advantages of the changes

- Data localisation can help law-enforcement agencies access data for investigations and enforcement.
- As of now, much of cross-border data transfer is governed by individual bilateral “mutual legal assistance treaties”.
- Accessing data through this route is a cumbersome process and also instances of cyber-attacks and surveillance can be checked easily.
- Social media is being used to spread fake news, which has resulted in lynchings, national security threats, which can now be monitored, checked and prevented in time.
- Data localisation will also increase the ability of the Indian government to tax Internet giants.
- A strong data protection legislation will also help to enforce data sovereignty.

Issues with the bill

- The current draft requires the DPA to maintain a cadre of adjudicating officers and specifies their desired areas of expertise.
- All other important details, like the terms of appointment, jurisdictional scope, and procedure for hearings, are, however, left to be decided by the central government.
- The Bill doesn’t even specify whether the adjudication process can, or should, be preceded by mediation, which could help in the amicable settlement of many complaints.
- Many contend that the physical location of the data is not relevant in the cyber world. Even if the data is stored in the country, the encryption keys may still be out of reach of national agencies.
- National security or reasonable purposes are an open-ended terms, this may lead to intrusion of state into the private lives of citizens.
- Technology giants like Facebook and Google have criticised protectionist policy on data protection (data localisation).
- Protectionist regime supress the values of a globalised, competitive internet marketplace, where costs and speeds determine information flows rather than nationalistic borders.
- Also, it may backfire on India’s own young startups that are attempting global growth, or on larger firms that process foreign data in India.

Data Protection Authority (DPA): The solution?

- One of the many important duties cast on the Data Protection Authority (DPA) that is to be created under the Bill is to adjudicate complaints received from data principals — individuals whose personal data is processed by others.
- The DPA is set to function as what the Financial Sector Legislative Reforms Commission (FSLRC) termed as a “mini-state”. This refers to an agency that is entrusted with a mix of quasi-legislative (regulation-making), executive (supervision and enforcement), and quasi-judicial (adjudication) functions.
- It comes with the risk that, absent structural safeguards, the agency might end up abusing or, conversely, neglecting some of its functions. A carefully-crafted regulatory design and robust accountability mechanisms are, therefore, essential.

Broad Mandate of the DPA, a problem

- Unlike other sectoral regulators that oversee specific businesses, the DPA’s authority will extend to anyone who deals with personal data.
- This may include individuals, private entities or any department or agency of the state.
- Further, since each data principal is party to multiple online and offline relationships, the universe of regulated transactions becomes even larger.

- Even a miniscule 0.5% rate of complaints out of the total shares of personal data will result in more than 10 million cases in a year. A caseload of this sort would be daunting for any agency.
- As a consequence, the DPA may either be overwhelmed by the volume of complaints or may grossly under-prioritise this aspect, resulting in delays, erosion of trust and poorer outcomes.

INDIA 3RD HIGHEST MILITARY SPENDER: SIPRI REPORT

Context:

Stockholm International Peace Research Institute (SIPRI) recently published the latest data on the military spending across the world – which has increased to USD 1,981 billion in 2020, during Covid-19 pandemic.

Relevance:

GS-III: Internal Security Challenges (Security Challenges & their Management), GS-III: Indian Economy (Budgeting)

Dimensions of the Article:

1. About SIPRI
2. India-Specific Highlights of the SIPRI Report on Military spending
3. General Highlights of the SIPRI report

About SIPRI

- Stockholm International Peace Research Institute (SIPRI) is an independent international think-tank institute dedicated to research into conflict, armaments, arms control and disarmament.
- It was established in 1966 at Stockholm (Sweden).
- It provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

India-Specific Highlights of the SIPRI Report on Military spending

- India was the third largest military spender in the world in 2020 – The top 2 were the US and China.
- India's military expenditure accounted for almost 4% of the global military expenditure share.
- India's spending since 2019 grew by more than 2% which is largely attributed to India's ongoing conflict with Pakistan and renewed border tension with China.
- India accounted for 9.5% of the total global arms imports during 2016-2020.

Reasons for this Increased Spending

- The continuing military confrontation with China in eastern Ladakh, of course, has led India to make several emergency arms purchases from abroad since the crisis erupted in early May 2020.
- India has to maintain an over 15-lakh strong armed forces because of the two active and unresolved borders with China and Pakistan.
- India's annual military expenditure also includes a huge pension bill for 33-lakh veterans and defence civilians.

- With a weak domestic defence-industrial base, India of course continues to languish in the strategically-vulnerable position of being the world's second-largest arms importer just behind Saudi Arabia.

General Highlights of the SIPRI report

Military spending as a share of Gross Domestic Product (GDP), reached a global average of 2.4% in 2020, up from 2.2% in 2019.

The five biggest spenders in 2020, which together accounted for 62% of global military expenditure were:

1. United States
2. China
3. India
4. Russia
5. United Kingdom.

- Nearly all members of the North Atlantic Treaty Organization (NATO) saw their military burden rise in 2020.
- The countries with the biggest increases in military burden among the top 15 spenders in 2020 were Saudi Arabia, Russia, Israel and US.
- In addition to China, India (USD 72.9 billion), Japan (USD 49.1 billion), South Korea (USD 45.7 billion) and Australia (USD 27.5 billion) were the largest military spenders in the Asia and Oceania region.
- The combined military spending of the 11 Middle Eastern countries for which SIPRI has spending figures decreased by 6.5% in 2020.

WHAT IS FACEBOOK'S OVERSIGHT BOARD?

Context:

Trump had been banned indefinitely by Facebook from posting or accessing his page on January 2021 following the chaotic situation of US Capitol Hill Siege.

Facebook's Oversight Board upheld the social media network's decision to indefinitely block Mr. Trump for using the platform to "incite violent insurrection against a democratically elected government."

Recently the Oversight Board overturned Facebook's decision to remove a post that had alleged that the RSS and Prime Minister Narendra Modi were threatening to kill Sikhs in India.

Relevance:

GS-III: Internal Security Challenges (Challenges to Internal Security Through Communication Networks, Role of Media & Social Networking Sites in Internal Security Challenges), GS-II: Polity and Governance (Government Policies & Interventions)

Dimensions of the Article:

1. What is Facebook's Oversight Board?
2. What are recommendations of the Oversight Board?

3. Law Related to Blocking of Internet Services/Content in India
4. Obligations of Intermediaries under the IT Act

What is Facebook's Oversight Board?

- The Oversight Board has been set up as an independent body that will help Facebook figure out what content can be allowed on the platform and what ought to be removed.
- It was said to have emerged out of the tensions around the often-conflicting goals of maintaining Facebook as a platform for free speech and effectively filtering out problematic speech.
- The members who make the Oversight Board came on board very recently, in 2020 and the board consists of 20 members.

What are recommendations of the Oversight Board?

- The Board wants Facebook to act quickly when it comes to content of a political nature coming from influential users.
- Its idea is to escalate such content to specialised staff as also assess potential harms from such accounts.
- It also wants Facebook to be more transparent about its policies regarding assistance to investigations as well as its penalty rules.
- It also wants Facebook to comprehensively review its "potential contribution to the narrative of electoral fraud and the exacerbated tensions that culminated in the violence in the United States on January 6. This should be an open reflection on the design and policy choices that Facebook has made that may allow its platform to be abused."

Law Related to Blocking of Internet Services/Content in India

- In India, the **Information Technology (IT) Act, 2000**, as amended from time to time, governs all activities related to the use of computer resources and covers all 'intermediaries' who play a role in the use of computer resources and electronic records. The role of the intermediaries has been spelt out in separate rules framed for the purpose in 2011- The **Information Technology (Intermediaries Guidelines) Rules, 2011**.
- **Section 69 of the IT Act** confers on the Central and State governments the power to issue directions "to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource".

The grounds on which these powers may be exercised are:

1. In the interest of the sovereignty or integrity of India, defence of India, the security of the state.
2. Friendly relations with foreign states.
3. Public order, or for preventing incitement to the commission of any cognizable offence relating to these.
4. For investigating any offence.

Section 69A of the IT Act enables the Centre to ask any agency of the government, or any intermediary, to block access to the public of any information generated, transmitted, received or stored or hosted on any computer resource.

Obligations of Intermediaries under the IT Act

- The term ‘intermediaries’ includes providers of telecom service, network service, Internet service and web hosting, besides search engines, online payment and auction sites, online marketplaces and cyber cafes.
- It includes any person who, on behalf of another, “receives, stores or transmits” any electronic record. Social media platforms would fall under this definition.
- Intermediaries are required to preserve and retain specified information in a manner and format prescribed by the Centre for a specified duration.
- When a direction is given for monitoring, the intermediary and any person in charge of a computer resource should extend technical assistance in the form of giving access or securing access to the resource involved.
- **Section 79 of the IT Act 2000** makes it clear that “an intermediary shall not be liable for any third-party information, data, or communication link made available or hosted by him”. This protects intermediaries such as Internet and data service providers and those hosting websites from being made liable for content that users may post or generate.

DATA PROTECTION IN INDIA & WHATSAPP’S PRIVACY POLICY

Context:

Instant messaging platform WhatsApp may face legal action in India by May 25 if it does not send a satisfactory reply to a new notice sent by the Ministry of Electronics and Information Technology asking the company to withdraw its latest privacy policy update.

Relevance:

GS-III: Internal Security Challenges (Cyber Security), Science and Technology (IT & Computers)

Dimensions of the Article:

1. About WhatsApp’s updated privacy policy
2. Significance of Data
3. Need for Data Protection
4. Personal Data Protection Bill 2019
5. Advantages of the changes
6. Issues with the bill

About WhatsApp’s updated privacy policy

- According to WhatsApp’s updated privacy policy, users would no longer be able to stop the app from sharing data (such as location and number) with its parent Facebook unless they delete their accounts altogether.
- Its privacy updates are designed to make the business interactions that take place on its platform easier while also personalising ads on Facebook. That is how it will have to make its money.
- According to the Government, the messaging app discriminates against Indian users vis-à-vis users in Europe on the matter of a choice to opt-out of the new privacy policy.
- WhatsApp users in Europe can opt-out of the new privacy policy owing to the laws in the European Union (EU) called the General Data Protection Regulation (GDPR), which shield them from sharing data from Facebook or grant them the power to say no to WhatsApp’s new terms of service.

Significance of Data

- Data is the large collection of information that is stored in a computer or on a network.
- Data is collected and handled by entities called data fiduciaries.
- While the fiduciary controls how and why data is processed, the processing itself may be by a third party, the data processor.
- This distinction is important to delineate responsibility as data moves from entity to entity. For example, in the US, Facebook (the data controller) fell into controversy for the actions of the data processor — Cambridge Analytica.
- The processing of this data (based on one's online habits and preferences, but without prior knowledge of the data subject) has become an important source of profits for big corporations.
- Apart from it, this has become a potential avenue for invasion of privacy, as it can reveal extremely personal aspects.
- Also, it is now clear that much of the future's economy and issues of national sovereignty will be predicated on the regulation of data.
- The physical attributes of data — where data is stored, where it is sent, where it is turned into something useful — are called data flows. Data localisation arguments are premised on the idea that data flows determine who has access to the data, who profits off it, who taxes and who "owns" it.

Need for Data Protection

- According to the Internet and Mobile Association of India (IAMAI)'s Digital in India report 2019, there are about 504 million active web users and India's online market is second only to China.
- Large collection of information about individuals and their online habits has become an important source of profits. It is also a potential avenue for invasion of privacy because it can reveal extremely personal aspects.
- Companies, governments, and political parties find it valuable because they can use it to find the most convincing ways to advertise to you online.

Personal Data Protection Bill 2019

- The Personal Data Protection Bill 2019 (PDP Bill 2019) is being analyzed by a Joint Parliamentary Committee (JPC) in consultation with experts and stakeholders.
- The Bill covers mechanisms for protection of personal data and proposes the setting up of a Data Protection Authority (DPA) of India for the same.
- Some key provisions the 2019 Bill provides for which the 2018 draft Bill did not, such as that the central government can exempt any government agency from the Bill and the Right to Be Forgotten, have been included.
- The Bill proposes "Purpose limitation" and "Collection limitation" clause, which limit the collection of data to what is needed for "clear, specific, and lawful" purposes.
- It also grants individuals the right to data portability and the ability to access and transfer one's own data. It also grants individuals the right to data portability, and the ability to access and transfer one's own data.
- Finally, it legislates on the right to be forgotten. With historical roots in European Union law, General Data Protection Regulation (GDPR), this right allows an individual to remove consent for data collection and disclosure.
- The Bill trifurcates data as follows:

1. Personal data: Data from which an individual can be identified like name, address etc.
2. Sensitive personal data (SPD): Some types of personal data like as financial, health, sexual orientation, biometric, genetic, transgender status, caste, religious belief, and more.
3. Critical personal data: Anything that the government at any time can deem critical, such as military or national security data.

Advantages of the changes

- Data localisation can help law-enforcement agencies access data for investigations and enforcement.
- As of now, much of cross-border data transfer is governed by individual bilateral "mutual legal assistance treaties".
- Accessing data through this route is a cumbersome process and also instances of cyber-attacks and surveillance can be checked easily.
- Social media is being used to spread fake news, which has resulted in lynchings, national security threats, which can now be monitored, checked and prevented in time.
- Data localisation will also increase the ability of the Indian government to tax Internet giants.
- A strong data protection legislation will also help to enforce data sovereignty.

Issues with the bill

- The current draft requires the DPA to maintain a cadre of adjudicating officers and specifies their desired areas of expertise.
- All other important details, like the terms of appointment, jurisdictional scope, and procedure for hearings, are, however, left to be decided by the central government.
- The Bill doesn't even specify whether the adjudication process can, or should, be preceded by mediation, which could help in the amicable settlement of many complaints.
- Many contend that the physical location of the data is not relevant in the cyber world. Even if the data is stored in the country, the encryption keys may still be out of reach of national agencies.
- National security or reasonable purposes are an open-ended term, this may lead to intrusion of state into the private lives of citizens.
- Technology giants like Facebook and Google have criticised protectionist policy on data protection (data localisation).
- Protectionist regime supress the values of a globalised, competitive internet marketplace, where costs and speeds determine information flows rather than nationalistic borders.
- Also, it may backfire on India's own young startups that are attempting global growth, or on larger firms that process foreign data in India.

GOVT CLEARS BUILDING OF 6 ATTACK SUBMARINES

Context:

The Defence Acquisition Council (DAC) gave the Indian Navy the go-ahead Friday to select an Indian strategic partner company which, in collaboration with a foreign Original Equipment Manufacturer (OEM), will build six conventional attack submarines in the country.

Relevance:

GS-III: Internal Security Challenges

Dimensions of the Article:

1. Defence Acquisition Council (DAC)
2. About the 6 conventional attack submarines

Defence Acquisition Council (DAC)

- As an overarching structure, the Defence Acquisition Council (DAC), under the Defence Minister is constituted for overall guidance of the defence procurement planning process.
- DAC is the highest decision-making body in the Defence Ministry for deciding on new policies and capital acquisitions for the three services (Army, Navy and Air Force) and the Indian Coast Guard.
- The objective of the Defence Acquisition Council is to ensure expeditious procurement of the approved requirements of the Armed Forces in terms of capabilities sought, and time frame prescribed, by optimally utilizing the allocated budgetary resources.
- It was formed, after the Group of Ministers recommendations on 'Reforming the National Security System', in 2001, post Kargil War (1999).

Composition of Defence Acquisition Council

1. Defence Minister: Chairman
2. Minister of State for Defence: Member
3. Chief of Army Staff: Member
4. Chief of Naval Staff: Member
5. Chief of Air Staff: Member
6. Defence Secretary: Member
7. Secretary Defence Research & Development: Member
8. Secretary Defence Production: Member
9. Chief of Integrated Staff Committees HQ IDS: Member
10. Director General (Acquisition): Member
11. Dy. Chief of Integrated Defence: Staff Member Secretary

About the 6 conventional attack submarines

- This project envisages indigenous construction of six conventional submarines equipped with the state-of-the-art Air Independent Propulsion system at an estimated cost of Rs 43,000 crore.
- Project 75 India or P75I will be the first under the strategic partnership model, promulgated in 2017 to boost indigenous defence manufacturing.
- The first submarine built under the project is likely to be delivered by 2030.
- The project had been approved in 2007, but remained on the backburner until 2019 when the government approved the Acceptance of Necessity.
- The five OEMs are Rosoboronexport (ROE) of Russia, ThyssenKrupp of Germany, Naval Group of France, Navantia of Spain and Daewoo Shipbuilding & Marine Engineering of South Korea.
- The DAC nod for six conventional submarines came on the day INS Chakra, leased from Russia and one of India's two nuclear submarines, was spotted off Singapore, reportedly on its way back to Russia — the 10-year lease term is ending soon.

