GSSCORE

An Institute for Civil Services

INTERVIEW GUIDANCE 2021

CURRENT AFFAIRS & MAJOR DEBATES

of

INTERNAL SECURITY

8448496262 | www.iasscore.in

CONTENTS

****

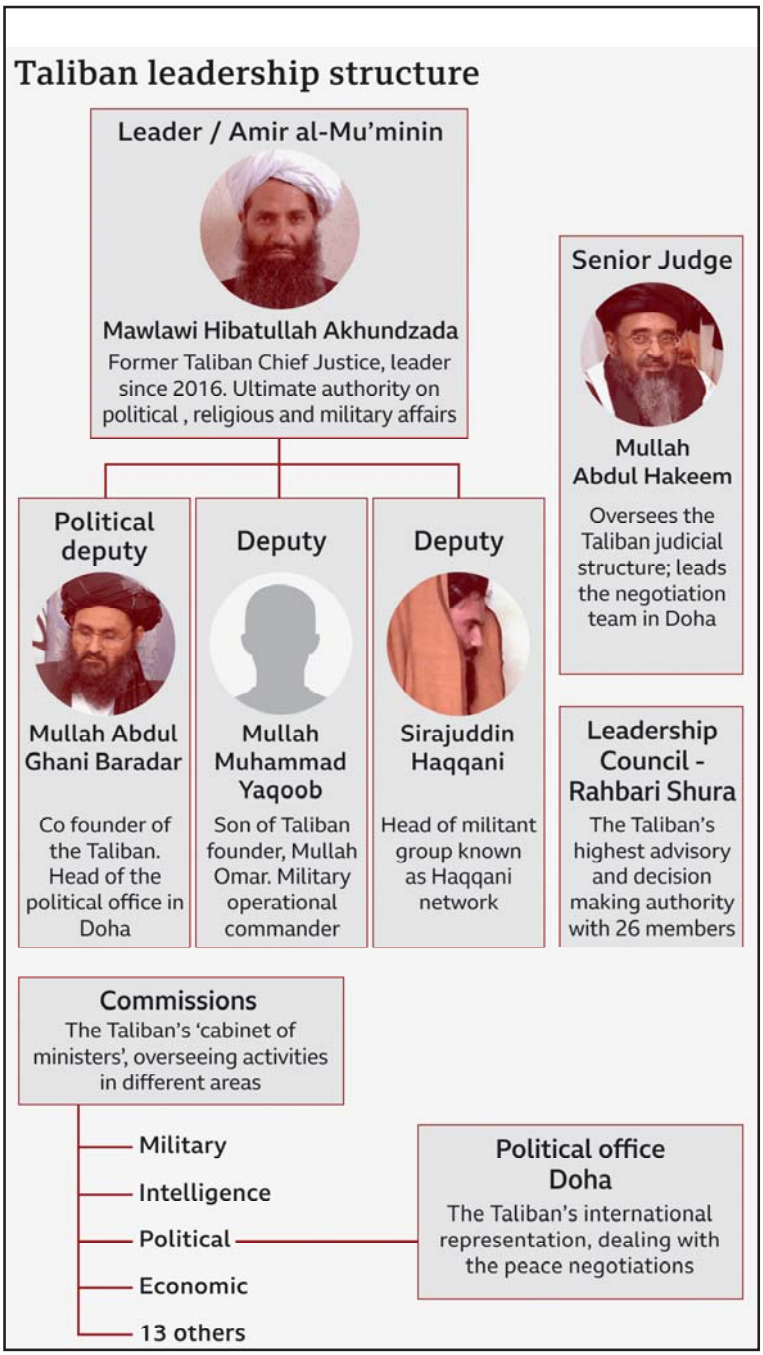
1 Rise of Taliban is internal security challenge for India

Context:

The rise of Taliban raises serious security concerns for India and the region as the terror groups having bases in Afghanistan could get further support to expand their activities.

Who are the Taliban?

- Taliban is a **Sunni fundamentalist organisation** that is involved in Afghan politics. It is also a military group that is involved in an insurgency against the currently elected government in Afghanistan.
- The Taliban controlled almost **three-quarters of the country from 1996 to 2001** and was notorious for their strict implementation of the **Sharia or Islamic law there.**
- The period saw widespread **abuse of human rights, especially targeted against women.**
- The current head of the Taliban is **Hibatullah Akhundzada.**
- Mullah Omar is regarded as the founder of the Taliban.
  - He died in 2013.
- The Taliban officially refers to itself as the '**Islamic Emirate of Afghanistan'.**
- The word **'Taliban' in Pashto means 'students'.**



Origins of the Taliban

- **Events that led to the rising in power of the Taliban-**
  - **The Saur Revolution in Afghanistan (April 27) in 1978** installed a communist party in power there.

- This government introduced many reforms for modernisation and hence was considered too radical by some.
- Rural areas and the traditional power structures were unhappy with the new scheme of things and this led to anti-government protests in many places.
- There were divisions even within the government.
- The **USSR** intervened in Afghanistan wanting to place a communist ally in government there.
- In **December 1979,** the **Soviet Army was deployed in Kabul (February 15)**. They orchestrated a **coup killing the ruling President Hafizullah Amin.**
- The **Soviets** installed their ally, Babrak Karmal as the President of Afghanistan.
- The USA and other western countries saw this as a **Soviet invasion.**
- A bitter war was fought between **Soviet troops and the insurgent groups called Mujahideen.**
  - While the **cities and towns were under Soviet control**, the **rural parts were under the control of the Mujahideen.**
- The Mujahideen were persistent in their fight against the USSR and were also supported by the **USA, China, Iran, Pakistan, Saudi Arabia and Egypt.** They were given training and weapons.
- The citizens of Afghanistan suffered the most in this protracted war. Many civilians lost their lives and homes. Afghan refugees poured into countries like **Pakistan, Iran and even India.**
- The **Soviets withdrew troops in 1989** after nine long years and at the cost of the lives of **20 lakh Afghan civilians.**
- Now, the government of Afghanistan had to fight the Mujahideen alone.
- The insurgents took control of **Kabul in 1992.** There was a bloody civil war as the Mujahideen themselves were divided into various factions all vying for power.
- **In 1994,** a group of students seized control of the city of **Kandahar** and started a battle for power to control the entire country. They were called the **Taliban.** They were **Islamic fundamentalis**ts. In fact, many of them were trained in camps in Pakistan where they were refugees.
- **In 1995,** the Taliban captured the province of **Herat** and in **1996, Kabul.**
- **By 1998,** almost the **entire country** was under the control of the **Taliban.**
- Some of the Mujahideen warlords fled to the north of the country and joined the **Northern Alliance** who were fighting the **Taliban.**

Taliban Latest Development

- The Taliban has taken control of **Afghanistan, as of 16th August 2021.**
- The quick collapse of the government in Afghanistan, and the Taliban taking over the presidential palace, seem to have triggered panic and fear among the people in Afghanistan, many of whom are taking flights to escape the country.
  - **President Ashraf Ghani** fled the country on **15th August,** reportedly to Tajikistan, although this is not confirmed.
- The Taliban (spelt alternatively as Taliban) is an **Islamic fundamentalist political and military organisation operating in Afghanistan.** They have dominated Afghan polity for quite some time and feature regularly in international affairs.

Afghanistan under the Taliban regime

- Initially, when they came to power, the people of Afghanistan generally welcomed the Taliban. This is because they seemed to offer stability in a country wracked by long and bloody civil wars.

- The Taliban's promise was to restore peace and prosperity in Afghanistan and enforce Sharia in the country.
- Afghans were tired of the fighting between the Soviets and the Mujahideen and welcomed the Taliban, who were successful initially in weeding out **corruption and removing lawlessness.**
- The Taliban introduced their **interpretation of Islamic law,** which meant that **several rights were suspended for people, especially women and children.**
- They endorsed **Sharia mixed with the Pashtun tribal code.**
- Women were required to **wear burqas** covering their whole bodies including faces; men had to **grow beards.**
- Women could not go out of the house **without a male family member** accompanying them. They could not work outside.
- The Taliban discouraged girls from going to school, and at one point, **banned girls above the age of eight from going to school.**
  - Schoolgirl and rights activist **Malala Yousafzai** was shot by Taliban gunmen in October 2012.
- Public executions were held for those accused of murder and adultery. Amputations were also done for those accused of stealing.
- They banned **television, music, kite-flying, cinema, photography, painting,** etc. Women were barred from attending sports events or playing them.
- People, especially women, faced public floggings for any perceived wrongs.
- The Taliban is also accused of carrying out massacres against civilians, especially ethnic or religious minority groups. Thousands were killed, women raped and people are still unaccounted for.
- Needless to say, they did not believe in democracy.
- The Taliban was much criticised for blowing up the **1500-year old Buddha statues** of Bamiyan because they were idols.

