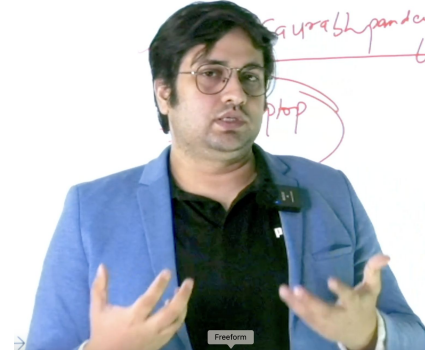


Topics - MINDS MAPS included



- What is Demand-Pull Inflation?
- cyberthreat
- Chandipura virus (CHPV)
- National Cyber Security Policy 2013
- What is Short Selling?
- Court of Arbitration for Sports
- Overview of AUKUS
- **Mains**



By saurabh Pandey



Target Mains -2024/25 -

Q 'AI will make cyberspace more vulnerable'

Elucidate

Connect with sir
9057921649

send your answer - Saurabh pandey
upsc telegram channel



Saurabh Pandey CSE

Saurabh Pandey CSE

4.8★

77 reviews

1K+

Downloads

3+

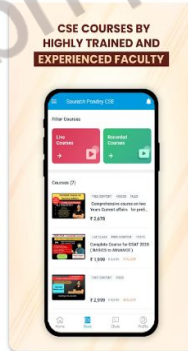
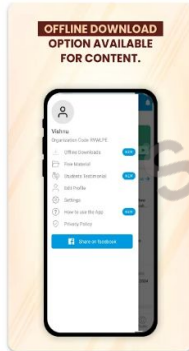
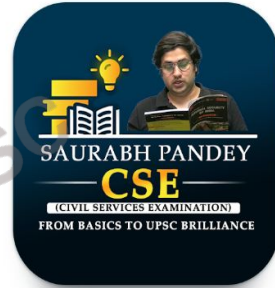
Rated for 3+ ○

Install

Share

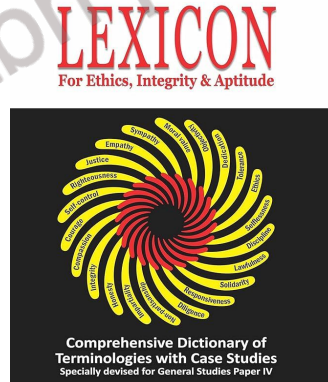
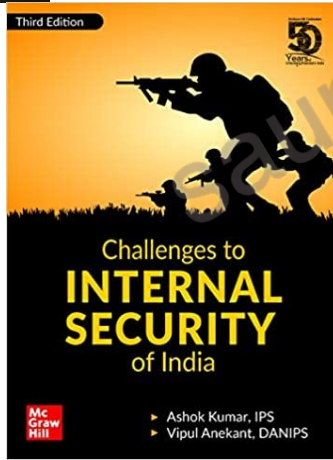
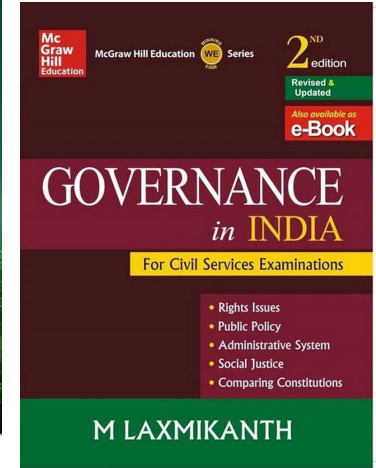
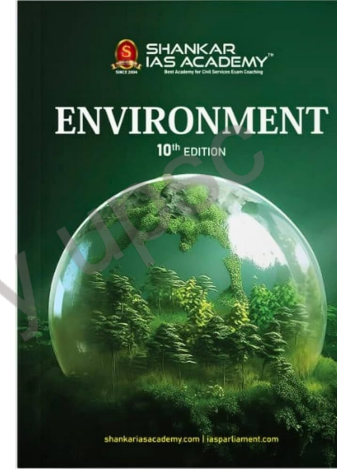
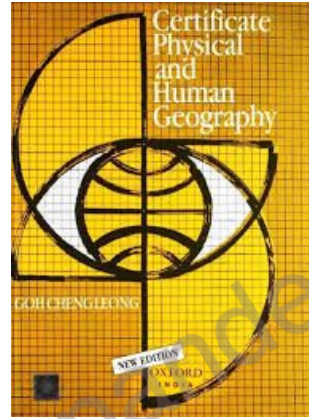
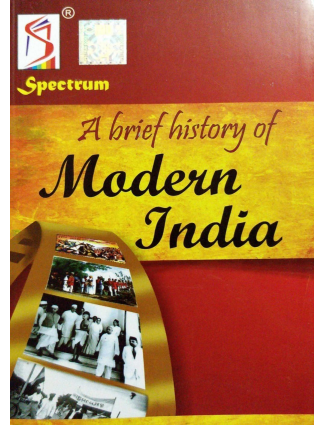
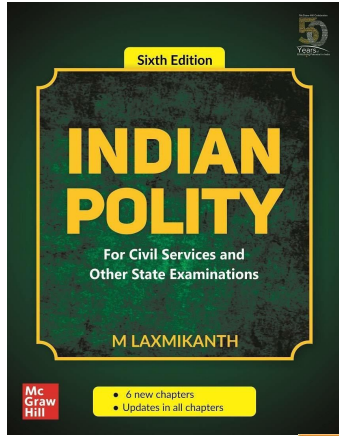
Add to wishlist