INNOVATIONS FOR DEFENCE EXCELLENCE CHALLENGE

Context:

Defence Minister has approved the budgetary support of Rs. 500 crore to Innovations for Defence Excellence (iDEX) challenge under the Defence Innovation Organisation (DIO) for the next five years.

Relevance:

Prelims, GS-III: Internal Security Challenges

Dimensions of the Article:

1. Defence India Startup Challenge (DISC)
2. Innovations for Defence Excellence (iDEX)
3. Other Related Initiatives:

Defence India Startup Challenge (DISC)

- iDEX-DIO had launched the Defence India Startup Challenge (DISC) to address problems faced by the Armed Forces, DPSUs & OFB.
- The Defence India Startup Challenge (DISC) has been launched under the Ministry of Defence in partnership with Atal Innovation Mission.
- The program aims at supporting Startups/MSMEs/Innovators to create prototypes and/or commercialize products/solutions in the area of National Defence and Security.

Defence Innovation Organization (DIO)

- Defence Innovation Organization (DIO) is a Non-Profit Organisation (NOPO) established under Section 8 of the Companies Act 2013.
- The founding members are Hindustan Aeronautics Limited (HAL) and Bharat Electronics Limited (BEL).

Innovations for Defence Excellence (iDEX)

- Innovations for Defence Excellence (iDEX) is an initiative taken by the government, launched in 2018, to contribute towards modernization of the Defence Industry.
- iDEX aims to promote innovation and technology development in Defence and Aerospace by engaging Industries (which includes MSMEs, start-ups, individual innovators, R&D institutes & academia).
- iDEX will provide the engaging industries with funding and other support to carry out Research & Development.
- iDEX will be funded and managed by Defence Innovation Organization (DIO), and will function as the executive arm of DIO.
- iDEX has partnered with leading incubators in the country to provide hand holding, technical support and guidance to the winners of iDEX challenges.

Main objectives of iDEX

1. To frame ‘corporate Venture Capital’ models for Indian Defence needs thereby identifying emerging technologies, connecting innovators with military units, facilitating co-creation of new and appropriate technologies and so forth into weapon systems used by Indian Armed Services.
2. To deliver military-grade products thereby solving the critical needs of the Indian defence set-up by developing or applying advanced technologies.
3. To devise a culture of innovation in the Indian Defence and Aerospace by engaging startups and innovators for co-creation and co-innovation.

Other Related Initiatives:

1. Defence Industrial Corridors: To support the growth of the Defence sector and enhance manufacturing capacity in the sector, two Defence Industrial Corridors are being set up in India, one in Uttar Pradesh and another in Tamil Nadu.
2. Strategic Partnership (SP) Model: It identifies a few Indian private companies who would initially tie up with global Original Equipment Manufacturers (OEMs) to seek technology transfers to set up domestic manufacturing infrastructure and supply chains. It is a part of Defence Acquisition Procedure (DAP) 2020. Under DAP 2020, the Ministry of Defence (MoD) has also notified a 'positive indigenisation list' of 108 items.
3. Artificial Intelligence in Defence: N Chandrasekaran Task Force was set up in 2018 to study implications of AI in national security. Defence Artificial Intelligence Project Agency (DAIPA) was created in March, 2019. DAIPA aims for greater thrust on Artificial Intelligence (AI) in Defence, formulation of an AI roadmap for each Defence PSU and Ordnance Factory Board to develop AI-enable products.

THE WORLD IS HARDLY WIRED FOR CYBER RESILIENCE

Context:

A string of high-profile cyberattacks in recent months has exposed vulnerabilities in the critical infrastructure of even advanced nations. This has reinforced the need for improved defences against actual, and potential, cyberattacks by all countries across continents.

Relevance:

GS-III: Internal Security Challenges (Basics of Cyber Security; Role of media and social-networking sites in internal security challenges; Internal security challenges through communication networks)

Mains Questions:

To what extent does the increasing sophistication in cyber-attacks affect the importance of Cyber Security? Discuss by throwing light on how cybersecurity is handled by other countries and India. (15 marks)

Dimensions of the Article:

1. What is Cyber Attack and Cyber Security?
2. Cybercrime at the international stage
3. International legislative responses and cooperation regarding cybercrime
4. Recently in news: America under attack
5. Targeting critical civilian targets
6. Increasing sophistication of the cybercriminals
7. Challenges of Cyber Security in India
8. Measures taken by the government to improve the Cyber Security

What is Cyber Attack and Cyber Security?

- A cyber attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cybercriminals use a variety of methods to launch a cyber attack, including malware, phishing, ransomware, denial of service, among other methods.

- Cybersecurity means securing the cyberspace from attack, damage, misuse and economic espionage. Cyberspace is a global domain within the information environment consisting of interdependent IT infrastructure such as Internet, Telecom networks, computer systems etc.

Cyberwarfare and cyberterrorism

- Cyberwarfare utilizes techniques of defending and attacking information and computer networks that inhabit cyberspace, often through a prolonged cyber campaign or series of related campaigns. It denies an opponent's ability to do the same, while employing technological instruments of war to attack an opponent's critical computer systems. Cyberterrorism, on the other hand, is "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population". That means the end result of both cyberwarfare and cyberterrorism is the same, to damage critical infrastructures and computer systems linked together within the confines of cyberspace.

Recently in news: America under attack

- Several high-profile cyberattacks were reported from the United States during the past several months.
- The end of 2020 witnessed the 'SolarWinds' cyberattack involving data breaches across critical wings of the U.S. government like defence, energy and state.
- Early 2021 witnessed a cyberattack by a Chinese group called Hafnium. Thousands of U.S. organizations were hacked and remote control was gained over the affected systems.
- Then there was the ransomware attack on Colonial Pipeline (which is the main supplier of oil to the U.S. East Coast) by Russia/East Europe-based cybercriminals, styled DarkSide. Colonial Pipeline had to pay out several million dollars as ransom to unlock its computers and release its files.

Targeting critical civilian targets

- Unlike the traditional approach to cyber warfare, cyber attacks are now being employed against civilian targets of critical importance. The fact that most nations have been concentrating mainly on cyber defences to protect military and strategic targets has left civilian targets vulnerable to attacks.
- Unlike previously where the banking and financial services were most prone to ransomware attacks, recently even oil, electricity grids, and health care are being increasingly targeted.
- Defending critical civilian targets against cyberattacks is almost certain to stretch the capability and resources of governments across the globe.

Increasing sophistication of the cybercriminals

- The technical competence of cybercriminals has only increased. They have been employing advanced methods like 'penetration testers' to probe high secure networks.
- Zero day software vulnerabilities are being increasingly used for cyber attacks such as ransomware, phishing and spear phishing.
- Cybercriminals are becoming more sophisticated in their modus operandi. They first steal sensitive data in targeted computers before launching a ransomware attack thus resulting in a kind of 'double jeopardy' for the targeted victim.

Terms Used

- A zero-day is a computer-software vulnerability unknown to those who should be interested in its mitigation. Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers or a network.
- Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access.
- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers or to deploy malicious software on the victim's infrastructure like ransomware. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
- Spear phishing is the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.

Cybercrime at the international stage

- There is no commonly agreed single definition of "cybercrime". It refers to illegal internet-mediated activities that often take place in global electronic networks.
- **Cybercrime is "international" or "transnational" – there are 'no cyber-borders between countries'.**
- International cybercrimes often challenge the effectiveness of domestic and international law, and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced.
- Cybercrime is a growing concern to countries at all levels of developments and affects both, buyers and sellers.
- While 154 countries (79 per cent) have enacted cybercrime legislation, the pattern varies by region: Europe has the highest adoption rate (93 per cent) and Asia and the Pacific the lowest (55 per cent).
- The evolving cybercrime landscape and resulting skills gaps are a significant challenge for law enforcement agencies and prosecutors, especially for cross-border enforcement.
- Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale.
- China–United States cooperation is one of the most striking progress recently, because they are the top two source countries of cybercrime.

International legislative responses and cooperation regarding cybercrime

International Telecommunication Union (ITU)

- The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cybersecurity issues. The ITU was the lead agency of the World Summit on the Information Society (WSIS).
- In 2003, Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cybercrime.
- In 2005, the Tunis Commitment and the Tunis Agenda were adopted for the Information Society.

G8

- Group of Eight (G8) is made up of the heads of eight industrialized countries: the U.S., the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada.
- In 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cybercrime, and designates all member countries to have a point of contact on 24 hours a day / 7 days a week basis.

United Nations

- In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology.

Council of Europe

- Council of Europe is an international organisation focusing on the development of human rights and democracy in its 47 European member states.
- In 2001, the Convention on Cybercrime, the first international convention aimed at Internet criminal behaviors, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member states. But only 25 countries ratified later.
- It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cybercriminal offenses qualification, provision for laws empowering law enforcement and enabling international cooperation.

Challenges of Cyber Security in India

- **Data colonization:** India is net exporter of information however data servers of majority of digital service providers are located outside India. Also, data is being misused for influencing electoral outcomes, spread of radicalism etc.
- **Digital Illiteracy:** Widespread Digital illiteracy makes Indian citizens highly susceptible to cyber fraud, cyber theft, etc.
- **Substandard devices:** In India, majority of devices used to access internet have inadequate security infrastructure making them susceptible to malwares such as recently detected 'Saposhi'. Also, rampant use of unlicensed software and underpaid licenses make them vulnerable as well.
- **Lack of adoption of new technology:** For example – The Banking infrastructure is not robust to cop-up with rising digital crime as 75% of total Credit and Debit card are based on magnetic strip which are easy to be cloned.
- **Lack of uniform standards:** There are variety of devices used with non-uniform standards which makes it difficult to provide for a uniform security protocol.
- **Import dependence:** Import dependence for majority of electronic devices from cell phones to equipment's used in power sector, defence, banking, communication and other critical infrastructure put India into a vulnerable situation.
- **Lack of adequate infrastructure and trained staff:** There are currently around 30,000 cyber security vacancies in India but demand far outstrips supply of people with required skills.
- **Under-reporting:** majority of cases of cybercrime remains unreported because of lack of awareness.

- **Unsynchronised Agencies:** Lack of coordination among various agencies working for cyber security. Private sector, despite being a major stakeholder in the cyberspace, has not been involved proactively for the security of the same.
- **Anonymity:** Even advanced precision threats carried out by hackers is difficult to attribute to specific actors, state or nonstate.

Measures taken by the government to improve the Cyber Security

1. **National Critical Information Infrastructure Protection Centre (NCIIPC)** to battle cyber security threats in strategic areas such as air control, nuclear and space. It will function under the National Technical Research Organisation, a technical intelligence gathering agency controlled directly by the National Security Adviser in PMO.
2. **National cyber coordination centre (NCCC)** to scan internet traffic coming into the country and provide real time situational awareness and alert various security agencies.
3. A new **Cyber and Information Security (CIS) Division** has been created to tackle internet crimes such as cyber threats, child pornography and online stalking.
4. **Cyber Surakshit Bharat Initiative** to strengthen Cybersecurity ecosystem in India. It is first public private partnership of its kind and will leverage the expertise of the IT industry in cybersecurity.
5. **Information Technology Act, 2000** (amended in 2008) to provide a legal framework for transactions carried out by means of electronic data interchange, for data access for cybersecurity etc.

INTEGRATED TRI-SERVICE THEATRE COMMANDS

Context:

A high-level committee consisting of representatives from the services and the Ministries concerned has been formed for wider consultations on the creation of integrated triservice theatre commands.

Relevance:

GS-III: Internal Security Challenges (Security Challenges & their Management in Border Areas, Security Forces and Agencies)

Dimensions of the Article:

1. About the Recent Move on formation of Integrated Theatre Command
2. About the Integrated Triservice Theatre Commands
3. Disadvantages of having an Integrated Tri-service Theatre Command

About the Recent Move on formation of Integrated Theatre Command

- A high-level committee has been formed for the consultations on the creation of integrated triservice theatre commands that will examine all issues and find a way forward before a formal note on their creation is sent to the Cabinet Committee on Security.
- The move was necessitated due to some aspects like bringing in paramilitary forces (which is under Home Ministry) under the purview of the theatre commands and financial implications that may arise in the process of integration.

- The proposed Air Defence Command plans to integrate all air assets of the armed forces while the Maritime Theatre Command plans to bring in all assets of Navy, Coast Guard as well as coastal formations of Army and Air Force under one umbrella.

About the Integrated Triservice Theatre Commands

- An integrated theatre command envisages a unified command of the three Services, under a single commander, for geographical theatres (areas) that are of strategic and security concern.
- The commander of such a force will be able to bear all resources at his disposal — from the Army, the Indian Air Force, and the Navy — with seamless efficacy.
- The integrated theatre commander will not be answerable to individual Services.
- Integration and jointness of the three forces will avoid duplication of resources. The resources available under each service will be available to other services too.
- The integrated theatre commander will not be answerable to individual Services, and will be free to train, equip and exercise his command to make it a cohesive fighting force capable of achieving designated goals.
- The logistic resources required to support its operations will also be placed at the disposal of the theatre commander so that it does not have to look for anything when operations are ongoing.
- This is in contrast to the model of service-specific commands which India currently has, wherein the Army, Air Force and Navy all have their own commands all over the country. In case of war, each Service Chief is expected to control the operations of his Service through individual commands, while they operate jointly.

Disadvantages of having an Integrated Tri-service Theatre Command

- There has been no occasion, during actual warfare, when the three services have not operated with commendable cooperation.
- Faraway land war and medium to high intensity wars are a distant possibility.
- With increased communication networks, interaction between three organizations is easy, they can come on board, can plan without much consideration of spatial distance, so there is no need for a new organisation.
- Domain knowledge of the integrated force commander is likely to be limited in respect of the other two Services components under his command, thereby limiting his ability to employ them in the most suitable manner and at the appropriate time.

WORLD DRUG REPORT & INTERNATIONAL DAY AGAINST DRUG ABUSE

Context:

June 26 every year is observed as International Day Against Drug Abuse and Illicit Trafficking or World Drug Day.

The United Nations Office on Drugs and Crime (UNODC) released the World Drug Report 2021 recently.

Relevance:

GS-II: Social Justice (Health related issues, Government Policies and Interventions), GS-III: Internal Security Challenges (Organized Crime and Terrorism), GS-II: International Relations (Important International Institutions), Prelims

Dimensions of the Article:

1. International Day Against Drug Abuse and Illicit Trafficking
2. Drug Abuse problem worsening due to Covid-19 Pandemic
3. About United Nations Office on Drugs and Crime (UNODC)
4. UNODC World Drug Report
5. Highlights of The World Drug Report 2021
6. India's Vulnerability

International Day Against Drug Abuse and Illicit Trafficking

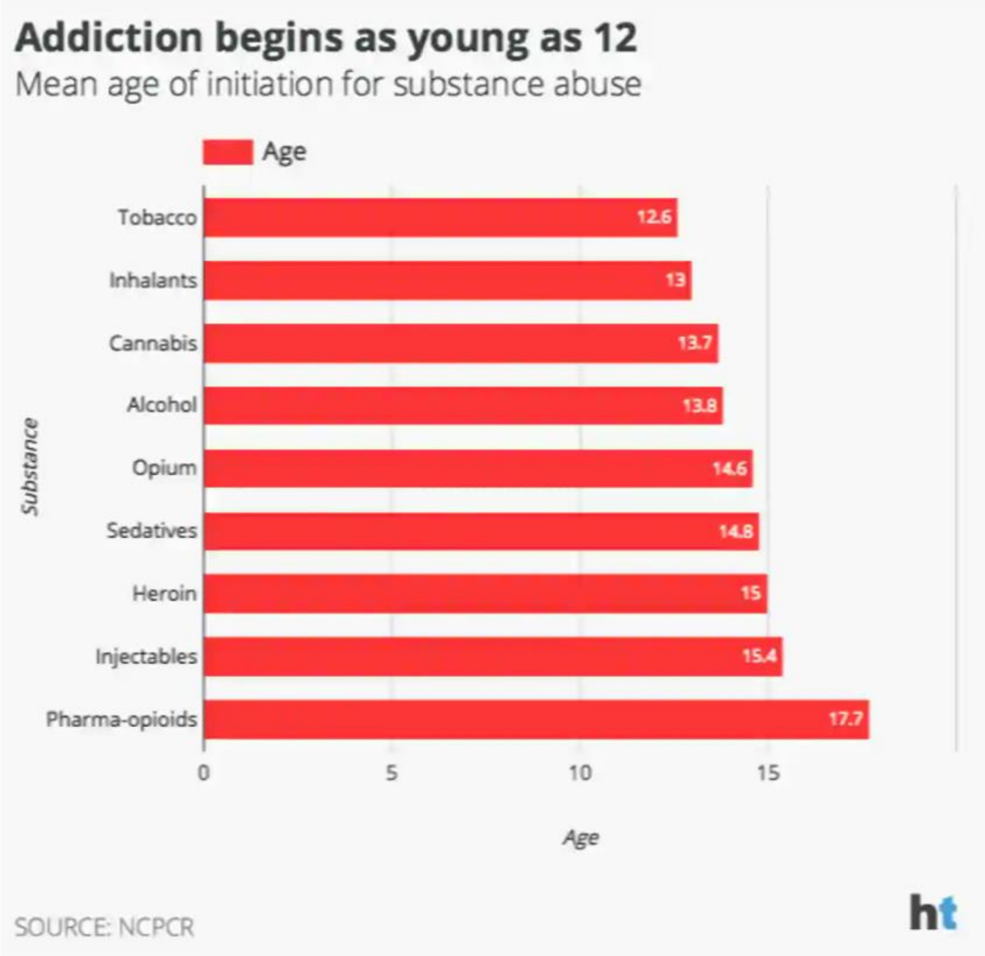
- International Day Against Drug Abuse and Illicit Trafficking is observed every year on June 26 with an aim to spread awareness about the global drug problem and eliminate drug misuse.
- Activists, therapists and organisations working in the field of preventing drug abuse come together on this day to help victims of this social evil.
- 'Share Drug Facts to Save Lives' is the theme of the International Day Against Drug Abuse and Illicit Trafficking 2021.
- The focus of 2021 is to curb the spread of misinformation on the topic and to encourage the exchange of facts related to drugs.