Taliban – International Relations

- Only three countries recognised the Taliban while they were in power namely, **Pakistan, United Arab Emirates and Saudi Arabia**. They are believed to have been receiving funds from both **Pakistan and Saudi Arabia.**
- After the **9/11 attacks** on the US, the Taliban drew focus from all over the globe.
- It was accused of sheltering **Osama Bin Laden and Al Qaeda,** who were blamed for the **9/11 attacks.**
- In fact, the **US intervened in Afghanistan in 2001 to deny Al Qaeda** a safe haven and a base to operate in the country.
- Pakistan officially broke off diplomatic ties with the organisation after 9/11. However, many top leaders of the Taliban are said to have escaped to **Quetta in Pakistan**, from where they were controlling the organisation.
- The Taliban were removed from power in **October 2001** by a coalition of forces led by the **USA and several other countries (including NATO nations).**
- In December 2001, a **new interim government** was placed in Afghanistan headed by **Hamid Karzai.**
- The country gradually started reconstruction work after long years of bitter battles and underdevelopment.
- However, the Taliban was reorganised by its leader Mullah Omar after its defeat, who launched an insurgency against the Afghan government.

- It wages war in the form of suicide attacks, ambushes and guerilla raids and turncoat killings against the coalition forces.
- Slowly through the second half of the 2000s, civilian killings rose in number.

Challenges for India

- **Issue of Indian Security:** The restoration of Taliban rule in Afghanistan presents some very serious potential challenges for Indian security. One of the major challenges include securing its development infrastructures in Afghanistan.
- **Spread of International Terrorism:** For India, a bigger challenge will be about the Taliban's renewed support for international terrorism and Pakistan's re-direction of jihadi groups that have allegedly fought with the Taliban towards India.
- **Religious Fundamentalism:** Like all radical groups, the Taliban will have trouble balancing its religious ideology with the imperatives of state interests.
  - India faces a challenge to deradicalise the region for long lasting peace and stability.
- **New Regional Geopolitical Developments:** There can be new regional geopolitical alignments (such as China-Pakistan-Taliban) which may go against the interests of India.
  - Meanwhile, the US withdrawal compels the creation of a new balance of power system in and around Afghanistan.
  - Moreover, the US and the West will try to shape the international attitudes towards the new regime.
- **No Contiguity with Taliban:** Unlike Pakistan, China and Iran, India has no contiguity with Afghanistan.
  - Russia has a security treaty with Tajikistan, for instance, and has deployed more troops there to prevent a destabilising spill over from the turmoil in Afghanistan into Central Asia.
  - India has no such security responsibilities and no direct access to Central Asia.
  - This may give reasons to the Taliban to hit back at India through Pakistan in J&K, given that LeT and Jaish are operating in Afghanistan alongside the Taliban.

India's Relations with the Taliban

- India has never recognised the Taliban while they were in power.
- **In 1999,** an Indian Airlines flight was **hijacked and landed in Kandahar,** and it was suspected that the Taliban supported the hijackers. India also supported a key **anti-Taliban group,** the **Northern Alliance.**
- Following the backdrop of the peace talks between the **United States and the Taliban in 2019,** the Taliban has sought positive relations with India.
  - To this effect, the Taliban have reiterated that Kashmir is an internal matter for India and will not seek to interfere in the matters of other nations.

2 Non-lapsable Modernisation Fund for Defence and Internal Security (MFDIS)

Context:

The 15th Finance Commission (the constitutional body that decides the shares of the Centre and states in all taxes and revenues) has recommended the constitution of a dedicated non-lapsable Modernisation Fund for Defence and Internal Security (MFDIS).

Background

- The Defence Ministry has for long been demanding a non-lapsable fund, keeping in view the long trajectory of military modernisation.
- While the threat along India's western borders remains both consistent and somewhat constant – as it weighs, that along our Northern borders has abruptly escalated.
- The threat is augmented by increasing Chinese presence in the Indian Ocean.
- The incontrovertible truth is military modernisation needs a boost to enhance the credibility of our deterrence.
- To address the shortages, especially in capital budget allocation, the Ministry of Defence is pursuing a non-lapsable **Defence Modernisation Fund.**
- In the action-taken report tabled in Parliament, the government said it had "in principle" accepted the creation of the fund in the Public Account of India.

About Non-lapsable Modernisation Fund

- The dedicated non-lapsable Modernisation Fund for Defence and Internal Security (MFDIS) aims to bridge the gap between **projected budgetary requirements** and the **allocation for defence and internal security**.
- The indicative size of the MFDIS for 2021 to 2026 is Rs. 2,38,354 crore and the maximum recommended is Rs. 51,000 crore a year.
- However, the unutilised amount from the normal budgetary allocations to the Defence Ministry and the Home Ministry for capital expenditure shall not be part of the fund.

Who would have rights on the fundings?

- The Defence Ministry would have exclusive rights over the use of the amounts deposited in the fund from the specified sources of revenue.
- The Home Ministry will only be permitted to use what is earmarked for it from the source of revenue.
- The fund may be operated by a suitably **empowered High-Powered Committee** headed by the **Cabinet Secretary** and consist of the **Secretaries of Defence, Home and Expenditure and the Chief of Defence Staff.**

Composition of the Fund

- The fund will have four specific sources of incremental funding, which include:
  - Transfers from the Consolidated Fund of India
  - Disinvestment proceeds of defence public sector undertakings (DPSUs)
  - Proceeds from the monetisation of surplus defence land, including realisation of arrears of payment for defence land used by the State governments and for public projects
  - Cost recovered from encroached land and proceeds of receipts from defence land

Consolidated Fund of India (CFI)

- As per **Article 266** of the Indian Constitution, all revenues received by the central government by way of tax collections, loans raised by issuing treasury bills, amongst other means, mandatorily accrue to the CFI while, receipts from small savings, provident fund collections and sundry sources are routed to the Public Account.
- In effect, the government merely acts akin to a banker or custodian of this money, holding it in a trust to be paid out when demanded by their rightful owners.

Utilization of the Fund

- The proceeds will be utilised for:
  - Capital investment for modernisation of the defence services
  - Capital investment for the Central Armed Police Forces (CAPF)
  - Modernisation of State police forces as projected by the Home Ministry
  - A small component as a welfare fund for soldiers and paramilitary personnel

What are Non-lapsable funds?

Non-lapsable funds are the funds allocated to certain schemes of the government, which have to be spent within the current fiscal year of allocation, if not then the fund will be evaporated and cannot be used in the next fiscal.

3 Drug trafficking in India

Introduction:

- **India is one of the world's largest illegal drug traffickers. Opiates, cannabis and amphetamine-type stimulants remain a major concern in the region, with record levels of cannabis treatment seized in India in 2018.**
- **Non-therapeutic use of prescription drugs, which contain controlled substances, continues to be cold. The global trend of buying drugs over the Internet, especially on 'black market' trading platforms using crypto currency has already spread throughout South Asia, including India.**

Dangerous drug trade in India:

- India has become a centre of smuggling. The cocaine offered here is not limited to India; traffickers exploit this route to gain access to other countries.
- India could have been used as a feeder had it not been for the high level of interest in this drug within the country.
- The Golden Triangle is a place where the borders of Thailand, Laos, and Myanmar meet at the confluence of the Ruak and Mekong rivers. According to the United Nations Office on Drugs and Crime (UNODC), opium production has increased by 22%.
- Golden Crescent is the name given to one of the two major Asian opium production centres (the other Golden Triangle), located at the crossroads of Central, South, and Western Asia. This space passes through three nations, Afghanistan, Iran, and Pakistan, whose mountains define the piece.
- Close to the Golden Crescent and the Golden Triangle, India is at risk of drug trafficking and drugs such as heroin, hashish, and synthetic drugs produced in these areas.
- The Golden Crescent, has been a major source of heroin trafficking in the country since the early 80's when traffickers began smuggling heroin into the region via India following the Iran-Iraq war.
- Opium production in Afghanistan, high domestic demand in India, and the consolidation of state government officials and border patrols together have contributed to this increase in heroin trafficking, particularly in the Punjab sector.
- Apart from drugs, India has experienced a dramatic increase in psychotropic drug use and treatment arrangements among addicts since the late 1990s.

- Strict drug and drug laws, rising heroin prices and easy availability of synthetic drugs have contributed to this change.
- India also produces a wide range of synthetic drugs and pre-smuggled chemicals from the country.

World Drug Report 2021

- An estimated 275 million people worldwide use drugs in the past year. More than 36 million people suffer from substance abuse disorders.
- The decline in marijuana use during the epidemic has been reported in many countries.
- Non-therapeutic use of therapies has also been observed at the same time.
- According to the latest international estimates, about 5.5 percent of people between the ages of 15 and 64 used drugs at least once a year.
- More than 11 million people worldwide are estimated to be injecting drugs - half of them with Hepatitis C.
- Opioids continue to account for the heavy disease burden associated with drug abuse.

How does it pose a threat to world security?

- These two illegal drug traffickers pose a serious threat to national security. Violations of the country's borders by drug traffickers mean that the same routes can be used to smuggle weapons and terrorists into the country.
- Interactions between drug traffickers, criminal organizations, and terrorists are another major threat. The seizure of drugs by the arms of border guards indicates the closeness between drug traffickers and anti-racism.
- Proceeds from illicit trafficking in drugs are used to finance terrorist activities. Troops from Kashmiri, Sikhs and the northeast have used drug money to finance their 'struggle' against India.
- The high availability of drugs and drugs promotes the need for drugs and drugs by local people. The use that produces unethical behaviour thus creates a problem for law and order in society.
- This causes significant economic damage to the country due to the loss of productivity and diversion of drug care and rehabilitation resources (Population becomes a burden).