This app is available for your device



App support ▾

ALL Advance books for upsc IN ONE COURSE



Chronicle
Nurturing Talent Since 1990

Starting 1st june

Visit -
saurabhpandeyupsc.com

Msg - 9057921649

Topic-What is Demand-Pull Inflation?

Understanding Demand-Pull Inflation

Definition: Demand-pull inflation occurs when the demand for goods and services exceeds their supply.

Causes:

Increased consumer spending 💰

Government spending 📈

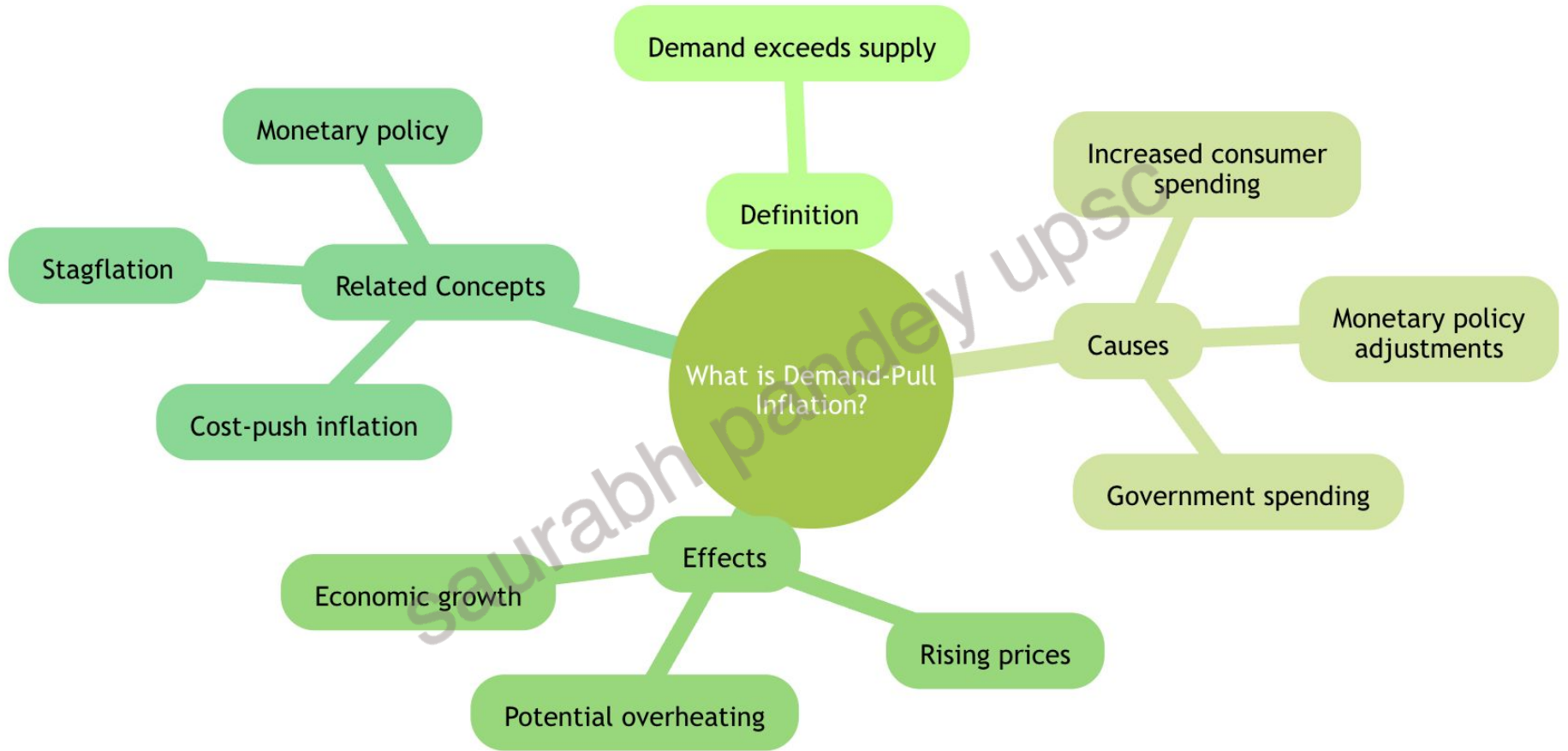
Monetary policy adjustments (e.g., low interest rates) 🏦

Effects:

Rising prices 📈

Economic growth (in the short term) 📊

Potential overheating of the economy 🔥



Topic- Chandipura virus (CHPV)

- Chandipura virus (CHPV) is a member of the genus Vesiculovirus within the family Rhabdoviridae.
- It is a negative-sense, single-stranded RNA virus. CHPV was first isolated in 1965 from the brains of children who had died of encephalitis in the Chandipura village of Bihar, India, hence its name.
- The virus is primarily transmitted through the bite of infected Aedes mosquitoes, and it can cause severe disease in humans, particularly affecting the central nervous system.