Drug Abuse problem worsening due to Covid-19 Pandemic

- The economic downturn caused by the global pandemic may drive more people to substance abuse or leave them vulnerable to involvement in drug trafficking and related crime.
- In the global recession that followed the 2008 financial crisis, drug users sought out cheaper synthetic substances and patterns of use shifted towards injecting drugs, while governments reduced budgets to deal with drug-related problems.
- All over the world, the risks and consequences of drug use are worsened by poverty, limited opportunities for education and jobs, stigma and social exclusion, which in turn helps to deepen inequalities, moving us further away from achieving the Sustainable Development Goals (SDGs).

Worrying Data Regarding Drug Abuse prevalence

- One out of three drug users is a woman but women represent only one out of five people in treatment.
- People in prison settings, minorities, immigrants and displaced people also face barriers to treatment due to discrimination and stigma.
- Number of people using drugs in 2018 increased by 30% from 2009, with adolescents and young adults accounting for the largest share of users.
- While the increase reflects population growth and other factors, the data nevertheless indicate that illicit drugs are more diverse, more potent and more available.
- At the same time, more than 80% of the world's population, mostly living in low- and middle-income countries, are deprived of access to controlled drugs for pain relief and other essential medical uses.



SOURCE: NCPCR

About United Nations Office on Drugs and Crime (UNODC)

- The United Nations Office on Drugs and Crime (UNODC) is a United Nations office that was established in 1997 and has its headquarters in Vienna, Austria.
- UNODC was established to assist the UN in better addressing a coordinated, comprehensive response to the interrelated issues of illicit trafficking in and abuse of drugs, crime prevention and criminal justice, international terrorism, and political corruption.
- These goals are pursued through three primary functions: (i) Research, (ii) Guidance and (iii) Support to governments in the adoption and implementation of various crime-, drug-, terrorism-, and corruption-related conventions, treaties and protocols, as well as technical/financial assistance to said governments to face their respective situations and challenges in these fields.
- The office aims long-term to better equip governments to handle drug-, crime-, terrorism-, and corruption-related issues, to maximise knowledge on these issues among governmental institutions and agencies, and also to maximise awareness of said matters in public opinion, globally, nationally and at community level.
- Approximately 90% of the Office's funding comes from voluntary contributions, mainly from governments.

UNODC World Drug Report

- Every year, the UN body United Nations Office on Drugs and Crime (UNODC) publishes **The World Drug Report** with statistics and data on how to tackle the global drug crisis.
- The World Drug Report is aimed at fostering greater international cooperation to counter the impact of the world drug problem on health, governance and security.

- By drugs, the Report refers to substances controlled under international drug control conventions, and their non-medical use.
- The Report, based on data and estimates collected or prepared by Governments, UNODC and other international institutions, attempts to identify trends in the evolution of global illicit drug markets.
- It provides estimates and information on trends in the production, trafficking and use of opium/heroin, coca/cocaine, cannabis and amphetamine-type stimulants.

Highlights of The World Drug Report 2021

- Between 2010-2019, the number of people using drugs increased by 22%, owing in part to an increase in the global population.
- Around 275 million people used drugs worldwide last year, while over 36 million people suffered from drug use disorders.
- Opioids continue to account for the largest burden of disease attributed to drug use.
- A rise in the non-medical use of pharmaceutical drugs was also observed during the coronavirus pandemic.
- In the last 24 years, cannabis potency had increased as much as four times in some parts, even as the percentage of adolescents who perceived the drug as harmful fell by as much as 40%.
- Access to drugs has also become simpler than ever with online sales, and major drug markets on the dark web are now worth some $315 million annually.
- In Asia, China and India are mainly linked to shipment of drugs sold on the 19 major darknet markets analysed over 2011-2020.
- Cannabis dominates drug transactions on Dark web and on clear web involves sale of Narcotic Drugs and Psychotropic Substances (NDPS) and substances used in the manufacture of synthetic drugs.

Impact of Covid-19 on Drug use according to the report

- The Covid-19 crisis has pushed more than 100 million people into extreme poverty, and has greatly exacerbated unemployment and inequalities, as the world lost 255 million jobs in 2020.
- Mental health conditions are also on the rise worldwide. Such socioeconomic stressors have likely accelerated demand for the drugs.
- Drug traffickers have quickly recovered from initial setbacks caused by lockdown restrictions and are operating at pre-pandemic levels once again.
- Contactless drug transactions, such as through the mail, are also on the rise, a trend possibly accelerated by the pandemic.
- Vendors play a cat-and-mouse game with law enforcement by marketing their products as “research chemicals” or advertising “custom synthesis”.

Positive outcome of the pandemic on

- A rise in the use of technology during the pandemic has also triggered innovation in drug prevention and treatment services, through more flexible models of service delivery such as telemedicine, enabling healthcare professionals to reach and treat more patients.
- The pharmaceutical opioids used to treat people with opioid use disorders have become increasingly accessible, as science-based treatment has become more broadly available.

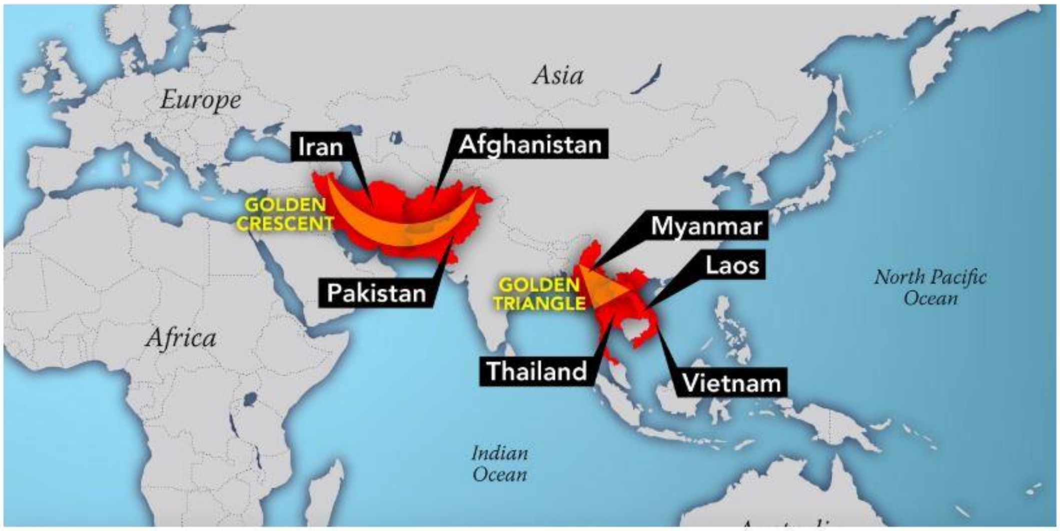
India’s Vulnerability

Golden crescent

- The Golden Crescent is the name given to one of Asia's two principal areas of illicit Opium production, located at the crossroads of central, south and western Asia.
- This space overlaps three nations, Afghanistan, Iran and Pakistan whose mountainous peripheries define the crescent.

Golden triangle

- The Golden Triangle is located in the area where the borders of Thailand, Myanmar and Laos meet at the confluence of the Ruak and Mekong Rivers.
- Along with the Golden Crescent, it is regarded as one of the largest producers of opium in the world since the 1950s until it was overtaken by the Golden Crescent in the early 21st century.



DRONE ATTACKS AT IAF JAMMU STATION

Context:

In a terror attack, two low-intensity explosions left two Indian Air Force (IAF) personnel injured at the Jammu Air Force Station and the devices are suspected to have been dropped and detonated by unmanned aerial vehicles.

Relevance:

GS-III: Internal Security Challenges (Defence Technology), GS-III: Science and Technology, GS-II: Governance (Government Policies & Interventions)

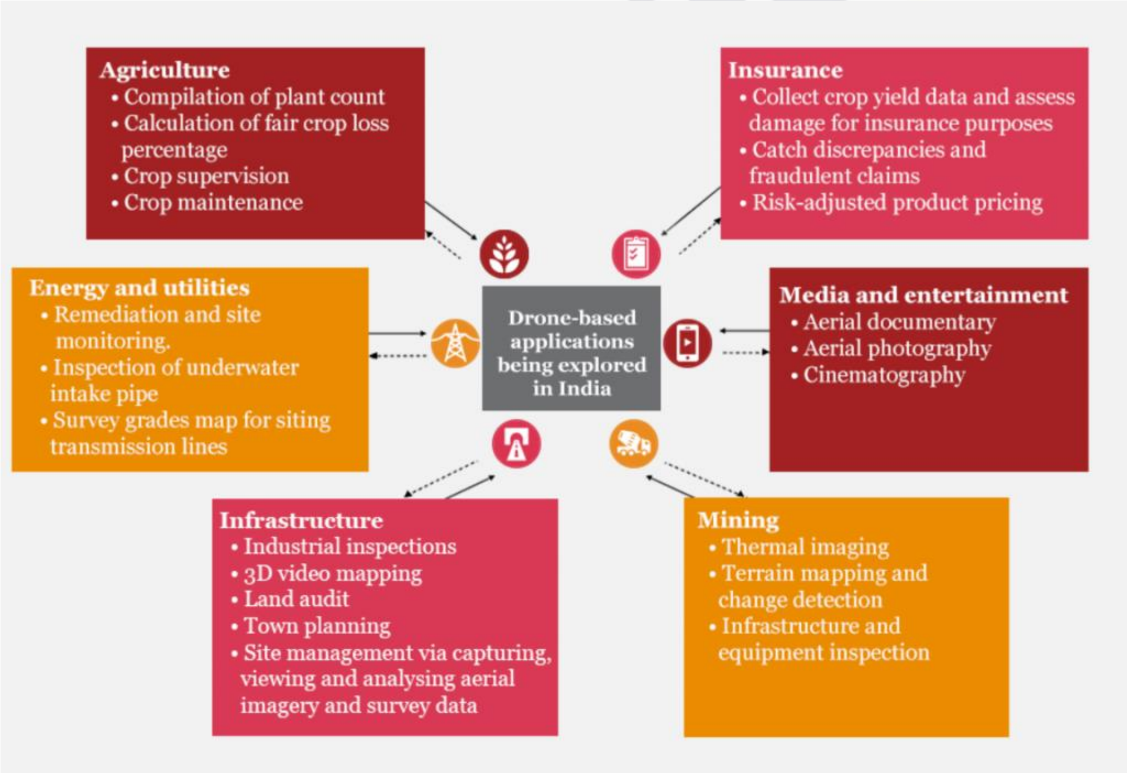
Dimensions of the Article:

1. About Drones
2. Usage of Drones Explored in India
3. Drone Attacks
4. About the Drone attack on Jammu Air Force Station
5. Regulation of Drone usage in India

About Drones

- Drone is a layman terminology for Unmanned Aircraft (UA). There are three subsets of Unmanned Aircraft- Remotely Piloted Aircraft (RPA), Autonomous Aircraft and Model Aircraft.
- Remotely Piloted Aircraft consists of remote pilot station(s), the required command and control links and any other components, as specified in the type design.
- Drones offer low-cost, safe and quick aerial surveys for data collection and are useful for industries such as power, mining, realty, oil and gas exploration, railways and highways. They are also effective in relief and rescue work and in policing.
- DGCA has designed five different categories of drones as: Nano, Micro, Small, Medium, and Large.

Usage of Drones Explored in India



Drone-based applications being explored in India

Agriculture
- Compilation of plant count
- Calculation of fair crop loss percentage
- Crop supervision
- Crop maintenance

Insurance
- Collect crop yield data and assess damage for insurance purposes
- Catch discrepancies and fraudulent claims
- Risk-adjusted product pricing

Energy and utilities
- Remediation and site monitoring.
- Inspection of underwater intake pipe
- Survey grades map for siting transmission lines

Media and entertainment
- Aerial documentary
- Aerial photography
- Cinematography

Infrastructure
- Industrial inspections
- 3D video mapping
- Land audit
- Town planning
- Site management via capturing, viewing and analysing aerial imagery and survey data

Mining
- Thermal imaging
- Terrain mapping and change detection
- Infrastructure and equipment inspection

- Agriculture- Gather data and automate redundant processes to maximize efficiency, to spray medicines, In a process of planting by distributing seed on the land, etc.
- Healthcare- Delivering quick access to drugs, blood, and medical technology in remote areas, transportation of harvested organs to recipients (through drones corridor), etc.

- Disaster Management- Surveillance of disaster-affected areas to assess damage, locate victims, and deliver aid.
- Urban Planning- Instant mapping and survey of the land which has to be developed avoiding congestion and increasing green cover. E.g.: Recently, the Greater Chennai Municipal Corporation (GCMC) became first Municipal Corporation to map Chennai using drones.
- Conservation of Endangered Species- Monitor and track the number of animals.
- Weather Forecasting- Drones can physically follow weather patterns as they develop to understand the environment and imminent weather trends in a better way.
- Waste Management- Identify where the garbage is so that it can be picked up the garbage picking vans. Drones can be used to clean ocean waste as well. UAV like Roomba by RanMarine operates at the vanguard of these initiatives and have helped to clean oceans in past.
- Mining- Drones in mining can be used in volumetric data capturing of ore, rock and minerals storage which is extremely difficult to measure manually.

Drone Attacks

- With the rapid proliferation of drone technology and exponential growth of its global market in recent years, the possibility of a drone attack cannot be ruled out even in the safest cities in the world.
- Drones are becoming security threats particularly in conflict zones where non-state actors are active and have easy access to the technology.
- The primary reason for this proliferation is that drones are relatively cheaper in comparison to conventional weapons and yet can achieve far more destructive results.
- The biggest advantage that comes with using a drone for combat purpose is that it can be controlled from a remote distance and does not endanger any member of the attacking side.
- Drones fly low and therefore cannot be detected by any radar system and this ensures their effective usage by negating chances of detection and neutralization.
- It is this easy-to-procure, easy-to-operate, and proven damage potential that makes it important for any country to equip its forces with anti-drone combat technology.
- These threats aside, what makes combat drones in the hands of non-state actors most dangerous is the threat of them being used deliver weapons of mass destruction.

About the Drone attack on Jammu Air Force Station

- Drones were used for the first time to drop explosive devices, triggering blasts inside the Air Force Station's technical area in Jammu.
- However, over the past two years, drones have been deployed regularly by Pakistan-based outfits to smuggle arms, ammunition and drugs into Indian territory.
- Although the local police suspect that the drones were flown from across the border, it is yet to be established beyond doubt
- Officials said the incident could be an extension of the trend Pakistan-based syndicates using drones to smuggle drugs and weapons into the Indian side, apart from conducting aerial surveillance.
- There have been warnings that Pakistan-based terrorist groups could attempt to target military bases with drones. After the drone attack on Saudi Aramco oil facilities in Eastern Saudi Arabia in September 2019, the armed forces held deliberations on the issue and put in place plans to procure counter-drone capabilities.

Regulation of Drone usage in India

Drone Regulation 1.0

- Drone Regulation 1.0 is a set of guidelines issued by Directorate General of Civil Aviation (DGCA) for commercial use of drones or remotely operated aircraft came into force from 2018.
- Under this regulation, the Digital Sky Platform will enable online registration of pilots, devices, service providers, and NPNT (no permission, no take-off).
- The Digital Sky Platform is a unique unmanned traffic management (UTM) system which is expected to facilitate registration and licensing of drones and operators in addition to giving instant (online) clearances to operators for every flight.
- The airspace has been partitioned into Red Zone (flying not permitted), Yellow Zone (controlled airspace), and Green Zone (automatic permission). The restricted locations are airports, near international border, near coastline, state secretariat complexes strategic locations, military installations.

