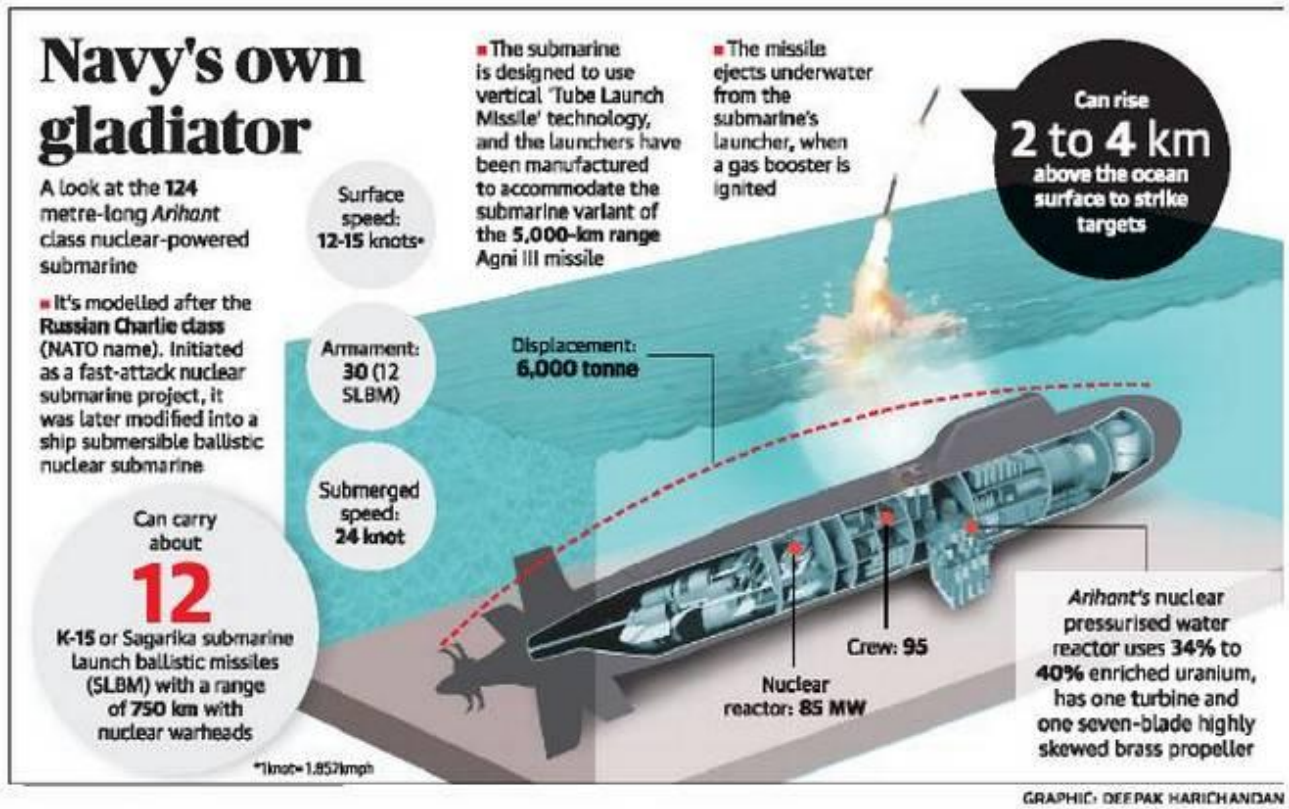
09-01-2018

INS Arihant

- INS Arihant is India's only operational ship submersible ballistic nuclear (SSBN) asset.
- It is its most dependable platform for a second-strike.
- This is because the other options, land-based and air-launched, are easier to detect.
- Arihant has been immobilised after 'accident' 10 months ago
- It can stay undetected deep underwater for long periods and ranges far and wide.
- INS Arihant and other nuclear launch platforms are operationally handled by the Strategic Forces Command.
- They report to the Nuclear Command Authority chaired by the Prime Minister.
- However, over 100 nuclear warheads are not mated with missiles or bombs and remain in civilian custody of the Atomic Energy Department and the DRDO.



Nuclear Command Authority (NCA)

- It is responsible for command, control and operational decisions regarding India's nuclear weapons programme.
- Organisational structure of NCA includes Political Council and Executive Council.
- Executive Council is headed by National Security Advisor and Political Council is headed by Prime Minister.