Conclusion

Given these challenges, India must adopt a comprehensive approach to reducing the supply and demand for drugs and drugs. Legislation and ensuring physical security of the coast and coast by strengthening patrols and surveillance are essential. Asking for the cooperation of neighbours by entering into several bilateral and multilateral agreements on the prohibition of illicit drug and chemical trade should be halted by drug lords across the border.

4 Covid 19 and Naxalism

Context:

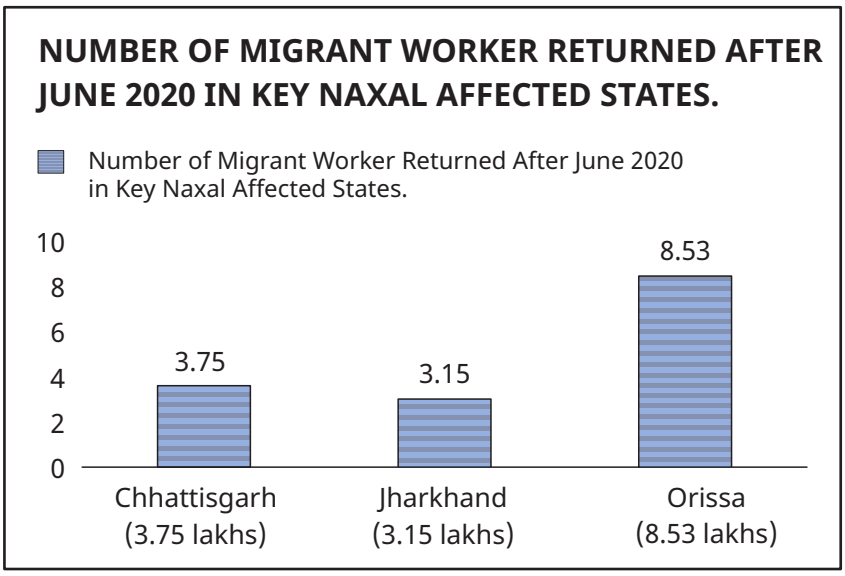
The outbreak of the COVID-19 pandemic and subsequent countrywide lockdown to prevent its transmission have variedly impacted the Indian Maoists. The lockdown has certainly increased Maoists' desperation to meet their demands of food supplies and other essentials.

Impact on Maoists

- The Maoists, in all the affected wing countries (LWE), are getting their share and other essentials through a network of assistants from the local market (weekly markets).
- With the haat markets temporarily closed, they are reportedly experiencing severe food shortages.
- Also, as all economic and construction activities have been put in place in these areas to ensure the effective operation of the closure, Maoists funds have been hit hard because the dismissal of contractors, the mining industry, truck drivers, etc., makes up a large portion of their finances.

Impact on rural and ethnic groups

- The Maoists reportedly devised a number of problem-solving strategies to overcome the impact of the closure of their budget and financial provision, albeit in a small way.
- The Bastar Maoists pressured the village chiefs and others to arrange food for them. In areas where residents could not afford to stockpile large quantities of rice, Maoists confiscated a one-month free share for each of the families below the poverty line (BPL).



- Maoists are also accused of transporting displaced workers to their villages instead of money.
- The Lockdown situation has heightened the frustrations of the Maoists and exploited the local people to achieve their goals.
- Maoists are enhancing their strength and preparing for future operations. They are recruiting jobless migrants in large numbers to beef up the declining carder, especially in the area they were finding resistant initially.
- The pandemic has made the intra-state movement of the Maoist leader much easier. Now they are quickly influencing the youth, including women, to join their grass route cadre.

A truce call made by a few Maoists to overcome the effects of lockdown

- Maoists reportedly offered a temporary fire fight earlier this month in Andhra Pradesh and Odisha provinces, especially in the Andhra Odisha Border Special Zonal Committee (AOBSZC).
- While the Maoists' refusal to 'simplify government relief activities in their key areas in the fight against COVID-19', it is believed that this provision is beneficial and misleading.
- Factors that could influence the Maoists' decision to launch telecommunications are: achieving possible respite so far has tightened security in their key areas, as well as increased social pressure to open the operation of COVID-19 in remote villages, which could exacerbate the plight of many needy people.

- The veracity of this dialogue is also disputed as it does not come from the entire Central Committee of the Communist Party of India (Maoist) or the CPI (Maoist).

Challenges are still there

- The game is still not over for Naxalite as the Covid-19 crisis has brought out the conditions that favour the Naxal movement.
- Decrease in the economic condition of the people.
- The fissure within the society between having and have nots with downtrodden people believing that they were the ones who paid the price for strict lockdown and have to lose their lives while the rich increase their wealth manifold in the same period.
- This disparity in society can allow the Naxalite to gain the ground where they never reached before.
- The further economic and social distress can give enough space to Maoists to gain the lost ground.
- The April 2021 deadly attack by Maoists on a joint team of Central Reserve Police Force (CRPF), District Reserve Guard (DSG), and Special Task Force (STF) could be a possible indication of their increased strength and morale.
- It is believed that the Maoists could also offer money and enlist the jobless migrant workers returning to their villages.
- Recently, a large group of armed Maoists from Andhra Pradesh, Telangana, Maharashtra, Jharkhand, Odisha and West Bengal has reportedly joined their Bastar colleagues to up the ante against the security forces.

Government response and Recommendation

- The testing time of Covid-19 is an opportunity for the government to allure the ultras to shed weapons and join the mainstream. When a restriction is already in place, the government needs to push for more non-kinetic methods for winning hearts and minds.
- Even the Maoist want the government to respond through kinetic means rather than through a developmental perspective.
- It is of no surprise that Naxalism flourished mainly in underdeveloped, mineral-rich forested areas of Central India, where they have a support base of downtrodden, uneducated, and Tribal populations.
- The percentage of people living below the poverty line is very high in the core Naxal affected area. Thus, the government's focus shall be on monitoring the migrant workers returning home and having statistical data about their employment status and livelihood condition.
- Further, the government shall focus on giving more rural-based employment opportunities to unemployed migrants. Last, the government shall keep a tight vigil on the recruitment drive carried out by Naxals in areas where migrant workers have returned in large numbers.

Need of Hour

- Intergovernmental governments, administrators and founders of security need to recognize that this organization cannot be approached by law and order.
- The process of improving the conditions of the poor and the nations clearly needs to be accelerated if the organization is to be considered successful.
- Winning the hearts and minds of the people of the nation and other marginalized groups will be at the heart of the rebel plan.
- The development of road and rail infrastructure will not only boost economic growth and development but also help fight Maoist propaganda.

- Improved road connectivity will have the effect of duplicating the security forces' performance in operations.
- Provide compensation and other life support programs to volunteers.

5 Draft Drone Rules, 2021 released by Ministry of Civil Aviation

Context:

The Ministry of Civil Aviation (MoCA) has released the updated, Drone Rules, 2021 for public consultation. The Drone Rules, 2021 will replace the UAS Rules 2021 (released on 12 March 2021).

About

About the Drone Rules, 2021

- **Applicability:** Drone Rules 2021 will apply to individuals owning, possessing, exporting, importing, manufacturing, trading, leasing, operating, transferring, or maintaining a drone in India. They don't apply to drones used by the armed forces.
- **Issuing authority:** The certificate will be issued by the **Quality Council of India** or a certification body authorized by the government.
- **Drone Promotion Council:** The draft policy talks about a potential trade body called the **Drone Promotion Council** to develop "a business-friendly regulatory regime".
- The council will work on automated permissions, incubator centers, and organize drone technology events and competitions to state the draft policy.
- **Drone Corridor:** The rules also envision a **drone corridor** that will cater to deliveries and taxis.
- A drone taxi, or passenger drone, is a pilotless helicopter that can fly at a speed of around 130 km/hour.
- **Safety features:** Safety features like 'No permission – no take-off' (NPNT), real-time tracking beacon, geo-fencing, etc. to be notified in the future. A six-month lead time will be provided for compliance.
- **Digital sky platform** shall be developed as a business-friendly single-window online system.
- **Airspace map:** An interactive **airspace map** with green, yellow, and red zones will be displayed on the digital sky platform.
- **Minimal human interface:** There will be a minimal human interface on the digital sky platform and most permissions will be self-generated.
- **Regulation of imports:** Import of drones and drone components to be regulated by DGFT.
- **Coverage:** Coverage of drones under **Drone Rules, 2021** increased from 300 kg to 500 kg. This will cover drone taxis also.

Why the Drone Rules are needed?

- The new rules come over a month after India witnessed what has been described as the country's **first-ever terror attack**carried out by a UAV.
- The new rules will give a push for 'Made-in-India' drone technology.

About Drones

- Drones are unmanned aerial vehicles that can be maneuvered remotely by a pilot.
- There are three subsets of Unmanned Aircraft:
  - Remotely Piloted Aircraft
  - Autonomous Aircraft
  - Model Aircraft
- Based on their weight, drones can be divided into five categories:
  - **nano** (weighing up to 250 g)
  - **micro** (250 g to 2 kg)
  - **small** (2-25 kg)
  - **medium** (25-150 kg)
  - **large** (over 150 kg)

6 Drone terror attack on Jammu base: dangerous new turning point

Context:

The recent drone strikes at the Indian Air Force Station in Jammu and subsequent sightings of drones close to military stations have set alarm bells ringing.