Drone Regulations 2.0

- Drone regulations 2.0, focuses on three thresholds:
  - BVLOS (Beyond Visual Line of Sight),
  - Delivery of payloads, and
  - Automate the air traffic management to the extent possible.
- The current policy allows one drone pilot for each drone whereas in the next set of regulations, one pilot can operate any number of drones. Under drone regulations 2.0, the drones will be tracked by computers through artificial intelligence.
- However, delivery of products by e-commerce players like Amazon and flying taxis like Uber Elevate are likely to be part of drone regulations 3.0.

Draft Unmanned Aircraft System (UAS) Rules, 2020

- The Draft Unmanned Aircraft System (UAS) Rules, 2020 are a set of rules notified by the government aims to regulate the production, import, trade, ownership, establishment of the drone ports (airports for drones) and operation of unmanned aircraft systems. It also seeks to create a framework for drones use by businesses.
- The Rules state that an authorised manufacturer or importer of drones can sell its devices only to an individual or entity approved by the aviation regulator Directorate General of Civil Aviation (DGCA) and only Nano class drones will be allowed to operate in India in general and only a qualified remote pilot will be permitted to operate heavier drones.
- The DGCA will have the powers to inspect a UAS manufacturing or maintenance facility before granting any authorisation under these rules.
- No UAS shall operate in India unless there is in existence a valid third-party insurance policy to cover the liability that may arise on account of a mishap involving such UAS.
- No UAS should carry any payload except as permitted by the DGCA.
- No person shall drop or project or permit to be dropped from a UAS in motion any object except when specified.
- For owning and using a drone, one has to be at least 18 years old and in the case of companies, the requirement is that their main place of business has to be in India and the chairman and at least two thirds of directors have to be Indian citizens.

IISS REPORT ON INDIA AS A CYBER POWER

Context:

According to a new report by the International Institute for Strategic Studies (IISS) India has made only modest progress in developing its policy and doctrine for cyberspace security despite the geostrategic instability of its region and a keen awareness of the cyber threat it faces.

Relevance:

GS-III: Internal Security Challenges (Cyber Security, Internal security challenges through communication networks, Role of media and social-networking sites in internal security challenges)

Dimensions of the Article:

1. About the report by IISS
2. Highlights of the IISS Study

About the report by IISS

- The report has done a qualitative assessment of cyber power in 15 countries. The 15 countries considered are:
  - Four members of the Five Eyes intelligence alliance – **the United States, the United Kingdom, Canada and Australia** and three cyber-capable allies of the Five Eyes states – **France, Israel and Japan.**
  - Four states at earlier stages in their cyber power development – **India, Indonesia, Malaysia and Vietnam.**
  - Four countries viewed by the Five Eyes and their allies as cyber threats – **China, Russia, Iran and North Korea.**
- The methodology analyses the cyber ecosystem of each state and how it intersects with international security, economic competition and military affairs. The countries are assessed in seven categories:
  - Strategy and doctrine
  - Governance, command and control
  - Core cyber-intelligence capability
  - Cyber empowerment and dependence
  - Cyber security and resilience
  - Global leadership in cyberspace affairs
  - Offensive cyber capability
- The report has divided the 15 states into three tiers of cyber power:
  - First Tier: States with world-leading strengths across all the categories in the methodology. The United States of America is the only country in this tier.
  - Second Tier: States that have world-leading strengths in some of the categories. Australia, Canada, China, France, Israel, Russia and the United Kingdom are in this tier.
  - Third Tier: States that have strengths or potential strengths in some of the categories but significant weaknesses in others. India, Indonesia, Iran, Japan, Malaysia, North Korea and Vietnam are in this tier.

Highlights of the IISS Study

On U.S. vs China

- In advanced cyber technologies and their exploitation for economic and military power, the US is still ahead of China.
- Since 2018, the US and several of its leading allies have agreed to restrict China's access to some Western technologies – By doing so, these countries have endorsed a partial decoupling of the West and China that could potentially impede the latter's ability to develop its own advanced technology.
- Thus, US digital-industrial superiority is likely to last for at least the next ten years.

On India

- India has made only "modest progress" in developing its policy and doctrine for cyberspace security despite the geo-strategic instability of its region and a keen awareness of the cyber threat it faces.
- The military confrontation with China in the disputed Ladakh border area in June 2020, followed by a sharp increase in Chinese activity against Indian networks, has heightened Indian concerns about cyber security, not least in systems supplied by China.
- India has some cyber-intelligence and offensive cyber capabilities but they are regionally focused, principally on Pakistan.
- India's approach towards institutional reform of cyber governance has been "slow and incremental", with key coordinating authorities for cyber security in the civil and military domains established only as late as 2018 and 2019 respectively.
- The strengths of the Indian digital economy include a vibrant start-up culture and a very large talent pool. The private sector has moved more quickly than the government in promoting national cyber security.
- The country is active and visible in cyber diplomacy but has not been among the leaders on global norms, preferring instead to make productive practical arrangements with key states. India is currently aiming to compensate for its weaknesses by building new capability with the help of key international partners – including the US, the UK and France – and by looking to concerted international action to develop norms of restraint.

ITU'S GLOBAL CYBERSECURITY INDEX

Context:

Recently, the Global Cybersecurity Index (GCI) 2020 was released by International Telecommunication Union (ITU) and it ranked India among the top 10 countries.

Relevance:

GS-III: Internal Security Challenges (Cybersecurity, Cyber warfare, Challenges to Internal Security Through Communication Networks)

Dimensions of the Article:

1. The Need, Challenges and Measures regarding Cyber Security in India
2. About the Global Cybersecurity Index (GCI) and ITU
3. Highlights of the Global Cybersecurity Index (GCI)
4. About India's Progress on cyberspace security

About the Global Cybersecurity Index (GCI) and ITU

- The Global Cybersecurity Index (GCI) assessment is done on the basis of performance on five parameters of cybersecurity including legal measures, technical measures, organisational measures, capacity development, and cooperation.
- The GCI is released by the International Telecommunication Union (ITU).
- The International Telecommunication Union is a specialized agency of the United Nations responsible for all matters related to information and communication technologies.
- The ITU promotes the shared global use of the radio spectrum, facilitates international cooperation in assigning satellite orbits, assists in developing and coordinating worldwide technical standards, and works to improve telecommunication infrastructure in the developing world.
- It is also active in the areas of broadband Internet, wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, TV broadcasting, and next-generation networks.
- The ITU was initially aimed at helping connect telegraphic networks between countries. However, with its mandate consistently broadening with the advent of new communications technologies – it adopted its current name in 1934.

Highlights of the Global Cybersecurity Index (GCI)

- The US topped the rankings on key cybersafety parameters and was placed above the UK (United Kingdom) and Saudi Arabia tied on the second position together. Following these 3 countries, Estonia was ranked third (3rd) in the index.
- India has been ranked tenth (10th) and has moved up 37 places. India has also secured the fourth position in the Asia Pacific region, underlining its commitment to cybersecurity.
- The GCI results for India show substantial overall improvement and strengthening under all parameters of the cybersecurity domain.
- India scored a total of 97.5 points from a possible maximum of 100 points, to make it to the tenth position worldwide in the GCI 2020.

About India's Progress on cyberspace security

- India has made only "modest progress" in developing its policy and doctrine for cyberspace security despite the geo-strategic instability of its region and a keen awareness of the cyber threat it faces.
- The military confrontation with China in the disputed Ladakh border area in June 2020, followed by a sharp increase in Chinese activity against Indian networks, has heightened Indian concerns about cyber security, not least in systems supplied by China.
- India has some cyber-intelligence and offensive cyber capabilities but they are regionally focused, principally on Pakistan.
- India's approach towards institutional reform of cyber governance has been "slow and incremental", with key coordinating authorities for cyber security in the civil and military domains established only as late as 2018 and 2019 respectively.
- The strengths of the Indian digital economy include a vibrant start-up culture and a very large talent pool. The private sector has moved more quickly than the government in promoting national cyber security.
- The country is active and visible in cyber diplomacy but has not been among the leaders on global norms, preferring instead to make productive practical arrangements with key states. India is currently aiming to compensate for its weaknesses by building new capability with the help of key international partners – including the US, the UK and France – and by looking to concerted international action to develop norms of restraint.

TRACKING FUGITIVES EVERYWHERE

Context:

Indian law on extradition is spread across the Indian Penal Code as well as various laws pertaining to narcotic drugs, Information Technology, hijacking, and so on.

Relevance:

GS-III: Internal Security Challenges (Various Agencies and other interventions regarding Internal Security and their mandate), GS-II: Polity and Governance (Government Policies and Interventions)

Dimensions of the Article:

1. Legal frameworks in India on Tracking Fugitives
2. Measures taken by the government in this regard

Legal frameworks in India on Tracking Fugitives

- India's legal framework with respect to extradition of fugitives is very robust. Various laws like Extradition Act, Narcotic Drugs and Psychotropic Substances Act, Prevention of Corruption Act, Prevention of Money Laundering act etc. have detailed extradition provisions related to fugitives.
- India also signed bilateral Extradition treaties with 43 countries for extradition of fugitives
- There exists a system of tracking criminals worldwide –through Interpol Notices and the sharing of immigration databases of different countries. There is a separate Interpol wing of CBI to receive red corner notices from Interpol regarding the information about fugitive criminals
- Generally central investigative agencies like CBI, ED or NIA pursue the fugitives vigorously using their expertise and above legal frameworks. However, state police departments have a tendency to close investigations once the accused have absconded. Because (unlike international tracking) there is no coordinated system or database for tracking criminals or wanted persons domestically
- In the absence of such a system, it is relatively easy for criminals from one police station/jurisdiction to melt into the population in any other area, almost undetected

Measures taken by the government in this regard

Crime and Criminal Tracking Network and Systems (CCTNS)

- Crime and Criminal Tracking Network and Systems (CCTNS) is a project initiated in June 2009 which aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing at the Police Station level. This will be done through adoption of principles of e-Governance, and creation of a nationwide networked infrastructure for evolution of IT-enabled state-of-the-art tracking system around "investigation of crime and detection of criminals". CCTNS is a Mission Mode Project (MMP) under the National e-Governance Plan of Govt. of India.

- The Full implementation of the Project with all the new components would lead to a Central citizen portal having linkages with State level citizen portals that will provide a number of citizen friendly services like Police Verification for various purposes including passport verification, reporting a crime including cyber-crime and online tracking of the case progress etc.

National Intelligence Grid (NATGRID)

- NATGRID initially started in 2009 is an online database for collating scattered pieces of information and putting them together on one platform.
- It links at least 10 Central government Intelligence and investigation agencies, such as the Intelligence Bureau, Research and Analysis Wing and others have access to the data on a secured platform.
- NATGRID is exempted from the Right to Information Act, 2005 under sub-section (2) of Section 24.
- The NATGRID enables multiple security and intelligence agencies to access a database related to immigration entry and exit, banking and telephone details, among others, from a common platform.
- The 10 user agencies will be linked independently with certain databases which will be procured from 21 providing organisations including telecom, tax records, bank, immigration etc. to generate intelligence inputs.

RBI BARS MASTERCARD FROM ISSUING NEW CARDS IN INDIA

Context:

The Reserve Bank of India (RBI) imposed restrictions on Mastercard Asia / Pacific Pte. Ltd. from on-boarding new domestic customers (debit, credit or prepaid) onto its card network for non-compliance with the regulator's directions.

According to the RBI, the U.S. card-issuer Mastercard has failed to comply with the local data storage rules announced by the central bank in 2018.

Relevance:

GS-III: Internal Security Challenges (Cyber Security, IT & Computers), GS-III: Indian Economy

Dimensions of the Article:

1. What is the RBI's data localisation policy?
2. What is the need for local data storage?
3. What lies ahead?

What is the RBI's data localisation policy?

- In 2018, the RBI had issued a circular ordering card companies such as Visa, Mastercard, and American Express to store all Indian customer data locally so that the regulator could have "unfettered supervisory access".

- This meant that foreign card companies had to store complete information about transactions made by Indian customers in servers located within India.
- The reason offered by the RBI to back up its data localisation rule was that local storage of consumer data is necessary to protect the privacy of Indian users and also to address national security concerns.

As per the data- localisation norms set by RBI:

- While there is no bar on the processing of payment transactions outside India, the Payment System Operators (PSOs) will have to ensure the data is stored only in India after the processing.
- In case the processing is done abroad, the data should be deleted from the systems abroad and brought back to India not later than the one business day or 24 hours from payment processing, whichever is earlier. The same should be stored only in India.
- The data stored in India can be accessed for handling customer disputes, whenever required.
- The payment system data may be shared with an overseas regulator if required, but with the approval of RBI.
- Some banks, especially foreign, that had been permitted to store the banking data abroad may continue to do so. However, in respect of domestic payment transactions, the data shall be stored only in India.
- The data stored domestically must include:
  1. End-to-end transaction details and information related to payment or settlement transaction collected or processed as part of a payment.
  2. Information such as customer name, mobile number, email, Aadhaar number, PAN number.
  3. Payment sensitive data such as customer and beneficiary account details; payment credentials such as OTP, PIN, Passwords.

What is the need for local data storage?

- Experts believe that customer privacy and national security are genuine concerns that need to be taken seriously. However, many also believe that data localisation rules are too stringent and they could simply be used by governments as tools of economic protectionism.
- For instance, they argue, it may not be strictly necessary for data to be stored locally to remain protected.
- Broadly speaking, formal international laws to govern the storage of digital information across borders may be sufficient to deal with these concerns.
- Governments, however, may still mandate data localisation in order to favour local companies to foreign ones.

Understanding the move

- China, for example, has used its cyber-security laws to discriminate against foreign companies. A similar trend may be playing out in India with the Centre’s emphasis on economic self-sufficiency.
- In 2018, Mastercard had launched a complaint with the U.S. government that Prime Minister Narendra Modi was actively promoting Indian cards like RuPay and that it was affecting the business of foreign card companies.
- Governments may also believe that mandating foreign companies to set up local infrastructure can boost their local economies.

What lies ahead?

- Indian banks that are currently enrolled in the Mastercard network are expected to make alternative arrangements with other card companies.

- The process is expected to take a few months, and their card business is expected to take a significant hit meanwhile.
- The RBI's data localisation policy, as it burdens foreign card companies, may end up favouring domestic card issuers like RuPay. Mastercard owns about one-third of the market share in India, and the RBI's ban is likely to significantly benefit its competitors.
- Similarly, the ban on American Express and Diners Club earlier in 2020 benefited the Indian card network RuPay.
- Some believe that even Visa, a foreign company which dominates card payments in India, may come under regulatory pressure in the near future.
- Thus, the card payments sector may end up being restricted to a few domestic companies, which in turn can lead to reduced competition. This could mean higher costs and lower quality services for customers.

INDIGENOUS PRODUCTION OF DEFENCE EQUIPMENT

Context:

Raksha Rajya Mantri in his reply in the Rajya Sabha said that the 'Make in India' scheme is implemented in defence sector to promote indigenous design, development and manufacture of defence items.

Relevance:

Prelims, GS-III: Internal Security Challenges

Dimensions of the Article:

1. Progress under the Make in India Scheme
2. Initiatives under the AatmaNirbhar Bharat Scheme in defence

Progress under the Make in India Scheme

- Many significant projects including 155mm Artillery Gun system 'Dhanush', Bridge Laying Tank, Thermal Imaging Sight Mark-II for T-72 tank, Light Combat Aircraft 'Tejas', 'Akash' Surface to Air Missile system, Submarine 'INS Kalvari', 'INS Chennai', Anti-Submarine Warfare Corvette (ASWC), Arjun Armoured Repair and Recovery Vehicle, Landing craft utility, etc. have been produced in the country under 'Make in India' initiative of the Government in last few years.
- As per Defence Acquisition Procedure (DAP), priority has been accorded to capital acquisition through 'Buy (Indian-IDDM)', 'Buy (Indian)', 'Buy and Make (Indian)', 'Buy and Make' 'Strategic Partnership Model' or 'Make' categories over Buy (Global) category.

Initiatives under the AatmaNirbhar Bharat Scheme in defence

- The Government has taken several policy initiatives and brought in reforms to promote indigenisation and self-reliance in defence manufacturing, under AatmaNirbhar Bharat Mission in the defence sector.
- Ministry of Defence has notified a **'First Positive Indigenisation list' and '2nd Positive Indigenisation list'** of more than 100 items each in 2021, for which there would be an embargo on the import beyond the timelines indicated against them. This offers a great opportunity to the Indian defence industry to manufacture these items using their own design and development capabilities to meet the requirements of the Indian Armed Forces.