- The Executive Council gives its opinion to the Political Council, which authorises a nuclear attack when deemed necessary.
- This kind of organisational structure is created to prevent the accidental or unauthorised use of nuclear weapons.
- Strategic Forces Command is a part of Nuclear Command Authority, responsible to operationalize the directives of NCA and for the management and administration of the country's tactical and strategic nuclear weapons stockpile.
- SFC is headed by Commander-in-chief of the rank of Air Marshal.
- It will have the sole responsibility of initiating the process of delivering nuclear weapons and warheads, after acquiring explicit approval from the NCA.

Mankidia Tribe

- Mankidia is one of the 13 Particularly Vulnerable Tribal Groups (PVTG) in Odisha.
- They critically depends on making rope with siali fibre that's richly available in Similipal Tiger Reserve (STR).
- They were denied habitat rights inside the STR under Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Forest Rights) Act, 2006.
- So they would now be deprived of the non-timber forest produce.
- This is because the State Forest Department has objected on grounds that tribals could be attacked by wild animals.
- Had it been approved, the Mankidia would have been the first PVTG to have habitat rights.
- In Odisha, processes have been initiated for according habitat rights to PVTGs such as Bondas, Didai, Hill Khadia and Paudi Bhuyan.
- "'Habitat' as defined under the FRA includes the area comprising the customary habitat and such other habitats in reserved forests and protected forests of primitive tribal groups and pre-agricultural communities and other forest dwelling STs.

Pratyush

- Pratyush is an array of computers recently unveiled in India.
- It can deliver a peak power of 6.8 petaflops.
- One petaflop is a million billion floating point operations per second and is a reflection of the computing capacity of a system.
- The machines will be installed at two government institutes: 4.0 petaflops HPC facility at Indian Institute of Tropical Meteorology (IITM), Pune & 2.8 petaflops facility at the National Centre for Medium Range Weather Forecast, Noida.
- Pratyush is also the fourth fastest supercomputer in the world dedicated for weather and climate research.

- A key function of the machine's computing power would be monsoon forecasting using a dynamical model.
- With the new system, it would be possible to map regions in India at a resolution of 3 km and the globe at 12 km.

Web portal to accept online abuse cases

- The Ministry of Home Affairs is set to launch a web portal where people who have faced online abuse can register complaints on a real-time basis.
- It includes victims of cybercrimes like financial frauds.
- The Centre also plans to give access rights to banks on the portal to address cases of fraudulent transactions online.
- According to India's Computer Emergency Response Team (CERT-In), there was a 21% increase per year in incidents of cybercrime.
- The portal has also been readied on the directives of a committee appointed by the Supreme Court to check circulation of child pornography and sexual violence videos on the Internet.

Source: PIB, The Hindu

09-01-2018

THE HINDU

A PAPER ANALYSIS

1. Cybercrime Victims can Complain Online

Front Page no-1

Topic : Gs-3 Science and technology, Gs-2 Governance

Cybercrime is a criminal action that encompasses mobile phones, laptop, network, and computer. It is a threat to country's external and internal security and monetary status. Crimes committed against publics with an illicit intention to cause physical or psychological harm, or loss to the victim directly or indirectly, by means of contemporary telecommunication networks such as social media network, the Internet and mobile phones. In States and Union Territories, Cyber Crime Cells have been set up for reporting and investigation of Cyber Crime cases. Apart from that, in the States of States of Arunachal Pradesh, Kerala, Assam, Mizoram, Nagaland, Meghalaya, Tripura, Manipur and Jammu & Kashmir, Government of India has additionally set up cyber forensic training and investigation labs for the training of Law Implementation and Judiciary.

Types and prevention of cyber crime

In technically driven society, people use various devices to make life simple. Globalization results in connecting people all around the world. The increasing access to and continuous use of technology has radically impacted the way in which people communicate and conduct their daily lives. The internet connects people and companies from opposite sides of the world fast, easily, and relatively economically. Nevertheless, the internet and computer can pose some threats which can have disparaging impact on civilisations. Cybercrime is a hazard against different organisations and people whose computers are connected to the internet and particularly mobile technology.