Background

- A **drone attack** was conducted on the Jammu Air Force Station on June 27 this year.
- It was the first such instance of suspected Pakistan-based terrorists deploying **unmanned aerial vehicles** to strike at vital installations.

Analysis

■ What is a drone?

- A drone refers to an unpiloted aircraft or spacecraft.
- A drone is also called an "unmanned aerial vehicle" or UAV. So, simply put, a drone is a flying robot.

UAVs in India

- **Heron:** In March this year, the Indian Army leased four Heron unmanned aerial vehicles (UAVs) from Israel.
  - Heron is the medium-altitude long endurance UAVs.
- **Ghatak UCAV:** The indigenously produced Ghatak UCAV is expected to make its maiden flight next year.
  - DRDO Ghatak is an autonomous stealthy unmanned combat air vehicle.

- **Rustom:** The indigenous tactical surveillance UAV Rustom also seems ready for induction into the army.
  - Rustom is a **Medium Altitude Long Endurance unmanned air vehicle.**
  - It is being developed by Defence Research and Development Organisation for the three services, Indian Army, Indian Navy and the Indian Air Force of the Indian Armed Forces

What are the rules on drones in India?

- The Ministry of Civil Aviation recently notified the **Unmanned Aircraft System Rules 2021** that govern the operation of drones and similar systems in India.
- Weight is the primary basis by which the rules classify drones vis-a-vis the specific rules governing their operation.
- **Permission required from:** Director General of Civil Aviation.

Name	Weight	Permission
Nano drones	weigh less than or equal to 250gm	No license or permit is needed to fly such drones
Micro drones	weighing more between 250gm and 2kg	UAS Operator Permit-I (UAOP-I)
Small drones	can weigh more than 2kg but should not exceed 25kg	UAS Operator Permit-I (UAOP-I)
Medium drones	can weigh between 25kg and 150kg	UAS Operator Permit-II (UAOP-II)
Large unmanned aircraft	weigh more than 150kg	UAS Operator Permit-II (UAOP-II)

What are the checks and bans in the Rules?

Several checks and bans are built into the rules to prevent drones posing a security threat. For example-

- **Return to home option:** All drones have to mandatorily contain autonomous flight termination system or return to home (RTH) option.
- **Geo-fencing system:** All drones should also come with **geo-fencing mechanism.**
  - **Geo-fencing systems** provide a means for restricting the movement of a drone for a real-world geographic location using the global positioning system (GPS) or radio frequency identification.
- **No-permission-no takeoff:** Further, all drones, except Nano models, will have to have a **tamper-proof 'No Permission–No Takeoff (NPNT) mechanism.**
- **No-fly areas:** There are also no-fly areas for drones that include airports, strategic locations, and the LoC with Pakistan and LAC with China, etc.

Are UAVs the double-edged swords?

■ Positive side

- UAVs have myriad applications—from delivering pizzas, shooting films, inspecting pipelines and power lines to spraying crops and helping cartographers.
- UAVs have a wide variety of law enforcement application, including mapping crime scenes, providing aerial images, and 3D mapping of crash scenes.

■ Negative side

- But like most technologies, UAVs are also double-edged swords, finding use as powerful weapons and force multipliers for the armed forces.
- The military UAV umbrella includes everything from **aero-models** and **decoys** to reconnaissance and **armed drones**; some provide commanders with real-time battlefield data to direct fire, while others can carry out precision strikes on targets miles away using satellite guidance.
- In fact, the latter are slowly taking over a range of dangerous missions that were flown by combat pilots earlier.

How UAVs have evolved over the years?

- First **UAVs** was used in **World War II** by **Britain.**
- Initially used as **target drones (for training anti-aircraft gunners)**
- Today, they have become the indispensable robotic air warriors.
- First modern UCAV appeared in the skies over the **Golan Heights** in 1973 during the **Arab-Israeli war**.

Why is it a serious issue?

- **Evade detection:** Drones fly low, they escape detection by radars and interjection by air defence systems.
- **Lack of effective policy:** No universal policy to deal with rogue drones in the country.
- **Underdeveloped capabilities:** Indian drone and anti-drone capability is still work in progress.

Deadly effects of drones

- Drones have been used with deadly effect, for example,
- Yemeni soil against the Saudi oil installations.
- They have also been used militarily with great success against the **Armenians** in **Nagorno-Karabakh** by **Turkey-**supported Azerbaijani forces.
- The Chinese have used drones for aerial surveillance in **Ladakh** during the current stand-off.
- The Americans have used armed drones in **Afghanistan** and in **Iraq** to eliminate terrorists, and even a high-ranking serving military officer as in the case of the **Iranian General Qasem Soleimani.**

Why terrorist are choosing drone technology?

- Acts of terrorism in India have been dominated by **AK 47-wielding terrorists, fedayeen human bombs**, and **planting of IED**. However, the scenario is changing.

- **Safety for terrorists:** Now, use of drones provides terrorists with maximum safety.
- **Cheaper deal:** Advances in technology have made the cost so low that it is cheaper than an AK-47.
- **Easily available**
- **Can be easily modified for different purposes**

Drone for terror

- In 2013, Al-Qaeda attempted drone attacks in Pakistan but failed
- In 2014, Islamic State used drones in Iraq and Syria
- Islamic State, Hezbollah, and Pakistan-based terror groups use drones for terrorism

What immediate measures are required?

- Drone detection system.
- High-tech interception, strict regulation a must.
- UAV defences should be augmented with acquisition of detection technologies.
- The electronic warfare (EW) capabilities of the armed forces should be enhanced and these should be equipped with kinetic and directed energy kill systems on priority.

7 Proposed model of the integrated theatre commands

Context:

Chief of Defence Staff General Bipin Rawat held a meeting in the backdrop of concerns about the proposed model of integrated theatre commands.

About

■ About the proposal under discussion

- A model with four to five integrated tri-Services theatre commands is under discussion, with each command headed by a three-star officer.
- This officer, the theatre commander, will report to the Chiefs of Staff Committee (COSC), which, as the name suggests, includes the three Service Chiefs, and is headed by the CDS as its permanent chairman.
- The Service chiefs currently have all the operational control over their forces; operational powers will now move to the COSC.
- Each of these commands will have the needed assets from all three forces.

The proposed commands are:

- **Maritime Theatre Command:** It will take care of all the maritime security needs of the country on both the eastern and the western seaboards, and will include air strike assets and amphibian forces of the Army.

- **Air Defence Command:** It will be mandated with air defence across the country and beyond. The fighter jets will have reconnaissance and surveillance assets as well.
- **Land-based commands:** Two or three land-based commands are proposed. If there are two commands, there will be one each for India's borders with China and Pakistan.
- **Logistics Command:** There will be a Logistics Command, which will have the logistics of all the Services under one person; and there will be a Training and Doctrine Command so that all Services work under a common doctrine and have some basic common training.

What is an Integrated theatre command?

- It is a unified command under which all the resources of the Army, the Navy and the Air Force are pooled, depending on the threat perception.
- The commands could be geographical that will look at a border with a particular country or thematic, as a command for all maritime threats.
- Several nations in the world have theatre commands, **including the United States and China**.
- The idea of creating an integrated tri-Services command in India had been recommended at various levels after the Kargil conflict.
- Gen Rawat was appointed Chief of Defence Staff to head the integrated command.

Existing commands in India

As of now, the three forces have 17 commands between them.

- **The Army has seven commands**: Northern, Eastern, Southern, Western, Central, Southwestern and Army Training Command (ATRAC).
- **The Air Force has seven as well:** Western, Eastern, Southern, Southwestern, Central, Training, and Maintenance commands.
- **The Navy has three**: Western, Eastern and Southern, of which Southern is largely about training.
- **Tri-Service Command**: There are two existing tri-Service commands as well — the Andaman and Nicobar Command (ANC), which is headed by rotation by officers from the three Services, and the Strategic Force Command, which is responsible for India's nuclear assets.

CDS and its need

- The creation of the Chief of Defence Staff (CDS) is a start to defence reforms. This would improve joint manship in peacetime.
- Major problems:
  - historical lack of unified war fighting strategy formulation at the apex military level
  - the unclear division of responsibility and resources between service Chiefs and Commanders in-Chief (C-in-Cs)
  - the differing natures of command and control between the three services, which manifest as differences in structural organisations.
- Treating India as one unified theatre can reduce these problems.
- This announcement was followed by the creation of a new Department of Military Affairs (DMA) to be headed by the CDS.

Status of Integrated Theatre Commands in China and USA

- Both the USA and China have well established integrated theatre commands.
- On the other hand, India is still struggling to get it.
- The area covered under the commands by both the countries can be seen in the pictures.

8 National Maritime Security Coordinator appointment

Context:

The Indian government is planning to create and appoint a National Maritime Security Coordinator (NMSC), two decades after the Kargil Group of Ministers' recommendation.