- **SRIJAN portal** to promote indigenisation was launched in 2020 listing over 10 thousand items (which were earlier imported) displayed on the portal for indigenization.
- More than 1500 components & spares have been indigenised in the year 2020-21 as a result of efforts of indigenisation by DPSUs, OFB & SHQs through their own process of indigenisation (In-house, Make-II & Other than Make-II).
- Defence Procurement Procedure (DPP) 2016 has been revised as Defence Acquisition Procedure (DAP)-2020, which is driven by the tenets of Defence Reforms announced as part of 'AatmaNirbhar Bharat Abhiyan'.
- In order to promote indigenous design and development of defence equipment 'Buy (Indian-IDDM (Indigenously Designed, Developed and Manufactured))' category has been accorded top most priority for procurement of capital equipment. The 'Make' Procedure of capital procurement has been simplified. There is a provision for funding up to 70% of development cost by the Government to Indian industry under Make-I category. In addition, there are specific reservations for MSMEs under the 'Make' procedure.
- The Government of India has enhanced FDI in Defence Sector up to 74% through the Automatic Route for companies seeking new defence industrial license and up to 100% by Government Route.
- An innovation ecosystem for Defence titled 'Innovations for Defence Excellence (iDEX)' has been launched in 2018 aimed at creation of an ecosystem to foster innovation and technology development in Defence and Aerospace. iDEX engages Industries including MSMEs, startups, individual innovators, R&D institutes and academia and provide them grants/funding and other support to carry out R&D which has potential for future adoption for Indian defence and aerospace needs.
- Government has notified the 'Strategic Partnership (SP)' Model in May, 2017, which envisages establishment of long-term strategic partnerships with Indian entities through a transparent and competitive process, wherein they would tie up with global Original Equipment Manufacturers (OEMs) to seek technology transfers to set up domestic manufacturing infrastructure and supply chains.
- An Inter-Governmental Agreement (IGA) on 'Mutual Cooperation in Joint Manufacturing of Spares, Components, Aggregates and other material related to Russian/Soviet Origin Arms and Defence Equipment' was signed in 2019 to enhance the After Sales Support and operational availability of Russian origin equipment currently in service in Indian Armed Forces.

SURVEILLANCE REFORM IS THE NEED OF THE HOUR

Context:

- It is worth asking why the government would need to hack phones and install spyware when existing laws already offer impunity for surveillance.
- This unsettling query arises on the basis of reports emerging from a collaborative investigation by journalists from around the world, including from India's The Wire, titled the 'Pegasus Project'.
- Reports say that over "300 verified Indian mobile telephone numbers, including those used by ministers, opposition leaders, journalists, the legal community, businessmen, government officials, scientists, rights activists and others", were targeted using spyware made by the Israeli firm, NSO Group.

Relevance:

- GS Paper 3: Challenges to Internal Security through Communication Networks, Role of Media and Social Networking Sites in Internal Security Challenges, Basics of Cyber Security.

Mains Questions:

1. The proposed legislation related to the personal data protection of citizens fails to consider surveillance. Critically examine. 15 Marks

Dimensions of the Article:

- About Data Protection
- Data protection and India
- Key features of Data protection framework as provided by Sri Krishna Committee:
- Key provisions of Draft Personal Data Protection Bill 2018
- Positive impact of the bill
- Issues with the bill
- Way Forward

About Data Protection

- Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology.
- It aims to strike a balance between individual privacy rights while still allowing data to be used for myriad purposes.
- It is required as the volume of data on internet is expanding exponentially and the spread of new technologies like artificial intelligence internet of things big data poses a threat of abuse and misuse of data.
- Any data protection framework should secure data in its entire life cycle – Data Collection, Data Processing, Data Use, Data Sharing, Data Destruction.
- Several countries have dedicated law for data protection like Japan's Act on Protection of Personal Information. Recently European Union has adopted General Data Protection Regulation 2018.

Data protection and India:

- India has around 40 cr internet users and 25cr social media users who spend significant time online. The average cost for data breach in India has gone up to Rs. 11.9 crore, an increase of 7.9% from 2017.
- Supreme Court in K.S. Puttaswamy case has declared Right to Privacy is a Fundamental right. Hence protecting individual privacy is constitutional duty of the state.
- India does not have any dedicated legal framework for data protection. Presently some acts cover the data protection in general.
    - **Sec 43 A of Information technology act 2000** protects user data from misuse but it is applicable to only corporate entities and not on government agency. Also the rules are restricted to sensitive personal data only — medical history, biometric information among other things.
    - **Other acts like consumer protection Act 2015, copyrights act 1957** among others also attempt to protect the personal information.
- **Various attempts at data protection include:**
    - **In 2011 justice A. P. Shah Panel on data privacy** recommended principles for data protection.
    - **In 2017, a data privacy and protection bill** was tabled in parliament.
    - **Recently Telecom regulatory authority of India (TRAI)** has given its guidelines for data security.
    - **Constitution of Justice B. N. Sri Krishna Committee** to prepare framework for data protection and a draft bill, which submitted its report recently. Based on the framework, the committee has also prepared a Draft Personal Data Protection Bill 2018

Key features of Data protection framework as provided by Sri Krishna Committee:

- **Fiduciary relationship:** The relationship between the individual and the service provider must be viewed as a fiduciary relationship. Therefore, the service provider processing the data is under an obligation to deal fairly with the individual's personal data, and use it for the authorised purposes only.

- **Definition of personal data:** It defined what constituted personal data as data from which an individual may be identified or identifiable, either directly or indirectly. It sought to distinguish personal data protection from the protection of sensitive personal data (e.g., caste, religion, and sexual orientation of the individual), since its processing could result in greater harm to the individual.
- **Consent-based data processing:** except these four cases: o where processing is relevant for the state to discharge its welfare functions o to comply with the law or with court orders in India o when necessitated by the requirement to act promptly (to save a life, for instance) o in employment contracts, in limited situations (such, as where giving the consent requires an unreasonable effort for the employer)
- **Ownership of personal data:** through rights such as right to access, confirm & correct data, right to object data processing and right to be forgotten.
- **Regulatory authority:** to inquire into and take action against any violations of the data protection regime. It may also categorise certain fiduciaries as significant data fiduciaries based on their ability to cause greater harm to individuals which will then be required to undertake additional obligations.
- **Amendments to other laws:** Minimum data protection standards should be adhered to for all data processing in the country authorized under various laws such as Information Technology Act, Census Act etc.

Key provisions of Draft Personal Data Protection Bill 2018

- **Objective:** To balance the growth of the digital economy and use of data as a means of communication between persons with a statutory regime that will protect the autonomy of individuals from encroachments by the state and private entities.
- **Rights of the individual:** The Bill sets out certain rights of the individual. These include: right to obtain confirmation from the fiduciary on whether its personal data has been processed, right to seek correction of inaccurate, incomplete, or out-of-date personal data, and right to have personal data transferred to any other data fiduciary in certain circumstances.
- **Obligations of the data fiduciary:** include implementation of policies with regard to processing of data, maintaining transparency with regard to its practices on processing data, implementing security safeguards (such, as encryption of data), and instituting grievance redressal mechanisms to address complaints of individuals.
- **Data Protection Authority:** to protect interests of individuals, prevent misuse of personal data, and ensure compliance with the Bill.
- **Data localization:** It mandates Data localization of at least one copy in India by data fiduciary.
- **Grounds for processing personal data:** The Bill allows processing of data by fiduciaries if consent is provided except certain circumstances as provided in the framework.
- **Grounds for processing sensitive personal data:** explicit consent of the individual is required for Processing of sensitive personal data except if necessary for any function of Parliament or state legislature, for providing benefits to the individual, or for the compliance of any court judgement.
- **Define Sensitive personal data:** It includes passwords, financial data, genetic data, caste, religious or political beliefs, or any other category of data specified by the Authority.
- **Transfer of data outside India:** Personal data (except sensitive personal data) may be transferred outside India only where the central government has prescribed that transfers to a particular country are permissible, or where the Authority approves the transfer.
- **Exemptions from compliance:** It also gives exemptions for processing of personal data for certain purposes, such as journalistic activities, law enforcement, security of state.
- **Offences and Penalties:** The Authority may levy penalties for various offences by the fiduciary including failure to perform its duties, data processing in violation of the Bill, and failure to comply with directions by the Authority. For example, under the Bill, the fiduciary is required to notify the Authority of any personal data breach which is likely to cause harm to the individual failing which can attract a penalty of the higher of Rs 5 crore or 2% of the worldwide turnover of the fiduciary.

- **Amendments to other laws:** The Bill makes consequential amendments to the Information Technology Act, 2000 and RTI Act to permit nondisclosure of personal information where harm to the individual outweighs public good.
- **Recognises privacy as a fundamental right:** It has provisions to protect personal data as an essential facet of information privacy.
- **Monitoring provisions:** Requirements of conducting Data Protection Impact Assessments, audits and appointing a Data Protection Officer are also included in the bill. There should be a periodic review to check if continued storage of data is necessary.

Positive impact of the bill

- The law will create the balance between the rights of the individual and the public good that comes from the digital economy.
- So far there is no dedicated framework for data protection across country. The proposed law will help create data security architecture and protection of personal information of citizens.
- The bill will put a check on state surveillance of citizens and help them against being victimized by state.

Issues with the bill

- There is no clarity on what kind of security standards should be followed by the data fiduciary.
- There are multiple standards being followed as of now. For example, payment companies which deal with financial data follow PCI-DSS (Payment Card Industry Data Security Standard), health firms follow HIPPA (Health Insurance Portability and Accountability Act) globally etc.
- The regulation may discourage people from using internet and social media as reflected in case of (EU's) General Data Protection Regulation (GDPR) which mandates that every EU citizen's data be stored within the EU. The Facebook and Twitter has noted drop in their revenue and visitors' numbers.
- It does not clearly define the government's accountability when it processes personal data of users without their consent.
- The bill also does not define the time frame for periodic review and frequency of data security audit of companies as well as for reporting of personal data breach at the fiduciary's end.
- **Issues with data localization:**
    - There is no evidence that data localization leads to better privacy and security of data.
    - The industry will have to incur the additional costs given the bill proposes that companies ensure the storage, on a server or data centre located in India, of at least one copy of personal data.
    - Keeping a copy in India does not really guarantee against breach of security or privacy. There have been cases of government beneficiaries' data residing on servers in India being published, going against Aadhaar Act.
- **The bill asks to replace sec 8(1) (j) of RTI act 2005** which may pose a threat to denial of information on the vague grounds of loss of reputation, mental injuries and will render the Act ineffective in securing access to public records pertaining to public servants.
- The exemption on the ground of security of state may be too broad and may lead to surveillance and systematic access to citizens' data by the state.

Way Forward:

- Surveillance reform is the need of the hour in India. Not only are existing protections weak but the proposed legislation related to the personal data protection of Indian citizens fails to consider surveillance while also providing wide exemptions to government authorities.

- When spyware is expensive and interception is inefficient, the individuals surveilled will be shortlisted by priority and perceived threat level to the existing regime.
- But as spyware becomes more affordable and interception becomes more efficient, there will no longer be a need to shortlist individuals. Everyone will be potentially subject to state-sponsored mass surveillance. The only solution is immediate and far-reaching surveillance reform.

PEGASUS SPYWARE ISSUE IN INDIA EXPLAINED FOR UPSC

Context:

A number of reports on **Pegasus Spyware in India** indicate that at least 1,000 Indian phone numbers are in a list of potential targets of surveillance using the Pegasus spyware. An Israeli company, the NSO group, sells the Pegasus spyware to “vetted governments”.

The evidence is strong that Indian citizens were indeed targets of a vicious and uncivil surveillance campaign by a government entity, Indian or foreign.

Relevance:

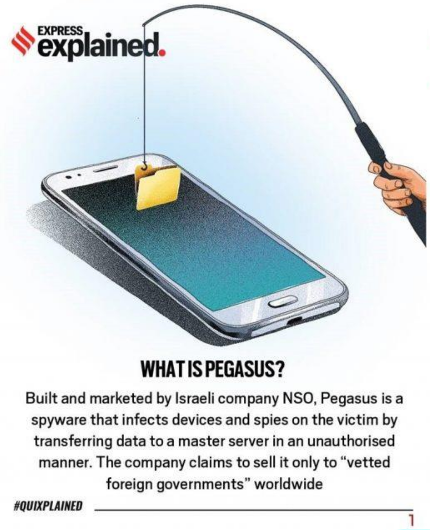
GS-III: Internal Security Challenges (Basics of Cyber Security; Role of media and social networking sites in internal security challenges; Internal security challenges through communication networks), GS-II: Polity and Governance (Constitutional Provisions, Fundamental Rights, Important Judgements)

Dimensions of the Article:

1. About the Pegasus Project
2. How dangerously compromising is Pegasus?
3. What is a spyware and what are other similar types of Cyber Attacks?
4. Pegasus in the news in the past
5. About the Pegasus Attacks in India
6. Issues in the past regarding Government’s surveillance
7. Legislations on Surveillance
8. K.S. Puttaswamy judgment, 2017 regarding Surveillance
9. Various recommendations in the past regarding Surveillance

About the Pegasus Project

- Pegasus is a type of malware classified as a spyware. Pegasus enables law enforcement and intelligence agencies to remotely and covertly extract” data “from virtually any mobile devices”
- The Spyware Pegasus can gain access to devices without the knowledge of users. After this, it can gather personal information and relay it back to whoever is using the software to spy.
- A zero-click attack helps spyware like Pegasus gain control over a device without human interaction or human error. Pegasus can infect a device without the target’s engagement or knowledge. So, all awareness about how to avoid a phishing attack or which links not to click are pointless.
- The Israeli firm NSO Group (set up in 2010) developed the Pegasus spyware. Since then, NSO’s attack capabilities have become more advanced.



EXPRESS explained.

WHAT IS PEGASUS?

Built and marketed by Israeli company NSO, Pegasus is a spyware that infects devices and spies on the victim by transferring data to a master server in an unauthorised manner. The company claims to sell it only to “vetted foreign governments” worldwide

#QUIXPLAINED 1

EXPRESS explained.

HOW DOES IT WORK?

- Pegasus, in the very basic form, can infect devices that are connected to the internet. Some updated versions, experts claim, can also infect phones even without the victim clicking on any links or messages
- Most spyware and stalkerware apps disguise themselves as anti-theft applications that can be used to track stolen or lost devices. While viruses and malware can be detected by anti-virus software, spyware and stalkerware apps disguise themselves as useful and send out stolen data to central servers without the knowledge of the users

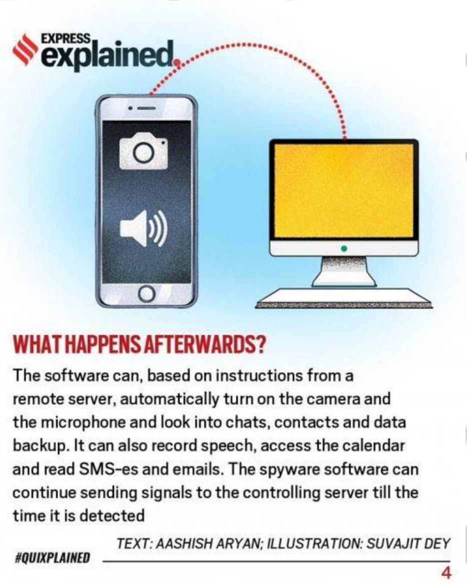
#QUIXPLAINED 2

EXPRESS explained.

HOW DOES IT INFECT A DEVICE?

- For spyware apps, the easiest method is to disguise the spying code inside the unauthorised versions of premium apps. On the other hand, stalkerware apps seek explicit permissions at the time of their installation
- Such stalkerware applications, once installed, hide themselves in the background, from where they continue functioning. Similarly, Pegasus infects phones and computers of victims either through vulnerabilities in most commonly used apps such as WhatsApp, iMessage, or SMS. The software tries to gain “root privileges” so that they can become device administrators

#QUIXPLAINED 3



EXPRESS explained.

WHAT HAPPENS AFTERWARDS?

The software can, based on instructions from a remote server, automatically turn on the camera and the microphone and look into chats, contacts and data backup. It can also record speech, access the calendar and read SMS-es and emails. The spyware software can continue sending signals to the controlling server till the time it is detected

TEXT: AASHISH ARYAN; ILLUSTRATION: SUVAJIT DEY

#QUIXPLAINED 4

How dangerously compromising is Pegasus?

- Upon installation, Pegasus contacts the attacker’s command and control (C&C) servers to receive and execute instructions and send back the target’s private data. This data can include passwords, contact lists, text messages, and live voice calls (even those via end-to-end-encrypted messaging apps).
- The attacker can control the phone’s camera and microphone, and use the GPS function to track a target.
- To avoid extensive bandwidth consumption that may alert a target, Pegasus sends only scheduled updates to a C&C server.
- The spyware can evade forensic analysis and avoid detection by anti-virus software. Also, the attacker can remove and deactivate the spyware, when and if necessary.