Cybercrime is a dangerous crime involving computers or digital devices, in which a computer can be either a target of the crime, a tool of the crime or contain evidence of the crime. Cybercrime basically defined as any criminal activity that occurs over the Internet. There are many examples such as fraud, malware such as viruses, identity theft and cyber stalking. In present environment, since most information processing

depends on the use of information technology, the control, prevention and investigation of cyber activities is vital to the success of the Organizations, Government's agencies and individuals. The procurement and maintenance of highly skill cybercrime expert by Government and Business Enterprises cannot be exaggerated.

Earlier, cybercrime was committed mainly by individuals or small groups. Presently, it is observed that there is highly complex cybercriminal networks bring together individuals at global level in real time to commit crimes.

Today, criminals that indulge in cybercrimes are not motivated by ego or expertise. Instead, they want to use their knowledge to gain profits promptly. They are using their capability to snip, deceive and exploit people as they find it easy to generate money without having to do an honest work. Cybercrimes have become major threat today.

Cybercrimes are broadly categorized into **three** groups such as crime against

1. Individual
2. Property
3. Government

1. Individual:

This type of cybercrime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". In present situation, law enforcement agencies are considering such cybercrime very serious and are joining forces worldwide to reach and arrest the committers.

2. Property:

Same as in the real world where a criminal can steal and pickpocket, even in the cyber world, offenders resort to stealing and robbing. In this case, they can steal a person's bank details and drain off money; misuse the credit card to make frequent purchases online; run a scam to get naive people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

3. Government:

Crimes against a government are denoted to as cyber terrorism. If criminals are successful, it can cause devastation and panic amongst the citizen. In this class,

criminals hack government websites, military websites or circulate propaganda. The committers can be terrorist outfits or unfriendly governments of other nations.

Types of Cyber Crimes:

There are many types of cybercrimes:

Hacking:

In this category, a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is categorized as a wrongdoing and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location. Many crackers also try to gain access to resources through the use of password cracking soft wares. Hackers can also monitor what users do on their computer and can also import files on their computer. A hacker could install several programs on to their system without their knowledge. Such programs could also be used to steal personal information such as passwords and credit card information.

Theft:

This type of cybercrime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Nowadays, the justice system is addressing this cybercrime and there are laws that avert people from unlawful downloading.

Cyber Stalking:

This is a type of online harassment wherein the victim is endangered to a barrage of online messages and emails. Normally, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more dejected.

Identity Theft:

This is a major problem with people using the Internet for cash transactions and banking services. In this cybercrime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card, full name and other sensitive information to drain off money or to buy things online in the victim's name. The

identity thief can use person's information to fraudulently apply for credit, file taxes, or get medical services. It can result in major financial losses for the victim and even spoil the victim's credit history.

Malicious Software:

This software, also called computer virus is Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to gather sensitive information or data or causing damage to software present in the system.

Child soliciting and Abuse:

This is also a type of cybercrime in which criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms visited by children in order to reduce and prevent child abuse and soliciting.

Virus dissemination: Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, web jacking, e-mail bombing etc.).

Computer vandalism:

It is a type of cybercrime that Damages or destroys data rather than stealing. It transmits virus.

Cyber terrorism: It is a use of Internet based attacks in terrorist activities. Technology savvy terrorists are using 512-bit encryption, which is impossible to decrypt.

Software piracy: It is a theft of software through the illegal copying of genuine programs. Distribution of products intended to pass for the original. If an individual with a single user license loads the software onto a friend's machine, or if a company loads a software package onto each employee's machine without buying a site license, then both the single user and the company have broken the terms of the software license agreement and are therefore guilty of software piracy. Software piracy involves the unauthorized use, duplication, distribution, or sale of commercially available software. Software piracy is often labelled as soft lifting, counterfeiting, Internet piracy, hard-disk loading, OEM unbundling and unauthorized renting.

Denial of service attacks: This crime is committed by the criminal, who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access.

09-01-2018

2. The age of crypto-economics {Digital Economy}

(The Hindu)

Front Page no-8

Topic : Gs-3 Science and technology, Economic Development

Why in news?

The Finance Ministry recently issued a statement warning against investing in bitcoin and other cryptocurrencies (CCs).