About

About the National Maritime Security Coordinator (NMSC)

- NMSC will act as an interface between the civilian and military maritime domain to enhance security architecture and energy security in India.
- It will break the silos and cut across the turf of **Navy, Coast Guard, State Maritime Boards** to enhance maritime domain awareness and ensure a better response.
- The Maritime Security Coordinator will work under **Indian National Security Advisor** and be the **principal advisor** to the government on the maritime security domain.
- The appointment of NMSC fills the need of the hour as the Navy, Coast Guard and state maritime boards all tend to work in silos with overlapping jurisdictions and are constantly at odds with each other.
- **Agenda:** The Chinese forays into the Indian Ocean via Pakistan and Myanmar will be on top of the NMSC agenda.

Significance of the NMSC

- 70 per cent of Indian trade including vital crude oil is transported through sea and the protection of sea shipping lanes is vital to India's security.
- With China moving towards a sea-based security doctrine and penetrating the Indian Ocean through Pakistan and Myanmar, the post of NMSC will be vital for maritime and energy security as Beijing plans to reach the eastern seaboard of Africa through the Indian maritime domain.
- The creation of NMSC is part of enhancing maritime capability through **Act East Policy, SAGAR (Security and Growth of All in the Region), Deep Ocean Mission and the Sagarmala project** to make **India's 12 major ports into the world-class standard.**

SAGAR (Security and Growth of All in the Region)

- It is India's policy or doctrine of maritime cooperation in the Indian Ocean region.
- India unveiled its strategic vision for the Indian Ocean i.e. Security and Growth for All in the Region (SAGAR), in 2015.

Deep Ocean Mission

- Deep Ocean mission is an Indian initiative to undertake deep ocean exploration focused on India's exclusive economic zones and continental shelf.

Sagarmala project

- The Sagarmala Programme is an initiative by the government of India to enhance the performance of the country's logistics sector.
- The programme envisages unlocking the potential of waterways and the coastline to minimize infrastructural investments required to meet these targets.
- The project was launched in 2015.

9 Assessing India's Cyber Security Infrastructure

Context:

According to recent reports (New York Times and Recorded Future), Chinese state-sponsored actors may have used malware to target India's power grid system and seaports. The reports claimed that "Red Echo", a group sponsored by the Chinese state, was behind the 12 October 2020 grid failure in Mumbai.

The concept of cyber attack

- The concept of a cyber attack or a computer network attack is rooted in this description.
- It can be described as a "deliberate exploitation of computer systems, technology-dependent enterprises and networks."
- Cyber attacks use "malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft."
- Cyberattacks give a country another option — less devastating than a nuclear attack, but capable of giving the country a strategic and psychological edge. China's recent cyber aggression can be analyzed through this lens.
- Possible reasons for increased cyber attacks from China:
  - One major factor is the border clash between the two countries in June 2020
  - Chinese may be using cyber attacks as a means of deterrence against India
  - Until recent years, China's focus had been on information theft
  - But Beijing has been increasingly active in placing code into infrastructure systems, knowing that when it is discovered, the fear of an attack can be as powerful a tool as an attack itself.
  - When vaccine companies are targeted, the motive could be competition

Different types of Cyberattacks

- **Botnet:** Botnet is a network of devices that have been infected with malicious software, such as a virus.

- **Malware:** Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.
- **Phishing:** Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email.
- **Ransomeware:** Among the types of cyber warfare attacks, ransomware stands as one of the riskiest ones as highly critical information can be at stake. In a ransomware attack, the victim is forced to delete all necessary information from their system if they fail to pay a ransom within the timeline given by cybercriminals.
- **Trojan Horses:** A Trojan is a malware software program that aims at hacking digital devices by appearing as useful software to the victims.
- It is one of the most dangerous types of Cyberattacks. It helps attackers get financial details alongside all other confidential information of the victims.
- **Worm:** A worm is a type of malware that doesn't attack a host file and replicates itself as it travels across computers and networks and leaves copies of itself in the memory of each computer.

What are the major dimensions of cyber threats?

There are three major dimensions of cyber threats:

- **Cyber Wars:** A cyber war is a "No contact" war, where the idea is to attack the critical information (CI) architecture of another state. Israel used STUXNET malware to destroy the Iranian nuclear programme.
- **Cyber Crimes:** Involves use of cyberspace for criminal activity including identity thefts and financial frauds. Eg. Adhaar card data and other biometric information has been hacked
- **Cyber Terrorism:** It is the use of cyberspace by a terrorist group for propaganda and recruitment. Eg. fake videos to incite and radicalize the vulnerable target
- Thus cyber security becomes important for the internal and well as external security of India.

Understanding the current state of cyber security in India:

- **National Security Council: The National Security Council**, chaired by National Security Adviser (NSA), plays a key role in shaping India's Cyber Policy Ecosystem.
- The NSA also chairs the **National Information Board**, which is the apex body for cross-ministry coordination on cybersecurity policymaking.
- **Cyber Security Policy:** The **National Cyber Security Policy, 2013** was developed to build secure and resilient cyberspace for India's citizens and businesses.
- **IT Act, 2000:** Currently, **the Information Act, 2000** is the primary law for dealing with cybercrime and digital commerce in the country.
- **NTRO:** The **National Technical Research Organisation (NTRO)** is the main agency designed to protect national critical infrastructure and to handle all the cybersecurity incidents in critical sectors of the country.
- **NCIIPC:** The National Critical Information Infrastructure Protection Centre (NCIIPC) was established under NTRO in 2014 to facilitate the Protection of Critical Infrastructure.
- **CERT-In:** The Indian **Computer Emergency Response Team (CERT-In)** is responsible for incident responses including analysis, forecasts and alerts on cybersecurity issues and breaches.
- **Indian Cyber Crime Coordination Centre (I4C):** The Central Government has rolled out a scheme for the establishment of the Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

Recent measures

- **Cyber Crime Volunteers:** The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs (MHA), recently launched the Cyber Crime Volunteers Program with the aim to allow citizens to register themselves as "**Cyber Crime Volunteers'**.
- While the country had earlier used **vertical surveillance (**usually state observes the citizens**)**, this new initiative is a case of **Lateral surveillance (**it is the case of social surveillance or peer-to-peer surveillance**).**
- **Cybercrime reporting portal:** The Government has launched the online cybercrime reporting portal, cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries, or sexually explicit content.
- **Cyber Swachhta Kendra:** Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programs and free tools to remove such programs.

What are the gaps in India's Cyber Security?

- The Institutional Framework has been plagued with **concerns around**
  - **lack of effective coordination**
  - **overlapping responsibilities**
  - **lack of clear institutional boundaries and accountability**
- **Outdated strategies:** India's National Cyber Security Strategy, which has been drafted by the NSC — a much-needed update to the National Cyber Security Policy 2013 — is yet to be released.
- **Inappropriate approach to deal with cyber conflict:** India is also **yet to clearly articulate a doctrine** that holistically captures its approach **to cyber conflict**, either for conducting offensive cyber operations, or the extent and scope of countermeasures against cyber attacks.
- **Absence of credible cyber deterrence strategy:** The absence of a credible cyber deterrence strategy means that states and non-state actors alike remain incentivized to undertake low-scale cyber operations for a variety of purposes — espionage, cyber crime, and even the disruption of critical information infrastructure.

International Telecommunication Union (a specialized agency of UN), ranked India HIGH in commitment to cyber security in its **'Global Cyber Security Index -2018'**

What measures are required?

- **Effective strategy and transparency:** Clearer strategy and greater transparency are the need of the hour to improve India's cybersecurity posture.
- **Better coordination:** Improved coordination is needed between the government and the private sector, as well as within the government itself — and at the national and state levels.
- **Focus on creating secure cyber ecosystem:** A clear public posture on cyber defence and warfare boosts citizen confidence, helps build trust among allies, and signals intent to potential adversaries, thus enabling a more stable and secure cyber ecosystem.
- **Learning from expertise:** A key opportunity herein is a precise articulation of how international law applies to cyberspace, which could mold the global governance debate to further India's strategic interests and capabilities.

- In particular, this should include positioning on not just non-binding norms but also legal obligations on 'red lines' with respect to cyberspace-targets that should be considered illegitimate due to their significance for human life, such as health-care systems, electricity grids, water supply, and financial systems.

10 Surveillance reform: The need of Hour

Context:

Recently a report named 'Pegasus Project' was published that says that over "300 verified Indian mobile telephone numbers were targeted using spyware made by the Israeli firm, NSO Group.

Background

■ Surveillance in India

- In India the government can surveillance through existing laws that offer impunity for surveillance. However, there are several issues associated with the surveillance regime.
- The Indian surveillance government relies on existing provisions under **the Indian Telegraph Act of 1885** and the **Information Technology (IT) Act of 2000.**
- These provisions are problematic and give the government complete anonymity regarding its capture and monitoring functions.
- While the provisions of the **Telegraph Act** relate to telephone conversations, IT Act deals with all communications made using a computer application.
- **Section 69 of the IT Act** and the **Restrictions Act of 2009** does not work better than the Telegraph Act, and it provides even the weakest protection against those tested.
- There is no provision, however, that allows the government to hack into anyone's phones as hacking of computer equipment, including cell phones and applications, is a criminal offense under the IT Act.
- However, self-monitoring, whether under the law or outside of it, is a gross violation of the fundamental rights of citizens.