What is a spyware (Like Pegasus Spyware in India) and what are other similar types of Cyber Attacks?

What is Malware?

- Malware is short for malicious software. Malware is a catch-all term for various softwares including viruses, adware, spyware, browser hijacking software, and fake security software.
- Ransomware, Spyware, Worms, viruses, and Trojans are all varieties of malware.

Types of Malware

- **Viruses** which are the most commonly-known form of malware and potentially the most destructive. They can do anything from erasing the data on your computer to hijacking your computer to attack other systems. Viruses can also send spam, or host and share illegal content.
- **Worm** is a type of malware that spreads copies of itself from computer to computer. Additionally, it can replicate itself without any human interaction. Also, it does not need to attach itself to a software program in order to cause damage.
- **Trojan** is a type of malware that is often disguised as legitimate software to be used by cyber-thieves and hackers trying to gain access to systems.
- **Spyware** collects your personal information and passes it on to interested third parties without your knowledge or consent. Spywares can also install Trojan viruses.
- **Ransomware** is malware that employs encryption to hold a victim’s information at ransom.
- **Adware** displays pop-up advertisements when you are online.
- **Fake security software** poses as legitimate software to trick you into opening your system to further infection, providing personal information, or paying for unnecessary or even damaging “clean ups”.
- **Browser hijacking software** changes your browser settings (such as your home page and toolbars), displays pop-up ads and creates new desktop shortcuts. Additionally, it can also relay your personal preferences to interested third parties.

Pegasus Spyware in India in the news in the past

- Researchers discovered the earliest version of Pegasus in 2016. This version infected phones through what is called spear-phishing – text messages or emails that trick a target into clicking on a malicious link.
- In 2019, WhatsApp blamed the NSO Group for exploiting a vulnerability in its video-calling feature which secretly transmitted malicious code in an effort to infect the victim’s phone with spyware without the person even having to answer the call.
- In 2020, a report showed government operatives used Pegasus to hack phones of employees at Al Jazeera and Al Araby.

About the Recent Pegasus Spyware Attacks in India

- Human Rights activists, journalists and lawyers around the world have been targeted with phone malware sold to authoritarian governments by an Israeli surveillance firm. Indian ministers, government officials and opposition leaders also figure in the list.
- In India, several opposition leaders including Rahul Gandhi were on the leaked potential targets’ list.
- Smartphones of Politicians, Journalists were hacked for gathering confidential information.
- This is the first time in the history of this country that all pillars of our democracy — judiciary, parliamentarians, media, executives and ministers — have been spied upon.
- The Indian government has denied any wrong doing or carrying out any unauthorised surveillance. However, the government has not confirmed or denied whether it has purchased or deployed Pegasus spyware.

Issues in the past regarding Government's surveillance

- In 2012 in Himachal Pradesh, the new government raided police agencies and recovered over a lakh phone conversations of over a thousand people, mainly political members, and many senior police officials, including the Director General of Police (DGP), who is legally responsible for conducting phone taps in the State.
- In 2013, India's current Home Minister Amit Shah was embroiled in a controversy dubbed "Snoopgate", with phone recordings alleged to be of him speaking to the head of an anti-terrorism unit to conduct covert surveillance without any legal basis (as there was no order signed by the State's Home Secretary which is a legal necessity for a phone tap).
- The UPA government in 2009 said that the CBDT had placed a PR professional, under surveillance due to fears of her being a foreign spy. Later on, the CBDT did not prosecute the person.

Such examples of unlawful surveillance which seem to be for political and personal gain are antithetical to the basic creed of democracy. Consequently, they also bring up the need for ensuring that the surveillance is necessary and proportionate.

Legislations on Surveillance

- The laws authorising interception and monitoring of communications are:
  1. Section 92 of the Criminal Procedure Code (CrPC)
  2. Rule 419A of the Telegraph Rules, and
  3. The rules under Sections 69 and 69B of the IT Act

Who can conduct Surveillance?

A limited number of agencies are provided powers to intercept and monitor.

- In 2014, the Ministry of Home Affairs told Parliament that nine central agencies and the DGPs of all States and Delhi were empowered to conduct interception under the Indian Telegraph Act.
- In 2018, 9 central agencies and 1 State agency were authorised to conduct intercepts under Section 69 of the IT Act.
- The Intelligence Organisations Act, which restricts the civil liberties of intelligence agency employees, only lists four agencies. However, the RTI Act lists 22 agencies as "intelligence and security organisations established by the central government" that are exempt from the RTI Act.

K.S. Puttaswamy judgment, 2017 regarding Surveillance

- The K.S. Puttaswamy judgment, 2017, made it clear that any invasion of privacy could only be justified if it satisfied three tests:
  1. The restriction must be by law;
  2. It must be necessary (only if other means are not available) and proportionate (only as much as needed);
  3. It must promote a legitimate state interest (e.g., national security).
- The judgement held that privacy concerns in this day and age of technology can arise from both the state as well as non-state entities. As such, a claim of violation of privacy lies against both of them.
- The Court also held that informational privacy in the age of the internet is not an absolute right and when an individual exercises his right to control over his data, it may lead to the violation of his privacy to a considerable extent.

- It was also laid down that the ambit of Article 21 is ever-expanding due to the agreement over the years among the Supreme Court judges. A plethora of rights have been added to Article 21 as a result.
- The court stated that Right to Privacy is an inherent and integral part of Part III of the Constitution that guarantees fundamental rights. The conflict in this area mainly arises between an individual's right to privacy and the legitimate aim of the government to implement its policies. Thus, we need to maintain a balance while doing the same.

Various recommendations in the past regarding Surveillance

- In 2010, then Vice-President called for a legislative basis for India's agencies and the creation of a standing committee of Parliament on intelligence to ensure that they remain accountable and respectful of civil liberties.
- The Cabinet Secretary in a note on surveillance in 2011 held that the Central Board of Direct Taxes having interception powers was a continuing violation of a 1975 Supreme Court judgment on the Telegraph Act.
- In 2013, the Ministry of Defence-funded think-tank published a report which recommended that the intelligence agencies in India must be provided a legal framework for their existence and functioning; their functioning must be under Parliamentary oversight and scrutiny.
- In 2018, the Srikrishna Committee on data protection noted that post the K.S. Puttaswamy judgment, most of India's intelligence agencies are "potentially unconstitutional". This is because they are not constituted under a statute passed by Parliament — the National Investigation Agency being an exception.

INDIA AND 26 BILATERAL PACTS TO FIGHT DRUG TRAFFICKING

Context:

According to a Ministry of Home Affairs (MHA) reply in the Lok Sabha – India has signed 26 bilateral pacts, 15 memoranda of understanding and two agreements on security cooperation with different countries for combating the drug trafficking problem.

Relevance:

GS-III: Internal Security Challenges (Organized Crime and Terrorism), GS-II: International Relations (Important International Agreements and Treaties affecting India's Interests), GS-I: Indian Society, GS-II: Social Justice (Health related issues, Government Policies and Interventions)

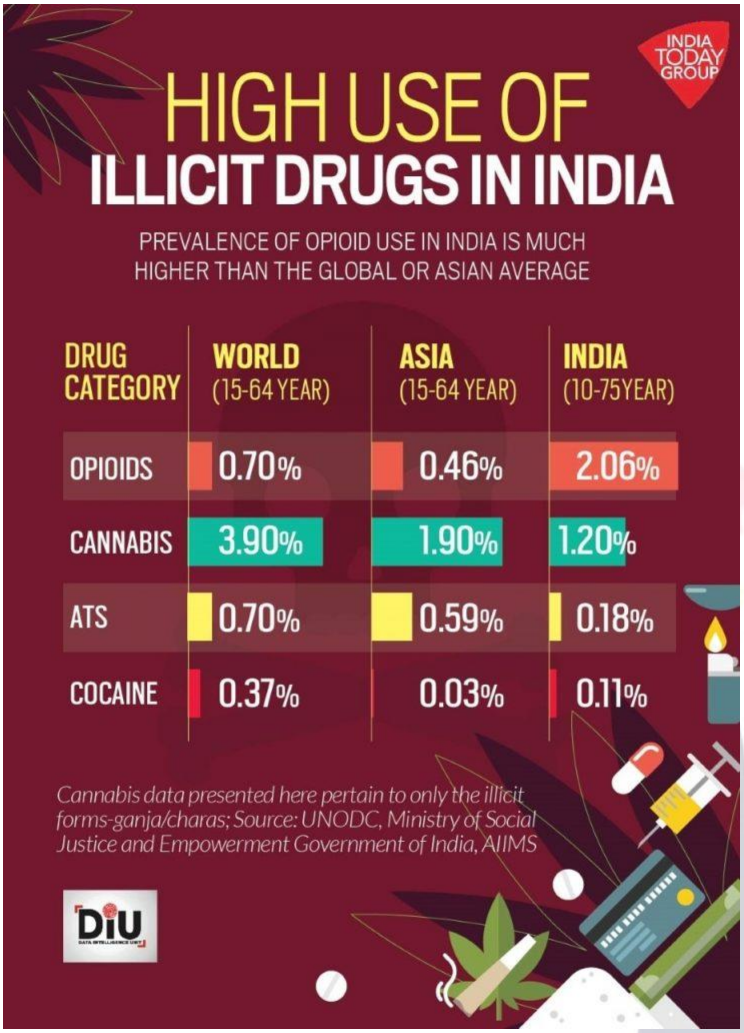
Dimensions of the Article:

1. Data on Drug Abuse problem in India: Report by AIIMS
2. India's Vulnerability
3. Data Regarding Drug Abuse in the world
4. Drug Abuse problem worsening due to Covid-19 Pandemic
5. India's International Coordination to fight Drug Abuse
6. Narcotic Drugs and Psychotropic Substances Act, (NDPS)
7. India's Anti-Drug Action Plan for 2020-21

8. Other Steps Taken in India

Data on Drug Abuse problem in India: Report by AIIMS

- In terms of users, India’s illicit drug markets are mostly dominated by cannabis and opioids. Alcohol is the most abused substance in India.
- The use of illegal cannabis in India is much lower than the global average – less than one-third. However, opioid use is three times higher than the worldwide average.
- Cannabis in the form of bhang is legal in India, whereas its other forms – ganja (marijuana) and charas (hashish) – are illegal. Opioids are sold as opium (doda, phukki or poppy husk), heroin (brown sugar, smack) and pharma opioids.
- India reported more than 2 crore opioid users in 2018, which was a five-fold jump in 14 years.
- The maximum growth was reported in consumption of heroin.
- India has more than 1 crore sedative users, the maximum number being in Uttar Pradesh, followed by Maharashtra, Punjab and Andhra Pradesh.
- Some drug users, relatively less in number, are taking the inhalational route and psychoactive drugs.
- Inhalants are the only drug category prevalent among children. More than 1% of children consume inhalants. Nearly 18 lakh adults and 4.6 lakh children are in the badly-addicted category.
- Cocaine is the less popular illicit drug in India with more than 10 lakh users. Being pretty expensive, it is mostly used by the well-off.
- Another drug category, hallucinogens, is used in limited circles, with over 12 lakh users in this category, of which one-third are in the harmful or dependent category.
- Findings show there are an estimated 8.5 lakh people who inject drugs (PWID) in India. Almost half of them inject heroin, while the same proportion is using injectable pharmaceutical opioids.



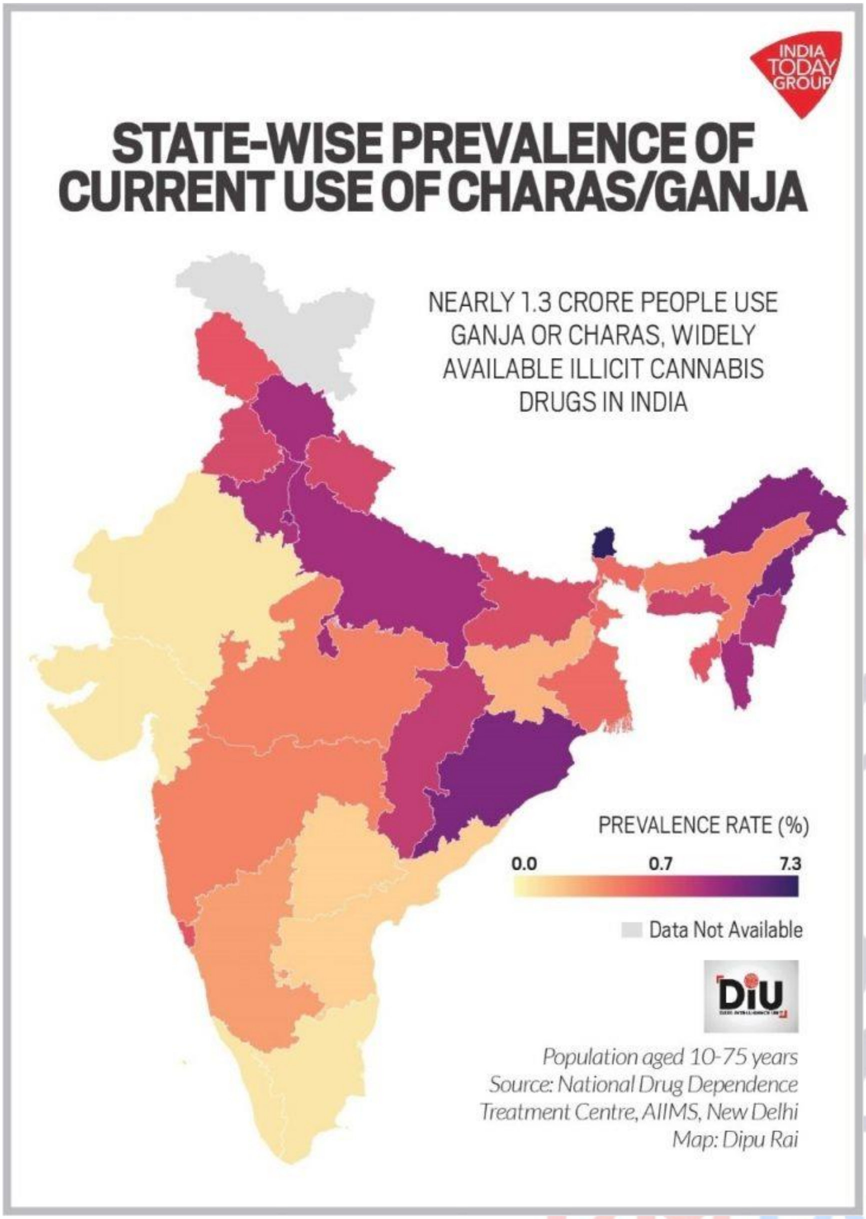
INDIA TODAY GROUP

HIGH USE OF ILLICIT DRUGS IN INDIA

PREVALENCE OF OPIOID USE IN INDIA IS MUCH HIGHER THAN THE GLOBAL OR ASIAN AVERAGE

DRUG CATEGORY	WORLD (15-64 YEAR)	ASIA (15-64 YEAR)	INDIA (10-75YEAR)
OPIOIDS	0.70%	0.46%	2.06%
CANNABIS	3.90%	1.90%	1.20%
ATS	0.70%	0.59%	0.18%
COCAINE	0.37%	0.03%	0.11%

Cannabis data presented here pertain to only the illicit forms-ganja/charas; Source: UNODC, Ministry of Social Justice and Empowerment Government of India, AIIMS