Likening CCs to 'Ponzi schemes', it linked them to terror-funding, smuggling, drug-trafficking, and money-laundering.

Why the distrust?

Aspects of the bitcoin phenomenon have attracted great interest

• The challenge it poses to states and central banks.

• The potential of its underlying technology to unleash a new wave of creative destruction.

World's top central bankers have finally realised the futility of trying to control CCs. They are preparing to join them — by issuing their own Central Bank Digital Currency (CBDCs).

Central Bank Digital Currency (CBDCs)

- Central bank digital currency (CBDC) (also called **"Digital Fiat Currency"** or "**digital base money**") is the digital form of fiat money which is a currency established as money by government regulation or law.
- Central bank digital currency is different from "**digital currency**" (or virtual currency and cryptocurrency), which are not issued by the state and lack the legal tender status declared by the government. As such, public digital currencies could compete with commercial bank deposits and challenge the status quo of the current fractional reserve banking system

Benefits and Impacts

Digital fiat currency is currently being studied and tested by governments and central banks in order to realize the many positive implications it contributes to financial

inclusion, economic growth, technology innovation and increased transaction efficiencies.

• **Safety of payments systems:** A secure and standard interoperable digital payment instrument issued and governed by a Central Bank and used as the national digital payment instruments boost confidence in privately controlled money systems and increase trust in the entire national payment system while also boosting competition in payment systems.

• **Protection of money as a public utility:** digital currencies issued by central banks would provide a modern alternative to physical cash – whose abolition is currently being envisaged.

• **Preservation of seigniorage income:** public digital currency issuance would avoid a predictable reduction of seignior age income for governments in the event of a disparition of physical cash.

• **Financial inclusion:** safe money accounts at the central banks could constitute a strong instrument of financial inclusion, allowing any legal resident or citizen to be provided with a free or low-cost basic bank account;

• **Technological efficiency:** instead of relying on intermediaries such as banks and clearing houses, money transfers and payments could be made in real time, directly from the payer to the payee.

• **Banking competition:** the provision of free bank accounts at the central bank offering complete safety of money deposits could strengthen competition between banks to attract bank deposits, for example by offering once again remunerated sight deposits.

• **Monetary policy transmission:** the issuance of central bank base money through transfers to the public could constitute a new channel for monetary policy transmission (ie. helicopter money), which would allow more direct control of the money supply than indirect tools such as quantitative easing and interest rates, and possibly lead the way towards a full reserve banking system.

• **Financial safety:** CBDC would limit the practice of fractional reserve banking and potentially render deposit guarantee schemes less needed.

Risks

A general concern is that the introduction of a CBDC would precipitate potential bank runs and thus make banks' funding position weaker.

Issue

In order to be functional, a virtual currency must solve the problem of double spending.

Given that anything digital can be copied, how do you prevent someone from spending the same unit of currency twice?

Solution

Nakamoto solved the double spending problem by designing a decentralised ledger that bundles data about transactions into blocks, timestamps them, and links each new block of transactions with the previous one in an immutable chain of blocks that are copied, authenticated, and updated continuously, and publicly, on thousands of computers — the blockchain.

3.Contested history *{Indian Politics}*

(The Hindu)

Front Page no-8

Topic,Gs-2 Governance,Polity

Context

Relations of the Government with the Hill Tribes of the North-East Frontier of Bengal.

Alexander Mackenzie's monumental work, History of the Relations of the Government with the Hill Tribes of the North-East Frontier of Bengal , first published in 1884

Lushai Expedition

The British Indian Army Lushai Expedition of 1871 to 1872 was a punitive incursion under the command of Generals Brownlow and Bourchier.

Objective

09-01-2018

To rescue British subjects who had been captured by the Lushais in raids into Assam—including a six-year-old girl called Mary Winchester—and to convince the hill tribes of the region that they had nothing to gain and everything to lose by placing themselves in a hostile position towards the British Government.

For the British, the expedition was a success: the prisoners were freed and the hill tribes agreed to negotiated peace terms. The border region was to remain peaceful until 1888 when large scaled raiding was resumed and another punitive expedition was organised.