What is Pegasus?

- Pegasus is a spyware that works by sending an exploit link.
- If the target user clicks on the link of spyware, the malware or the code that allows the surveillance is installed on the user's phone.
- Once the Pegasus is installed, the attacker has complete access to the target's phone.
- The first case on Pegasus's spyware operations emerged in 2016, when Ahmed Mansoor, a human rights activist in the UAE, was targeted with an SMS link on his iPhone 6.
- Apple responded by making out an update to "patch" or fix the issue.
- Pegasus delivers "a chain of zero-day exploits to penetrate the security features on the phone and installs Pegasus without the user's knowledge or permission.

About the Pegasus Malware Attack

- The surveillance was carried out on users in 20 countries, "between in and around April 2019 and May 2019".
- The surveillance was carried out by using a spyware tool called **Pegasus** that was developed by an **Israeli firm, the NSO Group.**
- Only a missed call on the app was all that was needed to install the software on the device.
- No clicking on a misleading link was required.

"Zero-day exploit"

- It is a completely unknown vulnerability. Even the software manufacturer is not aware of it, and there is, thus, no patch or fix available for it.

Impact

- **Threat to Freedom of the Press:** Monitoring affects media freedom. In 2019, similar allegations were made about Pegasus' use of journalists and human rights activists.
  - The World Press Freedom Index produced by Reporters Without Borders ranked India in 142 out of 180 countries by 2021.
  - Privacy and free speech are what enable good reporting. They protect journalists from the threat of private and public sanctions through official reporting.
- **Contrary to the Right to Privacy:** The very existence of a security system affects the right to privacy and the exercise of freedom of speech and personal freedom under Articles 19 and 21 of the Constitution, respectively.
  - Fear of citizens knowing that their email is being read by the government could affect their ability to express, accept and discuss unfamiliar ideas.
  - In the absence of secrecy, the safety of journalists, especially those whose work criticizes the government, and the personal safety of their sources are at stake.
- **State of Authorization:** Employment promotes the spread of dictatorship in the public service because it allows managers to exercise an unequal amount of power in the citizenry and have an impact on their lives.
- **Against Procedure:** Employment, when fully implemented by an authority, reduces Articles 32 and 226 of the Constitution as is the case in private.
  - Therefore, the affected person cannot show a violation of their rights. This violates not only the purposes of proper procedure and separation of powers but also violates the requirement of process protection as mandated in **Puttaswamy v. Union of India (2017).**

Analysis

■ Issues with Surveillance system

- Monitoring itself, whether under the law or outside of it, is a gross violation of the fundamental rights of citizens.
- **Violations of freedom of speech:** The existence of a system of surveillance affects the right to privacy and the exercise of freedom of speech and personal freedom under **Articles 19** and **21** of the Constitution, respectively.
- It prevents people from learning and exchanging strange, controversial or provocative ideas.
- **There is no element of legal scrutiny:** There is also no space for the intended person to go to court of law before or during or after or acts of observation as the system itself is confidential.

- **No oversight:** In the absence of parliamentary or legislative oversight, electronic surveillance gives the council the power to influence both subject matter and all categories of people, resulting in a negative impact on free speech.
- **Opposition to the separation of powers:** Constitutional officials such as the sitting judge of the Supreme Court have been reported to be under the control of Pegasus.
- The acquisition of immeasurable power by a single branch of government threatens the separation of state power.
- Existing provisions are not enough to prevent the spread of dictatorship because they allow the authorities to use an unequal amount of power.

What measures are required?

- **Administrative Justice:** In order to satisfy the principle of "proper legal process", to maintain the separation of powers effectively and to meet the requirements of procedural protection and environmental justice, it is necessary to consider judgments.
- Only the judiciary can determine whether certain conditions of oversight are equal, whether there are other complex mechanisms in place, and balancing the need for government objectives with the rights of the people affected.
- The need to oversee the processes of general surveillance systems, as well as the investigation into Pegasus burglary, is also important because leaked details of the target numbers contained the telephone number of a sitting High Court judge sitting, which also casts doubt on Indian independence.
- Monitoring conversion is a need for an hour in India as a complete overhaul of the monitoring framework is outdated.
- Not only is the existing security weakened but the proposed law relating to the protection of personal data of Indian citizens fails to address scrutiny while providing extensive relief to government officials.
- There needs to be greater clarity in the system as in the current system, organs of state are not accountable to anyone other than government itself.
- The current argument, therefore, is not about 'whether to be watched at all', but about 'how, when, and what kind of surveillance'.
- If the purpose of Protecting national security can be achieved through minor violations of fundamental rights, the government is constitutionally obliged to implement a mechanism that, in fact, involves minor violations.
- Changes in the Indian surveillance regime should include code of conduct that looks at the ethical aspects of employment.

11 Need to Understand Cyber Threats before fighting them

Context:

National Cyber Safety and Security Standards is carrying out extensive awareness, training and education campaigns, so that the public are made aware of the dangers of the internet, and how they should be careful and avoid falling into cyber traps. Understanding the concept of cyber threats is important to handle the issue.

How Vulnerable is India?

- India's cyber security chief Gulshan Rai told Parliament's finance standing committee in July 2017, that cyber threats had evolved swiftly from viruses and "nuisance" attacks in the early 2000s to sophisticated malware and advanced denial of service, and could pose the risk of severely destructive attacks by 2020.
- With little control over the hardware used by Indian Internet users as well as the information that is carried through them, India's national security architecture faces a difficult task in cyberspace.
- India's infrastructure is susceptible to four kinds of digital intrusions: espionage, which involves intruding into systems to steal information of strategic or commercial value; cybercrime, referring to electronic fraud or other acts of serious criminal consequence; attacks, intended at disrupting services or systems for a temporary period; and war, caused by a large-scale and systematic digital assault on India's critical installations.

Cyber Crimes

- **Cyber Defamation:** In simple words, it implies defamation by anything which can be read, seen or heard with the help of computers/technology.
- **Corporate Cyber Smear:** Harmful and defamatory online message has been termed as corporate cyber smear.
- **Digital Forgery:** Digital forgery implies making use of digital technology to forge a document.
- **Online Gambling:** The act of gambling is categorized as an offence in some countries and has a legal sanctity in others. The main concern with online gambling is that most virtual casinos are based offshore making them difficult to regulate.
- **Online sale of illegal articles:** There are certain articles like drugs, guns, pirated software or music that might not be permitted to be sold under the law of a particular country.
- **E-mail spamming/e-mail bombing:** Spam refers to sending of unsolicited messages in bulk. Technically, it overflows the limited-sized memory by excessively large input data. In relation to e-mail accounts, it means bombing an e-mail account with a large number of messages maybe the same or different messages.

Cyber Terrorism

Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

- **Pakistan/India Conflict:** As tensions between the neighboring regions of India and Pakistan over Kashmir grew over time, Pro-Pakistan cyber-terrorists and recruited hackers began to target India's Internet Community. Groups such as G-Force and Doctor Nuker have defaced or disrupted service of several major entities in India such as the Zee TV Network, The India Institute of Science and the Bhabha Atomic Research Center which all have political ties.
- **Tamil Tiger Attempt:** In 1998, with surges of violence committed in Sri Lanka over several years, the group known as the Tamil Tigers, a violent guerrilla organization, bombarded Sri Lankan embassies with over 800 e-mails a day.
- **ISIS:** Recent activities of ISIS in Middle East and series of videos released by them are potential cyber terrors. They are using Cyber space for their propaganda and for influencing vulnerable people to join ISIS. It is threat to the world and the way they are growing needs global cooperation to check them before they create havoc.

Tools to Protect Against Cyber Threats

- **Digital Signature:** It is only a technique that can be used for different authentication purposes. For an E-record, it comes functionally very close to the traditional handwritten signatures.
- **Security Audit:** A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria.
- **Encryption:** One of the most powerful and important methods for security in computer systems is to encrypt sensitive records and messages in transit and in storage.
- **Cyber Forensics:** Cyber Forensics is a very important ingredient in the investigation of cybercrimes. Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve a crime.
- **E-discovery:** Investigation includes areas like money laundering, corruption, financial frauds, cybercrimes, serious frauds and white collar crimes investigation, etc. Presently e-discovery services in India are in infancy stage and this is the reason why many cases of corporate frauds and cybercrimes remain unreported.

Cyber Security in India

- **Information Technology Act, 2000:** The Information Technology Act, 2000 intends to give legal recognition to e-commerce and e-governance and facilitate its development as an alternate to paper based traditional methods. The Act has adopted a functional equivalents approach in which paper based requirements such as documents, records and signatures are replaced with their electronic counterparts.
- **Indian Computer Emergency Response Team:** Is an office within the Ministry of Electronics and Information Technology. It is the nodal agency to deal with cyber security threats like hacking and phishing.
- Ministry of Electronics and Information Technology has launched five cyber-security tools, as part of its **Cyber Swachhta Kendra (CSK),** to prevent users from facing threats on the web. These tools are: Bot Removal Tool, USB Pratirodh, App Samvid, M-Kavach, and Browser JS Guard.
- **National Information Infrastructure Protection Centre (NIIPC):** NIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defense. They would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defense and Law enforcement agencies with a view to protecting these agencies' ability to collect, analyze and disseminate intelligence.
- **Standardization, Testing and Quality Certification (STQC) Directorate-**STQC is a part of Department of Information Technology and is an internationally recognized Assurance Service providing organization. It has also established a test/evaluation facility for comprehensive testing of IT security products as per ISO 15408 common criteria security testing standards.
- **The Cyber Regulations Appellate Tribunal:** It has been established by the Central Government in accordance with the provisions contained under Section 48(1) of the Information Technology Act, 2000.