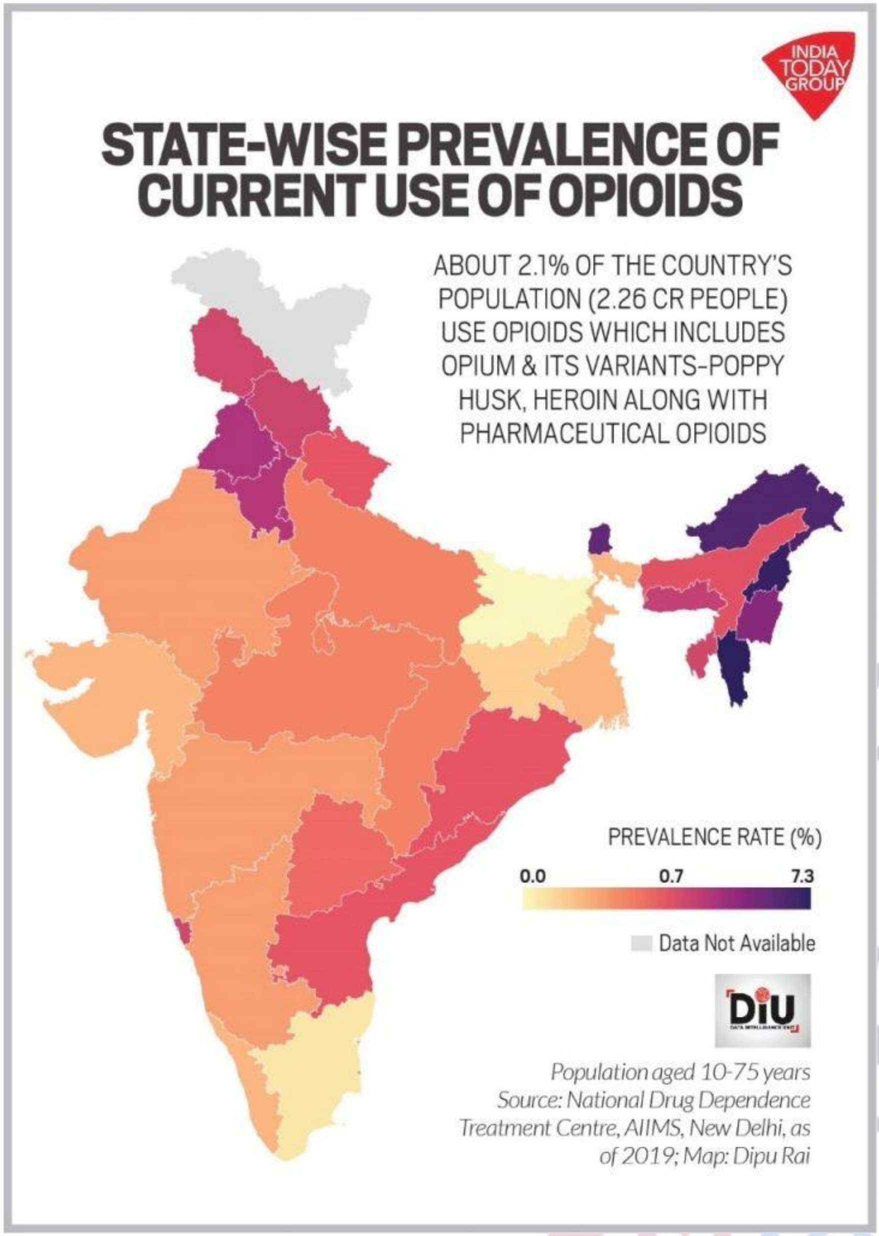


INDIA TODAY GROUP

STATE-WISE PREVALENCE OF CURRENT USE OF CHARAS/GANJA

NEARLY 1.3 CRORE PEOPLE USE GANJA OR CHARAS, WIDELY AVAILABLE ILLICIT CANNABIS DRUGS IN INDIA

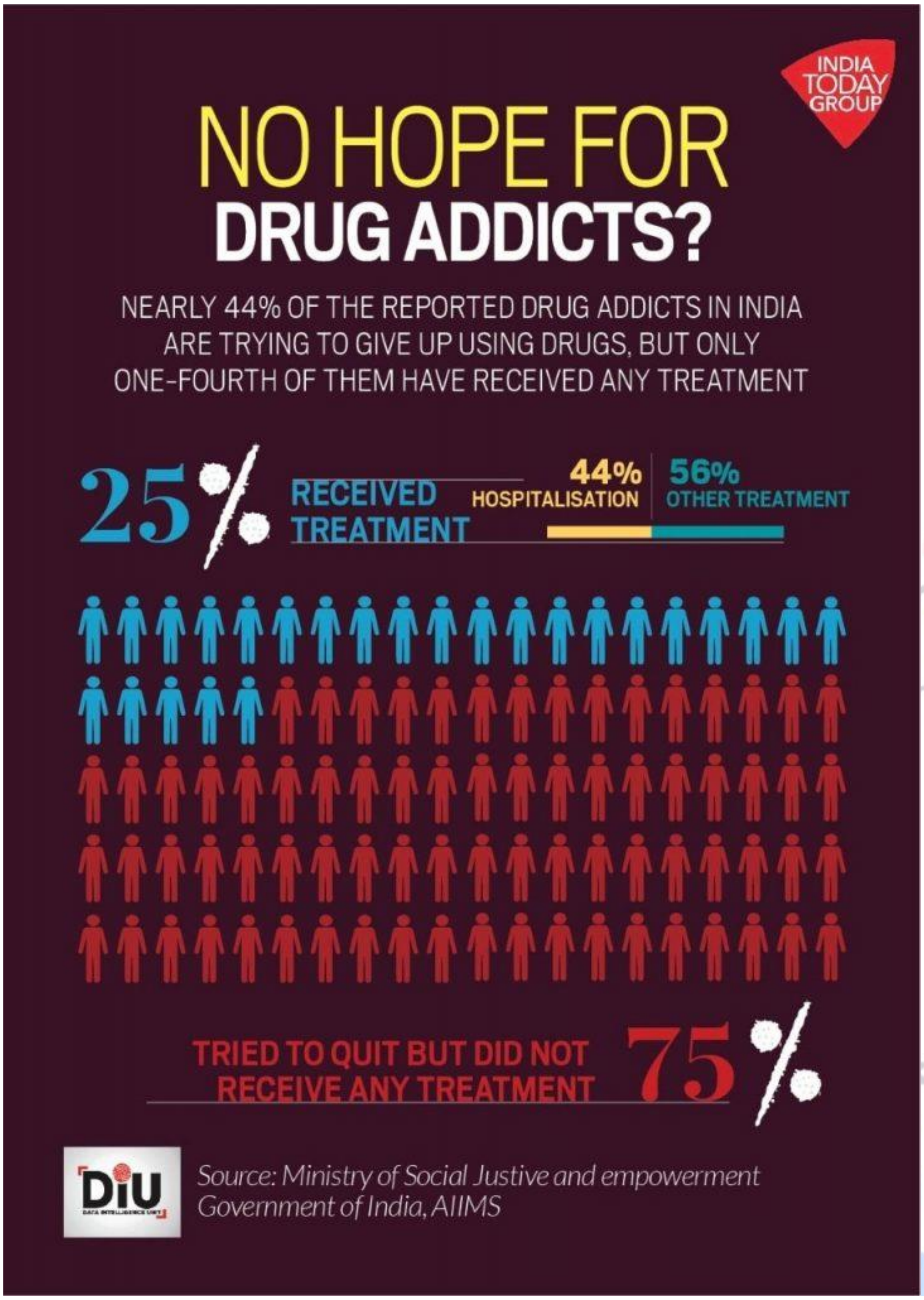
Population aged 10-75 years
Source: National Drug Dependence Treatment Centre, AIIMS, New Delhi
Map: Dipu Rai



STATE-WISE PREVALENCE OF CURRENT USE OF OPIOIDS

ABOUT 2.1% OF THE COUNTRY'S POPULATION (2.26 CR PEOPLE) USE OPIOIDS WHICH INCLUDES OPIUM & ITS VARIANTS-POPPY HUSK, HEROIN ALONG WITH PHARMACEUTICAL OPIOIDS

Population aged 10-75 years
Source: National Drug Dependence Treatment Centre, AIIMS, New Delhi, as of 2019; Map: Dipu Rai



NO HOPE FOR DRUG ADDICTS?

NEARLY 44% OF THE REPORTED DRUG ADDICTS IN INDIA ARE TRYING TO GIVE UP USING DRUGS, BUT ONLY ONE-FOURTH OF THEM HAVE RECEIVED ANY TREATMENT

Source: Ministry of Social Justive and empowerment Government of India, AIIMS

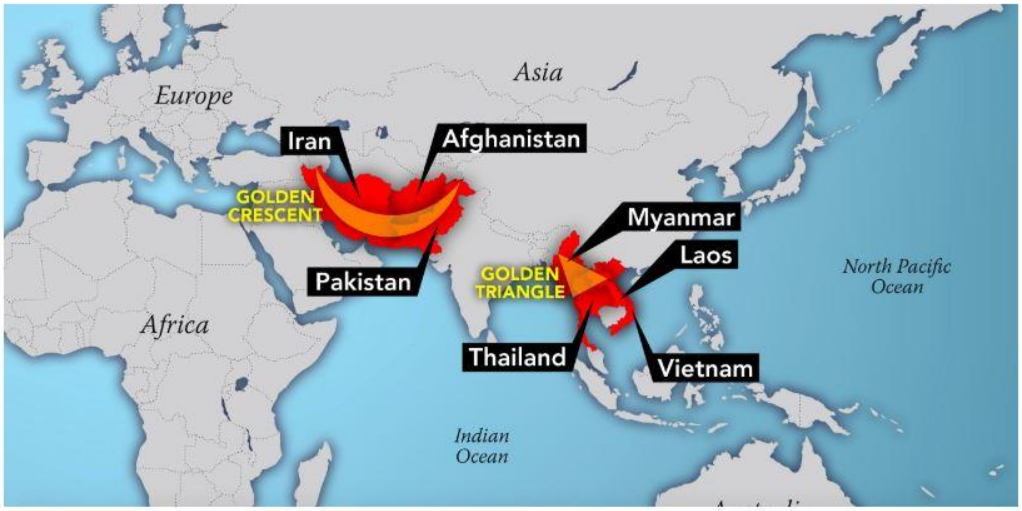
India's Vulnerability

Golden crescent

- The Golden Crescent is the name given to one of Asia's two principal areas of illicit Opium production, located at the crossroads of central, south and western Asia.
- This space overlaps three nations, Afghanistan, Iran and Pakistan whose mountainous peripheries define the crescent.

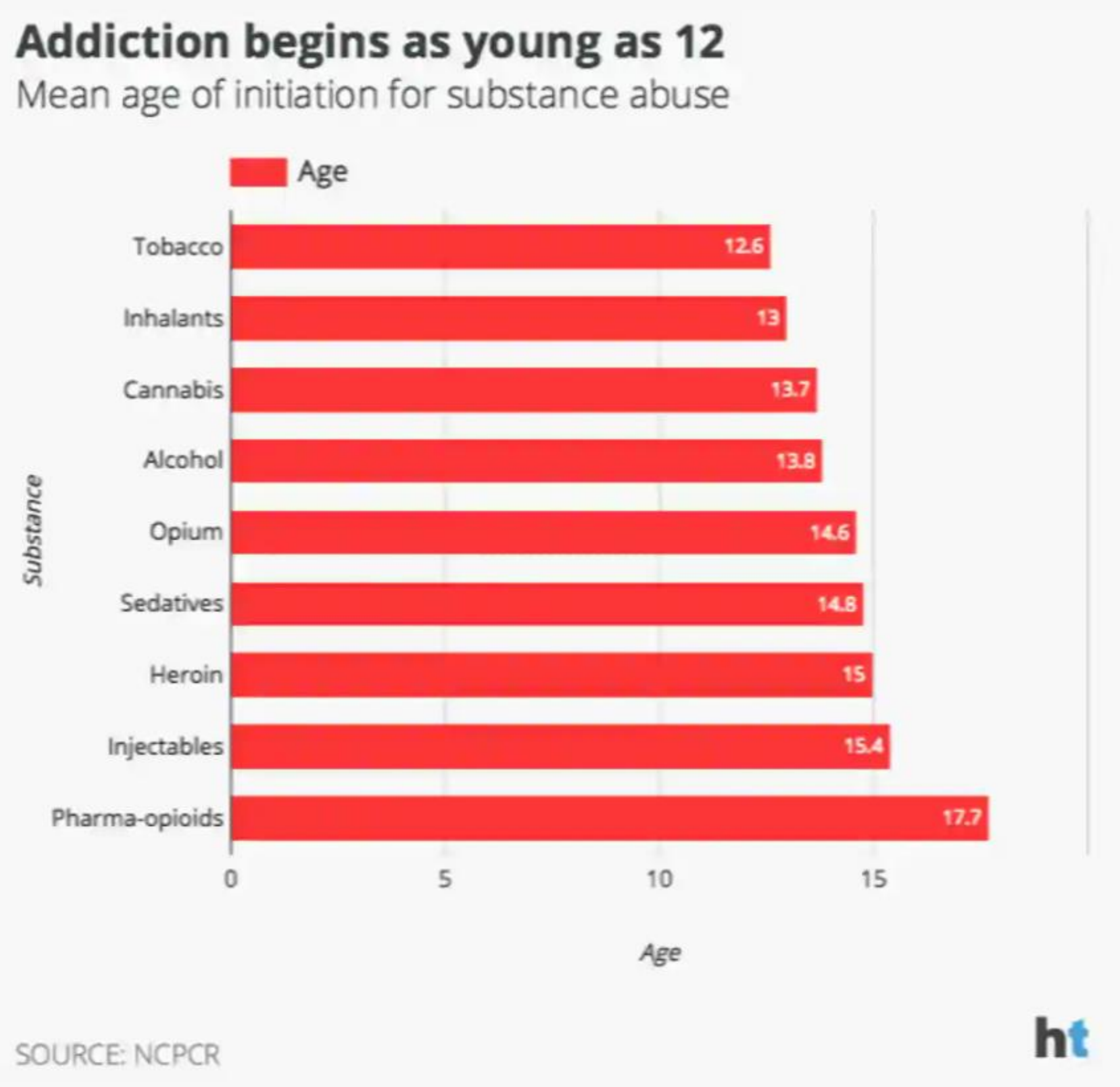
Golden triangle

- The Golden Triangle is located in the area where the borders of Thailand, Myanmar and Laos meet at the confluence of the Ruak and Mekong Rivers.
- Along with the Golden Crescent, it is regarded as one of the largest producers of opium in the world since the 1950s until it was overtaken by the Golden Crescent in the early 21st century.



Data Regarding Drug Abuse in the world

- One out of three drug users is a woman but women represent only one out of five people in treatment.
- People in prison settings, minorities, immigrants and displaced people also face barriers to treatment due to discrimination and stigma.
- Number of people using drugs in 2018 increased by 30% from 2009, with adolescents and young adults accounting for the largest share of users.
- While the increase reflects population growth and other factors, the data nevertheless indicate that illicit drugs are more diverse, more potent and more available.
- At the same time, more than 80% of the world’s population, mostly living in low- and middle-income countries, are deprived of access to controlled drugs for pain relief and other essential medical uses.



SOURCE: NCPCR

Drug Abuse problem worsening due to Covid-19 Pandemic

- The economic downturn caused by the global pandemic may drive more people to substance abuse or leave them vulnerable to involvement in drug trafficking and related crime.
- In the global recession that followed the 2008 financial crisis, drug users sought out cheaper synthetic substances and patterns of use shifted towards injecting drugs, while governments reduced budgets to deal with drug-related problems.
- All over the world, the risks and consequences of drug use are worsened by poverty, limited opportunities for education and jobs, stigma and social exclusion, which in turn helps to deepen inequalities, moving us further away from achieving the Sustainable Development Goals (SDGs).

India's International Coordination to fight Drug Abuse

- The Narcotics Control Bureau (NCB) coordinated with various international organisations for sharing information and intelligence to combat transnational drug trafficking.
- The Various International Organizations that the NCB works with include:

1. The SAARC Drug Offences Monitoring Desk; Brazil, Russia, India, China and South Africa (BRICS);

2. Colombo Plan: A regional organisation of 27 countries designed to strengthen economic and social development of member countries in the Asia-Pacific region;
3. Association of Southeast Asian Nations (ASEAN) and ASEAN Senior Officials on Drug Matters (ASOD);
4. Bay of Bengal Initiative For Multi-Sectoral Technical and Economic Co-Operation (BIMSTEC);
5. The United Nations Office on Drugs and Crime (UNODC);
6. The International Narcotics Control Board (INCB).

- For coordination among various Central and State agencies, **the Narco Coordination Centre (NCORD)** mechanism was set up by the MHA in year 2016 for effective drug law enforcement. This NCORD system has been restructured into a four-tier scheme up to district level on July 29, 2019, for better coordination.

Narcotic Drugs and Psychotropic Substances Act, (NDPS)

- The Narcotic Drugs and Psychotropic Substances Act, 1985, commonly referred to as the NDPS Act prohibits a person the production/manufacturing/cultivation, possession, sale, purchasing, transport, storage, and/or consumption of any narcotic drug or psychotropic substance.
- India had no legislation regarding narcotics until 1985.
- The Act is designed to fulfill India's treaty obligations under the Single Convention on Narcotic Drugs, Convention on Psychotropic Substances, and United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.
- The Narcotics Control Bureau is a statutory body that was set up under the act with effect from 1986.

India's Anti-Drug Action Plan for 2020-21

- The annual Anti-Drug Action Plan for 2020-21 for 272 districts was launched by the Ministry of Social Justice and Empowerment in June 2020.
- The action plan for 2020-21 included awareness generation programmes, identification of drug-dependent population, focus on treatment facilities and capacity-building for service-providers to curb drug abuse and alcoholism.
- De-addiction Facilities would be set up in the "most affected" 272 districts identified by the Narcotics Control Bureau focussing on building up treatment and de-addiction facilities and giving emphasis on reaching the youth and high-risk population.
- Integrated Rehabilitation Centre for Addicts (IRCAs) funded by the Ministry would reach out to communities to help those affected by drug addiction.