After turning the Burmese out of Assam during the First Anglo-Burmese War in 1824, the Bengal Government of the East India Company attempted to administer all that was not absolutely necessary for the control of the frontier through Purandar Singha a native prince; this arrangement failed, and Assam became a non-regulation province in 1838. On its southern borders lay the Lushais, the principal tribes known to Assam being Thadoe and Poitoo Kukies. For many years, long before the British occupation, the inhabitants of the plains to the south had lived in dread of the Kukies, who used to come down and attack the villages, massacring the inhabitants, taking their heads, and plundering and burning their houses.

Boundary modifications

- In 1834, when the boundary of Manipur was redrawn to gift the disputed Kabaw valley to Burma, Chassad-Kuki settlements were left neither in Manipur nor Burma.
- This 1834 line came to be known as the **Pemberton Line,** after Capt. R. Boileau Pemberton who drew it along the foot of "**Muring hills**" (British records), indicating that these hills were once the domain of the Maring Nagas.
- The boundary was redrawn to bring Chassad within Manipur and this brought peace. The boundary became the **Pemberton-Johnstone Line** after Col. James Johnstone, head of the 1881 boundary commission. Burma was invited but failed to turn up.
- This boundary was modified again in 1896 and thereafter came to be known as the **Pemberton-Johnstone-Maxwell Line**. This is the line ratified by the Rangoon Agreement of 1967 between India and Burma. The 1834 line is India's earliest demarcated international boundary.

09-01-2018

4. Behavioural economics needs a unifying theory *{Economy}*

(Livemint)

Topic :Gs-Economic Development

Context

Economics models are mathematical in nature, and representing the full complexity of human behaviour with math would make models unwieldy

Issues

- Behavioural ideas are difficult to put into economic models. For one thing, many psychological biases and irrationalities involve people behaving in very complex, situation-dependent ways. Economics models are mathematical in nature, and representing the full complexity of human behaviour with math would make models unwieldy.
- A second problem is that drawing too many different insights can lead to a problem called overfitting.

Solution

- **Enter Xavier Gabaix**. The French-born Harvard professor has been on somewhat of a mission to incorporate behavioural economics into the mainstream.
- Gabaix's unified theory is based on limited human attention. Standard economic theory requires that consumers and businesspeople pay close attention to a vast array of prices, quantities and other information.

09-01-2018

5. Larger Bench to decide on Sec. 377

{The Hindu}

Front Page no-1

Topic ,Gs-2 Governance,Polity

Petition seeks to quash law criminalising homosexualitySocietal morality changeswith time: Supreme CourtConcept of consensual sex may need more protection: apex court

- Petition Seeks Quashing of law Criminalising
- Social Morality Changes with time Supreme Court
    - Concept of Consensual Sex may need more Protection :apex Court

6.Madhubani Painting
{The Hindhu}

Front Page no-2

Topic :Gs-1 Art and Culture

Madhubani painting originated from Maithili village of the Bihar. Primarily, the womenfolk of the village drew the paintings on the walls of their home, as a demonstration of their feelings, hopes, and ideas.

Later these paintings started becoming a part of festivities and special occasions. Gradually, the Madhubani painting traversed the traditional boundaries and began arriving experts of art, both at the national as well as the international level.

Base and style

The base of freshly plastered mud wall of huts has now been replaced by cloth, handmade paper, and canvas. Since the paintings have been restricted to a limited geographical range, the themes, as well as the style, are not diverse. These paintings make use of three-dimensional images.

Color

The colors that are used are derived largely from plants.

Themes of Madhubani Paintings

The themes on which these paintings are based include nature and mythological events. It revolves around Hindu deities like Krishna, Lakshmi, Shiva, Durga, Rama, and Saraswati.

The natural themes that are used incorporate the Sun, the Moon, and the religious plants. There are some paintings with themes based on court scenes and social events.

If any unfilled space is left after painting the central theme, it is filled up with the motifs of animals, flowers, and birds or geometric patterns.

Making Madhubani Paintings

Madhubani paintings use the brush made of cotton, draped around a bamboo stick. There is no shading in the application of colors. A double line is drawn for outlines and the gap is filled with either cross or straight miniature lines.

- Black color is made by mixing coal to cow dung
- Yellow color from combining turmeric with the milk of banyan leaves
- Blue color from indigo
- Red from the kusam flower juice or red sandalwood
- Green color from the leaves of the wood apple tree
- White from rice powder
- Orange color from palasha flowers