Conclusion

With the huge growth in the number of Internet users all over the world, the security of data and its proper management plays a vital role for future prosperity and potentiality.

12 Data protection and Aadhar security

Context:

What is data protection? What is mean by data protection of Aadhar? Does Aadhar data protection have loop holes? What are the measures taken for Aadhar data protection?

What is data protection?

- Data protection is a concept which seeks to protect the personal data of user which is with data processor (companies and govt.) from leakage and misuse.
- India did not have a strong data protection law and that's why state's obligation to ensure fundament right to privacy was not being honored. That is why Justice B.N. Sri Krishna committee was constituted to give draft personal data protection bill. It provided many recommendations for same.
- Aadhar is a 12 digit unique identification number issued by the Unique Identification Authority of India (UIDAI) to Indian residents. The number is issued after completing a verification process laid down by the UIDAI that involves submission of address proof, date of birth, bio-metrics and IRIS scan.
- Getting your Aadhar card has become extremely important as government has made it mandatory for carrying out financial transactions and to take benefit of several social schemes. But, the extreme involvement of third parties in collecting data for Aadhar card verification has left people skeptical about the safety and protection of all the personal information being shared to unknown sources.

Strength of B.N. Sri Krishna report

- If data is leaked or misused by data processors then there will be penalty.
- 'Critical personal data' of Indian users must be stored and processed in India.
- Data processors have to appoint data protection officers to register and work upon grievances.
- Provision for compensation to users if data is compromised.
- Right to withdraw consent.
- The copy of data, other that critical personal data should be in Indian for investigation.

Weakness of the report

- The draft bill is tilted towards government data processors.
- The consent can be relaxed or waived off for govt. when it collects data.
- Govt. can use data for purpose other than the stated one.
- This may give rise to surveillance state.
- Right to forgotten is in complete as it does not delete the data with data processors

Aadhar security measures

- Protecting the information of an individual is inherently available in the design of the UID project, which is primarily done by the allocation of random 12 digit numbers that do not reveal anything about an individual. In addition to this, there are several other measures UID has taken to safeguard the interests of the residents and to fulfill their objective of data security and collection.

- As per the policy designed by UIDAI, no data collection agency can collect sensitive information about an individual like religion, caste, class, income, community, income, and ethnicity. Thus it is impossible for anyone to profile individuals using the UID system.
- The only response that anyone would receive from the UIDAI system for verifying the identity will either be 'yes' or 'no'. The system is designed in a way that it will not reveal anything from the database other than this.
- The UIDAI database is not linked to any other database or system in any way which may threaten the safety of the information collected. The only purpose of Aadhar database is to verify the identity of an individual while getting any service, which shall only be provided after the consent of the Aadhar holder.
- The UIDAI database is heavily guarded both electronically as well as physically with exception to a few individuals with extremely high clearance. The best in class encryption features are being used to protect the data in a highly secured vault and every access to that vault is properly logged for future reference.
- The severe penalty will be imposed on any kind of security violation or disclosure of the identity information.

Security Concerns That Are Still Unaddressed

- Despite having a stringent security system in place and criminal penalties imposed on all kind of data security breach, the concerns over data security are still very there because of the involvement of third parties in collecting such confidential data. However, a majority of experts time and again have backed the security claims made by UIDAI stating that several governmental agencies like Passport Authority of India have been using third-party agencies for collecting biometric and demographic information.
- If we take this into perspective, it can be said that the involvement of third-party agencies is not something that is happening with government services for the first time. In addition to that, the government has kept some legal status in place that prevents third-party agencies from breaching the security of Aadhar data information. They are only given the responsibility of collecting and transmitting the encrypted data to UIDAI directly and receive acknowledgment for their service. Also, UIDAI has well-placed measures for security and data protection that prevents any kind of security breach to confidential data.

Balanced view

- When we are pursuing Digital India, cashless economy, etc.,we ought to have strong data protection to honour fundamental right to privacy. Justice B.N. Shri Krishna committee works for this purpose. This will raise our global status as a county which honour human rights. Moreover, UIDAI has ensured security of Aadhar data, so there is no need to make unnecessary hue and cry for Aadhar data security. Aadhar linking is being done for administrative conveniences.

13 Debate on Cyber Security in India

Context:

- **A stringent data protection law is urgently needed in India to address the mounting concerns over privacy of citizens as the country is moving in a big way towards digital governance.**

- **We are in the stage of digital economy, digital governance, and digital storage of all knowledge... Digital footprints are everywhere. The digital footprints will identify you... Is it good, is it bad that is the debate.**

Recent Issues

- Cyberattacks on Estonian networks in 2007, on Georgian networks in 2008, and the Stuxnet attack in 2010 that destroyed the Iranian uranium enrichment centrifuges alerted the world to the reality of cyberwarfare.
- It started in mid-March 2017 with international media reports claiming that the profiles of 50 million Facebook users were harvested by UK-based data analytics firm Cambridge Analytica to influence the US presidential election and the pro-Brexit campaign as well as polls in other countries.
- Beyond the global impact of the biggest-ever data breaches and the social media behemoth Facebook, the scandal brought to the fore the shortcomings of India's laws to deal with ever advancing issues of online privacy and data theft in the country.

Nature of Cyber attacks and issues

- Attacks are often anonymous and difficult to attribute to specific actors, state or non-state. Advanced Precision Threats (APTs) carried out by anonymous hackers are often silent and go unnoticed for long periods.
- Detecting and responding to such attacks is a daunting task. Analysts have been debating whether cyber deterrence, on the lines of nuclear deterrence, can dissuade such attackers.
- Cyber deterrence can be of two kinds: by denying attacks (defensive) and by punishment (offensive). Cyber defences are raised so that the attacker is unable to pierce the adversary's networks. In the latter case, the cyber attacker is assured of a devastating response.
- Evidently, neither deterrence by denial nor by punishment works in cyberspace. Attackers are able to bypass the best of cyber defences. For offensive cyber deterrence, it is necessary to identify the attacker with pinpointed accuracy. But attribution is the Achilles heel of offensive cyber deterrence.

Challenges in preventing cyber attacks

- Much like state actors, many companies are developing their own capabilities of going after suspected cyber-attackers in what is called 'hunting'. Such unchecked proliferationof offensive cyber tools and practices can destabilise the entire cyberspace in the absence of any accepted norms of behaviour.
- The international community has been unable to agree on suitable norms of behaviour in cyberspace. In 2013, the UN Group of Government and Experts (UNGGE) had suggested 11norms.
- However, implementing them in cyberspace is a difficult task. In a major setback to the process of norms development, the 2015 UNGGE failed to arrive at a consensus. Presently, there are no acceptable norms of behaviour in cyberspace.

How to address

- The attackers' assets can be targeted in a kinetic military response. Economic sanctions can be imposed. Irrespective of the problems associated with the efficacy of the concept of cyber deterrence, countries are acquiring offensive capabilities in cyberspace. They are building bits of software called 'cyberweapons' that can do enormous damage to the adversary's networks.

- The Indian military needs to make aproper assessment of an offensive cyber doctrine adopted by many countries and undertake action that goes beyond simply the building of defensive capabilities. Offensive cyber response is not limited to states alone.

Issues in India

- In India, it is imperative that cyber networks, software and cyber-physical systems, and platforms should be cyber-secure. This requires a judicious mix of people, policies and technology, as well as robust public-private partnership.
- The reliance on imported information and communication technology (ICT) products and our inability to screen them for vulnerabilities is a major cybersecurity risk.
- Institutions such as the National Cybersecurity Coordinator (NCC), National Technical Research Organisation, Computer Emergency Response Team and the National Cyber Security Coordinator Centre are all doing a reasonable job. But they suffer from the lack of skilled manpower and proper coordination.
- The existing National Information Board (NIB), headed by the National Security Adviser (NSA), duly empowered, can play the role of an apex body in India. NCC, set up in 2015 as a part of the National Security Council Secretariat, should be strengthened to bring about a much-needed synergy among various institutions and to work out a coordinated approach to cyber security, including cyber deterrence.

14 Issues related to Border Management

Context:

Recent developments at India's border warrant a comprehensive review of border management to ensure the all-weather security of its borders.