Other Steps Taken in India

1. **Narco-Coordination Centre (NCORD):** Government had constituted Narco Coordination Centre (NCORD), the mechanism under Director General (DG), Narcotics Control Bureau (NCB), in order to have effective coordination among all the drug law enforcement agencies and other stakeholders, and also to provide a common platform for discussions on drug-trafficking related issues.
2. **National Fund for Control of Drug Abuse:** The government has constituted a fund called "National Fund for Control of Drug Abuse" to meet the expenditure incurred in connection with combating illicit traffic in Narcotic Drugs; rehabilitating addicts, and educating the public against drug abuse, etc.
3. **Seizure Information Management System (SIMS):** SIMS is a step taken towards digitization of pan-India drug seizure data in 2019 for all the drug law enforcement agencies under the mandate of Narcotics Drugs and Psychotropic Substances Act (NDPS). Narcotics Control Bureau (NCB) was provided with the funds for developing SIMS which will create a complete online database of drug offences and offenders.

ESSENTIAL DEFENCE SERVICES BILL, 2021

Context:

Recently, the Minister of State for Defence introduced the Essential Defence Services Bill in the Lok Sabha.

Relevance:

GS-III: Internal Security Challenges, GS-II: Polity and Governance (Government Policies and Interventions)

Dimensions of the Article:

1. What is the Essential Defence Services Bill?
2. Understanding Strikes and the punishments in this context:
3. Industrial Disputes Act 1947

What is the Essential Defence Services Bill?

- Essentially, the Essential Defence Services Bill is aimed at preventing the staff of the government-owned ordnance factories from going on a strike.
- It will amend the Industrial Disputes Act, 1947 to include essential defence services under public utility services.
- The Bill introduced recently, mentioned that that it is meant to "provide for the maintenance of essential defence services so as to secure the security of nation and the life and property of public at large".
- The Government said that since it is "essential that an uninterrupted supply of ordnance items to the armed forces be maintained for the defence preparedness of the country and the ordnance factories continue to function without any disruptions, it was felt necessary that the Government should have power to meet the emergency created by such attempts and ensure the maintenance of essential defence services **in public interest or interest of the sovereignty and integrity of India or security of any State or decency or morality".**

These are the lines along which reasonable restrictions can be imposed by law (imposed only by authority of law and NOT by executive action alone), on the Fundamental Rights Guaranteed under Article 19.

1. On Freedom of Speech and Expression:
   - Sovereignty and integrity of India,
   - The security of the State,
   - Friendly relations with foreign States,
   - Public order,
   - Decency or morality or
   - In relation to Contempt of Court,
   - Defamation or
   - Incitement to an offence.
2. On Freedom to Assemble Peaceably and Without Arms:
   - Sovereignty and integrity of India or
   - Public order
3. On Freedom to Form Associations or Unions:
   - Sovereignty and integrity of India
   - Public order or

- Morality

4. On Freedom to Move Freely throughout the Territory of India:
    - Interests of the General Public
    - Protection of the Interests of any Scheduled Tribe
5. On Freedom to Reside and Settle in any part of the territory of India:
    - Interests of the General Public
    - Protection of the Interests of any Scheduled Tribe
6. On Freedom to Practice any Profession, or to Carry on any Occupation, Trade or Business:
    - Interests of the general public

What does the new bill allow the government to do?

- The Government can declare any service as an essential defence service if its cessation would affect the:
- Production of defence equipment or goods.
- Operation or maintenance of industrial establishments or units engaged in such production.
- Repair or maintenance of products connected with defence.
- Government may prohibit strikes, lock-outs, and lay-offs in units engaged in essential defence services.
- It may issue such an order, if necessary, in the interest of sovereignty and integrity of India, security of any state, public order, public, decency and morality.

Understanding Strikes and the punishments in this context:

- Strikes are defined as a cessation of work by a body of persons acting together and they may include: Mass leaves, coordinated refusals of any number of persons to work, Refusal to work overtime where it is absolutely necessary for essential services to continue, or any other such activity that disrupts work in essential services (in this case, defence).
- Employers violating the prohibition order through illegal lock-outs or lay-offs will be punished with up to one year imprisonment or Rs 10,000 fine, or both.
- Persons commencing or participating in illegal strikes – Up to one year imprisonment or Rs 10,000 fine, or both.
- Persons instigating, inciting, or taking actions to continue illegal strikes, or knowingly supplying money for such purposes- Up to two years imprisonment or Rs 15,000 fine, or both.

Do we have a Fundamental Right to Strike in India?

- **Right to strike is not expressly recognized in the Constitution of India.**
- **The Supreme Court settled the case of Kameshwar Prasad v. The State of Bihar 1958 by stating that strike is not a fundamental right. Government employees have no legal or moral rights to go on strikes.**
- **India recognized strike as a statutory right under the Industrial Disputes Act, 1947.**

Industrial Disputes Act 1947

- The Industrial Disputes Act, 1947 (came into effect in April 1947 – before Independence) extends to the whole of India and regulates Indian labour law so far as those that concern trade unions as well as Individual workman employed in any Industry within the territory of Indian mainland.
- The Industrial Disputes Act 1947 defines public utility service and strike and puts certain prohibitions on the right to strike.

- The laws apply only to the organised sector and Every person employed in an establishment for hire or reward including contract labour, apprentices and part-time employees to do any manual, clerical, skilled, unskilled, technical, operational or supervisory work, is covered by the Act.
- It provides that no person employed in public utility service shall go on strike in breach of contract:
  - Without giving the employer notice of strike within six weeks before striking.
  - Within fourteen days of giving such notice.
  - Before the expiry of the date of strike specified in any such notice as aforesaid.
  - During the pendency of any conciliation proceedings before a conciliation officer and seven days after the conclusion of such proceedings.
- It is to be noted that these provisions do not prohibit the workmen from going on strike but require them to fulfill the condition before going on strike. Further these provisions apply to a public utility service only.
- This Act though does not apply to persons mainly in managerial or administrative capacity, persons engaged in a supervisory capacity and drawing > 10,000 p.m or executing managerial functions and persons subject to Army Act, Air Force and Navy Act or those in police service or officer or employee of a prison.

T.N., U.P. AND DEFENCE INDUSTRIAL CORRIDORS (DIC)

Context:

Tamil Nadu and Uttar Pradesh have acquired land for the Defence Industrial Corridors (DIC).

Relevance:

Prelims, GS-III: Internal Security Challenges (Defence Technology and Infrastructure developments, Government Policies and Interventions)

Dimensions of the Article:

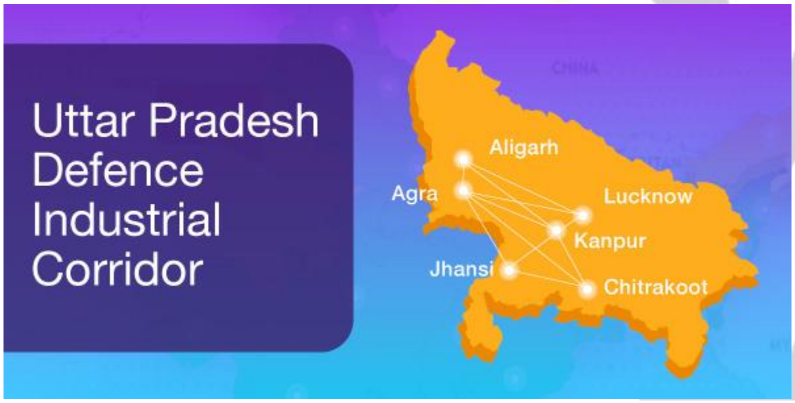
1. What are Defence Industrial Corridors (DIC)?
2. Uttar Pradesh Defence Industrial Corridor
3. Tamil Nadu Defence Corridor

What are Defence Industrial Corridors (DIC)?

- Defence Industrial Corridors (DIC) are corridors will facilitate a well-planned and efficient industrial base that will lead to increased defence production in the country.
- The corridors overlap with existing defence public sector companies, and aim to ensure connectivity among various defence industrial units.
- Developments of these corridors is significant as India is among the top 5 military spenders and one of the emerging defence manufacturing hubs in the world.
- Promoting Make in India, the Defence Industrial Corridors will catalyse indigenous production of defence and aerospace-related items.
- The combined efforts of the Government and private players will help achieve India's goal of self-reliance in defence, generate direct and indirect employment opportunities and spur the growth of private domestic manufacturers, Micro Small and Medium Enterprises (MSMEs) and Star-ups.
- Two Defence Industrial Corridors are being set up in India, one in Uttar Pradesh and another in Tamil Nadu.

Uttar Pradesh Defence Industrial Corridor

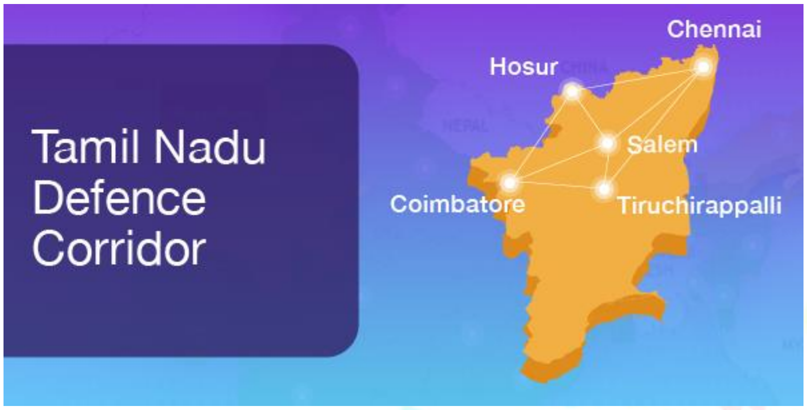
- The Uttar Pradesh Defence Industrial Corridor is being set up by the Uttar Pradesh Expressways Industrial Development Authority (UPEIDA). It consists of the following six nodal points with the potential to develop defence industries in the corridor:
  1. Agra
  2. Aligarh
  3. Chitrakoot
  4. Jhansi
  5. Kanpur
  6. Lucknow
- Plug and Play support will be provided to the industries in the corridor, which will consist of the following facilities:
  1. Assured water supply and uninterrupted electricity (132 KVA) along with pelican wire fencing boundary wall at the site
  2. Connectivity with 4-lane heavy-duty highway connected with Bundelkhand Expressway and Delhi-Jhansi
  3. Single Window approvals and clearances to Defence and Aerospace (D&A) manufacturing units via Nivesh Mitra, the single window system of the state
  4. Labour Permits for D&A industry towards flexible employment conditions
  5. Simple Procedures and rationalised regulatory regime with easy reimbursement of incentives and subsidies



Tamil Nadu Defence Corridor

- The Tamil Nadu Defence Corridor, being set up by the Government of Tamil Nadu, consists of the following five nodal points:
  1. Chennai
  2. Coimbatore
  3. Hosur
  4. Salem
  5. Tiruchirappalli
- The State holds the following strategic advantages which makes it a suitable destination for a defence corridor:
  1. The large coastal line which has four large seaports (three government and one private) and 22 minor ports
  2. The state has four international airports at Chennai, Coimbatore, Trichy, Madurai; and two domestic airports at Tuticorin and Salem
  3. A power surplus state with renewable energy capacity of 11,113 MW
  4. Tamil Nadu's capital city Chennai is connected to the world by three submarine cables providing a bandwidth of 14.8 Tbps

5. A destination of choice for Korean investors; the state is the largest Recipient of Korean Foreign Direct Investment (FDI) to India.



MADE-IN-INDIA CARRIER – INS VIKRANT

Context:

Recently, India's first indigenous aircraft carrier (IAC-1) set out to sea for its maiden set of trials, propelling India to a select group of nations capable of designing and building a complex platform such as this.

Relevance:

Prelims, GS-III: Internal Security Challenges (Security Challenges & their Management in Border Areas, Technological Advancements in Defence sector), Science and Technology (Indigenization of Technology)

Dimensions of the Article:

1. About INS Vikrant (Indigenous)
2. Current Status of Indian Navy, and Vikrant's significance

About INS Vikrant (Indigenous)

- The vessel is named Vikrant after the decommissioned maiden carrier of the Navy.
- It will have an air component of 30 aircraft, comprising MiG-29K fighter jets, Kamov-31 airborne early warning helicopters and the soon-to-be-inducted MH-60R multi-role helicopter, besides the indigenous Advanced Light Helicopters.
- It is expected to have a top speed of 30 knots (approximately 55 kmph) and is propelled by four gas turbines. Its endurance is 7,500 nautical miles at 18 knots (32 kmph) speed.
- The shipborne weapons include Barak LR SAM and AK-630, while it has MFSTAR and RAN-40L 3D radars as sensors. The vessel has a Shakti EW (Electronic Warfare) Suite.
- It has a pair of runways and a 'short take off but arrested recovery' system to control aircraft operations.

Current Status of Indian Navy, and Vikrant's significance

- At present, India has only one aircraft carrier, the Russian-origin INS Vikramaditya – and with the commissioning of INS Vikrant in the near future – it will become India's first indigenous aircraft carrier and its only second aircraft carrier.
- As per the Maritime Capability Perspective Plan, by 2027, India ought to have about 200 ships but there is still a lot to cover to reach the target.
- However, the cause is not mainly funding but procedural delays or some self imposed restrictions.
- The navy ensures that it has state of the art SONARs and Radars. Also, many of the ships contain a high amount of indigenous content.
- The combat capability, reach and versatility of the new Vikrant aircraft carrier will add formidable capabilities in the defence in the country and help secure India's interests in the maritime domain.
- It would offer an incomparable military instrument with its ability to project air power over long distances, including air interdiction, anti-surface warfare, offensive and defensive counter-air, airborne anti-submarine warfare and airborne early warning.

ITBP INDUCTS ITS FIRST WOMEN OFFICERS

Context:

The India-China LAC guarding the Indo-Tibetan Border Police (ITBP) force commissioned its first two women officers in combat after they completed their training.

Relevance:

GS-III: Internal Security Challenges (Various Security Forces/Agencies and their mandate)

Dimensions of the Article:

1. About the Indo-Tibetan Border Police (ITBP)
2. Central Armed Police Forces (CAPF)

About the Indo-Tibetan Border Police (ITBP)

- Indo-Tibetan Border Police Force (ITBPF) is a Central Armed Police Force (CAPF) functioning under the Ministry of Home Affairs, Government of India.
- The ITBP was established in 1962 under the Central Reserve Police Force (CRPF) act, during the India-China War and is a border guarding police force specializing in high altitude operations.
- However, in 1992, parliament enacted the Indo-Tibetan Border Police Force (ITBPF) Act and the rules were framed in 1994.
- The ITBP, which started with 4 battalions, has, since restructuring in 1978, undergone expansion to a force of 60 Battalions with 15 Sectors and 05 Frontiers as of 2018 with a sanctioned strength of almost 90 thousand personnel.
- The ITBP is trained in the Civil Medical Camp, disaster management, and nuclear, biological and chemical disasters.
- ITBP personnel have been deployed abroad in UN peacekeeping missions in various countries as well.
- Presently, ITBP is deployed on border guarding duties from Karakoram Pass in Ladakh to Jachep La in Arunachal Pradesh covering ~3,500 km of Indo-China Border.

- ITBP Border Out Posts are of the height upto 18,750 feet where the temperature dips down minus 40 degree Celsius.

For the first time: 2 women Assistant Commandants

- The ITBP started recruiting women combat officers in its cadre from 2016 through an all-India examination conducted by the Union Public Service Commission (UPSC).
- Before this, it only had combat women in the constabulary ranks.
- Out of the total 53 officers, 42 officers are in the general duty combat cadre, while 11 are in the engineering cadre of the about 90,000 personnel strong mountain warfare trained force.

Central Armed Police Forces (CAPF)

- The Central Armed Police Forces (CAPF) comprises five Armed forces of the Union of India under the authority of the Ministry of Home Affairs.
- The 5 forces of CAPF are:

1. Border Security Force (BSF),
2. Central Reserve Police Force (CRPF),
3. Central Industrial Security Force (CISF),
4. Indo-Tibetan Border Police (ITBP) and the
5. Sashastra Seema Bal (SSB).

- Apart from the primary role, all CAPFs are involved in assisting Police in Law & Order situations and also Army in Counter-Terrorist Operations. BSF & CRPF have assisted the army during external aggression in the past.
- Central Armed Police Forces personnel also serve in various important organisations such as Research and Analysis Wing (RAW), Special Protection Group (SPG), National Investigation Agency (NIA), Intelligence Bureau (IB), Central Bureau of Investigation (CBI), National Disaster Response Force (NDRF), Narcotics Control Bureau (NCB) etc.