Background

- India has 14,880 kilometres of land border running through 92 districts in 17 States and a coastline of 5,422 kilometres touching 12 States and Union Territories.
- India also has a total of 1197 islands accounting for 2094 kilometres of additional coastline. There are 51 Bangladeshi enclaves (area involved 7,110.02 acres) in India and 111 Indian enclaves (area involved 17,158.13 acres) in Bangladesh.
- In fact, barring Madhya Pradesh, Chhattisgarh, Jharkhand, Delhi and Haryana, all other States in the country have one or more international borders or a coastline and can be regarded as frontline States from the point of view of border management.
- From **Sir Creek** to the **Bay of Bengal,** India's land borders present a geographical diversity of a unique kind.
- Much of its borders are topographically difficult. Challenges in border management are peculiar. Hence, 'the proper management of borders is vitally important for national security.'

Analysis

■ India's Land Border Management

- India's border management is an integral part of India's defence and commerce.
- The state secures **sovereignty** through maintaining and regulating borders with neighbouring countries.
- India shares a land border with **7 countries**- Afghanistan, Pakistan, Bangladesh, China, Nepal, Bhutan, and Myanmar.
- India's border management comprises of border region development, communication, and coordination with the neighbouring states and programs to enhance the national interests of India. India has a multidimensional border management problem.
- Managing land borders is very different from managing coastal and riverine borders.

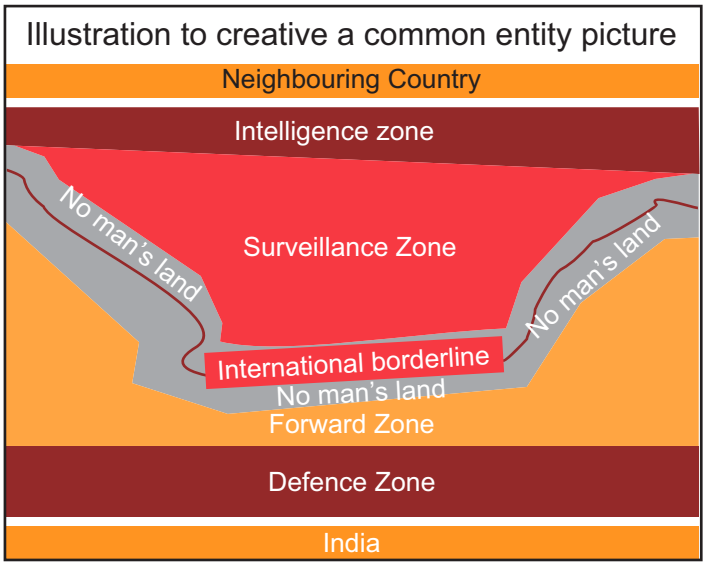
Type of Land border

India has three types of land border: international borderline (IBL), line of control (LoC) and line of actual control (LoAC).

- IBL is the demarcation that has been agreed upon and ratified by both the neighbouring countries, and has been accepted by the rest of the world.
- LoC is the de facto border and separates Pakistan-occupied Kashmir from India's state of – Jammu & Kashmir.
- LoAC is the boundary line that separates Indian-held lands from Chinese-controlled territory. The disputed and unsettled nature of our boundaries (both land and maritime) has made their security much more difficult.

■ Coastal Borders

- The management of Coastal borders is a problem of a different scale altogether.
- The **Mumbai terror attacks** brought home the need to strengthen coastal surveillance.
- **Coast Guard patrols** the territorial sea while the Navy operates in the high seas.
- Sea routes are used to **smuggle** people, arms, drugs and other contraband.
- India has made some progress in improving the coast surveillance but it is difficult to achieve total success.



■ Solution

- The government is thinking of setting up a **maritime commission** to deal with coastal security.
- This will help bring the required focus on the problem, **improve the coordination** and help **monitor** the various projects.
- **Coastal police** need to be strengthened.
- The **use of technology** becomes imperative in managing large borders, be it on land or the sea or the rivers.
- In **particular GPS**, satellite surveillance become important.

Island Territories

- The ANI are two groups of islands—the **Andaman Islands and the Nicobar Islands**, covering an area of 8,249 sq km.
- The islands are governed as **a single Union Territory** by the Central Government of India, through the Andaman Nicobar Administration.
- The ANI are also home to India's **only integrated tri-service command of the armed forces**—the Andaman and Nicobar Command for maritime surveillance and enhancing India's strategic presence in the eastern Indian Oceanas it merges into the Pacific.
- Being the common maritime space between India and Southeast Asia, the Bay of Bengal and the adjoining Andaman Sea are cardinal for peninsular India's strategic manoeuvres.
- At the same time, India's aspirations in the Bay co-exist with its apprehensions over the belligerent rise of China in these waters.
- As the sole archipelago of the Bay, striding important **Sea Lines of Communication** (SLOCs) and overlooking the Malacca Strait, the Andaman and Nicobar Islands are extremely critical for India's strategic interests.
- However, for years since independence in 1947, the Indian government regarded the development of the islands with **"benign neglect",** despite repeated proposals for the establishment of a transhipment port and bunkering facilities, amongst others.
- While this passivity has made it difficult to undertake rapid construction measures, it had not been cultivated without reason.

- The problems of island territories require a **special focus and approach**.
- Andaman and Nicobar Islands are highly strategic as well as ecologically fragile.
- We need special policies for the development of these islands. The same can be said of the Lakshadweep Islands.

Shekatkar Committee recommendations

- Government has accepted and implemented three important recommendations of Committee of Experts (CoE) under the Chairmanship of Lt General D B Shekatkar (Retd) relating **to border Infrastructure.**
- These were related to **speeding up road construction**, leading to socio economic development in the border areas.
- On the matter related to creating border infrastructure, the Government has implemented recommendation of CoE to **outsource road construction** work beyond optimal capacity of Border Roads Organisation (BRO).
- It has been made mandatory to adopt **Engineering Procurement Contract** (EPC) mode for execution of all works costing more than Rs 100 crore.
- New Technology **like blasting technology** for precision blasting, **use of Geo-Textiles** for soil stabilisation, **cementitious base for pavements**, **plastic coated aggregates** for surfacing, is also being used to enhance the pace of construction.

Why multiple security agencies increases the complexity of border management?

- India's border sharing itself makes India's task more complex than most other countries. This complexity is accentuated by the fact that along with the army, we have multiple other security agencies — the **Central Armed Police Force (CAPF)** and the **Paramilitary Forces (PMF)** — sharing the responsibility.
- While the **army** is deployed along the LoC and AGPL, the **Border Security Force (BSF)** looks after the international border with Pakistan and Bangladesh.
- Guarding the LAC has been assigned to the **Indo-Tibetan Border Police (ITBP)** and **Assam Rifles.**
- The **Sashastra Seema Bal (SSB)** is responsible for guarding the borders with Nepal and Bhutan.
- The **Assam Rifles** looks after our border with Myanmar.
- In a nutshell, in addition to the army, we have four agencies guarding borders with six neighbours. Conversely, maritime borders are guarded by a single agency — the **Coast Guard.**

Department of border management (DBM)

- A department of border management (DBM) in the MHA was set up.
- DBM has been spearheading the border management effort in the country.
- Some of the tasks it has performed are: the construction of the border guarding infrastructure, construction of integrated check posts to facilitate trade and movement of people, socio-economic development of border areas.
- MHA also equips and trains the border guarding forces.
- A principle of 'one border one force' has been accepted to streamline the deployment of border guarding forces.

Issues emerged due to multiple security agencies

- **Lack of coherent policy**: Due to multiple bodies, there is a lack of a coherent policy on training, planning and the conduct of guarding operations among various outfits.
- **Lack of coordination:** Overall coordination is also affected.
- Going by the instances along the western border, our adversary has often escalated violations by resorting to the prolonged use of military resources.
- Similarly, their modus operandi has also undergone a qualitative change whereby they have buttressed border security by co-opting military battle drills and sub-unit tactics such as sniping, launching raids and ambushes on the Loc/international border by deploying regular troops.
- Chinese provocations along the LAC are military operations. Clearly, the peace-time scenario is now by and large militarised.

How a 'single security agency' can solve India's issues?

- India needs a single security agency adequately equipped, suitably armed and trained in advanced military drills and sub-unit tactics to guard our borders.
- The manpower and infrastructure should be created by pooling and merging the resources of the CAPF and Assam Rifles.
- Further, to augment the battle efficiency, a fixed percentage of manpower, including the officer cadre, should be drawn on deputation from the army.
- The proposed outfit, let's call it the National Border Guard, (NBG), should have the explicit mandate to effectively retaliate against cross-border transgressions and stabilise the situation till the operations are taken over by the armed forces.

Global practice

Most countries have raised specialised and dedicated armed bodies for border security. For example-

- Iran has the **Border Guard Command**
- Italy has the **Border Police Service**
- Russia has created a **Border Guard Service**
- US has **Homeland Security**.
- Closer home, in China, it is the **People's Armed Police**, while Pakistan has a **Frontier Corps** for its western border and the **Rangers** looking after the Indo-Pak Border.

Way Forward

India's territorial borders, both land and sea, suffer from diverse physical, ethnic and cultural contradictions. While the state has a major role in securing war frontier, the **populations** along territorial peripheries, too, can play an important role in securing our interests. The people living in these areas are the **most important ingredient** towards a secure and safe border area. This would entail **reconceptualising the concept of border guarding** to effective border management, where local people became the centre of gravity of all actions. The border guarding forces have to evolve ways and means to mainstream **the local population in the management of the border areas.**

****