- **Chandipura virus infection in humans can lead to a range of symptoms, including fever, headache, nausea, vomiting, and in severe cases, encephalitis, which can be fatal.**
- **The virus has been reported to cause outbreaks with high case fatality rates, particularly among children under the age of 15.**
- **There is no specific treatment for Chandipura virus infection, and management is supportive, focusing on relieving symptoms and complications.**

- **Epidemiologically, CHPV has been associated with regions in India, particularly the states of Bihar, Uttar Pradesh, and Gujarat.**
- **There have been sporadic outbreaks reported, with the virus remaining a public health concern due to its potential to cause severe disease and the lack of specific treatments or vaccines.**
- **Surveillance and control measures, including mosquito control programs, are important to prevent the spread of CHPV.**
- **Additionally, research into the development of vaccines and antiviral therapies is ongoing to address this and other emerging infectious diseases.**

Topic- cyberthreat

- It is indeed true that spreading disinformation has become far easier with the advent of AI.
- Deep fakes, comprising digitally manipulated video, audio, or images, repeatedly hit the headlines today, causing a miasma of disinformation.
- The truth is revealed much later — and after the damage has been done.

- **A ‘glitch’ in a software update concerning Microsoft Windows caused a massive outage, which initially affected parts of the United States, but rapidly spread to different parts of the globe, including India.**
- **It disrupted flight operations, air traffic, stock exchanges and more.**
- **The Indian Computer Emergency Response Team (CERT-IN) issued a severity rating of ‘critical’ for the incident.**
- **This was, however, not a cyberattack, but it provided a preview of the kind of disruption that could take place in the event of a cyberattack**

- **widespread disruption that occurred in 2017 in the wake of the WannaCry ransomware attack employing the WannaCry ransomware cryptoworm, which infected well over 2,30,000 computers in 150 countries, resulting in damage amounting to billions of dollars.**
- **The same year witnessed another cyberattack using the Shmoon Computer Virus which was directed mainly against oil companies such as SA ARAMCO (Saudi Arabia) and RasGas (Qatar), and was labelled, at the time, as the ‘biggest hack in history’.**

Again, around the same period, a cyber attack involving the ‘Petya’ Malware severely affected banks, electricity grids and a host of other institutions across Europe and the United Kingdom, as also the U.S. and Australia.

Few cyberattacks have, however, had a more devastating impact than that caused by the Stuxnet ‘attack’ in 2010. Over 2,00,000 computers were impacted and physically degraded as a result.

Stuxnet was a malicious computer worm, believed to have been in development for nearly \square five years, and specifically targeting supervisory control and data acquisition systems.

The target in this case was the Iran nuclear programme, leading to the inference that it was state sponsored

Steps to overcome cyber threat

- One of the most widespread cyber frauds is ‘phishing’, that involves stealing personal information such as customer ID, credit\debit card numbers, and even PIN.
- . Industry and private institutions, however, appear to be lagging behind. It is the latter segment that is, perhaps, the most vulnerable to digital attacks. Having in place firewalls, antivirus defences and a good back-up and disaster recovery system are not enough.
- Most CEOs of companies, again, are not adequately equipped to deal with digital threats.

- Hence it might be useful to have a chief information and security officer to look at their systems and advise them as to what they should do.
- Awareness of the growing danger of digital threats is but the first step in the battle against cyber and AI-directed threats.
- Unauthorised use of Generative AI content has already become the stock-in-trade of digital bullying.
- Preventing this demands a great deal of effort and adequate budgetary allocations — whether in the private or public domain.

Overview

**Cybersecurity is crucial to protect sensitive information.
Awareness and proactive measures are key to combatting threats.**

Main Steps:

Awareness

**Understanding types of cyber threats.
Educating employees about phishing and scams.**

Risk Assessment

**Identify vulnerabilities within systems.
Evaluate the potential impact of threats.**

Implementation of Security Measures

**Firewalls and Antivirus Software.
Regular updates and patches to software.**

Data Encryption

Encrypt sensitive data to prevent unauthorized access.

Incident Response Plan

Develop a plan for responding to cyber incidents.
Regular drills to test the effectiveness of the plan.

Continuous Monitoring

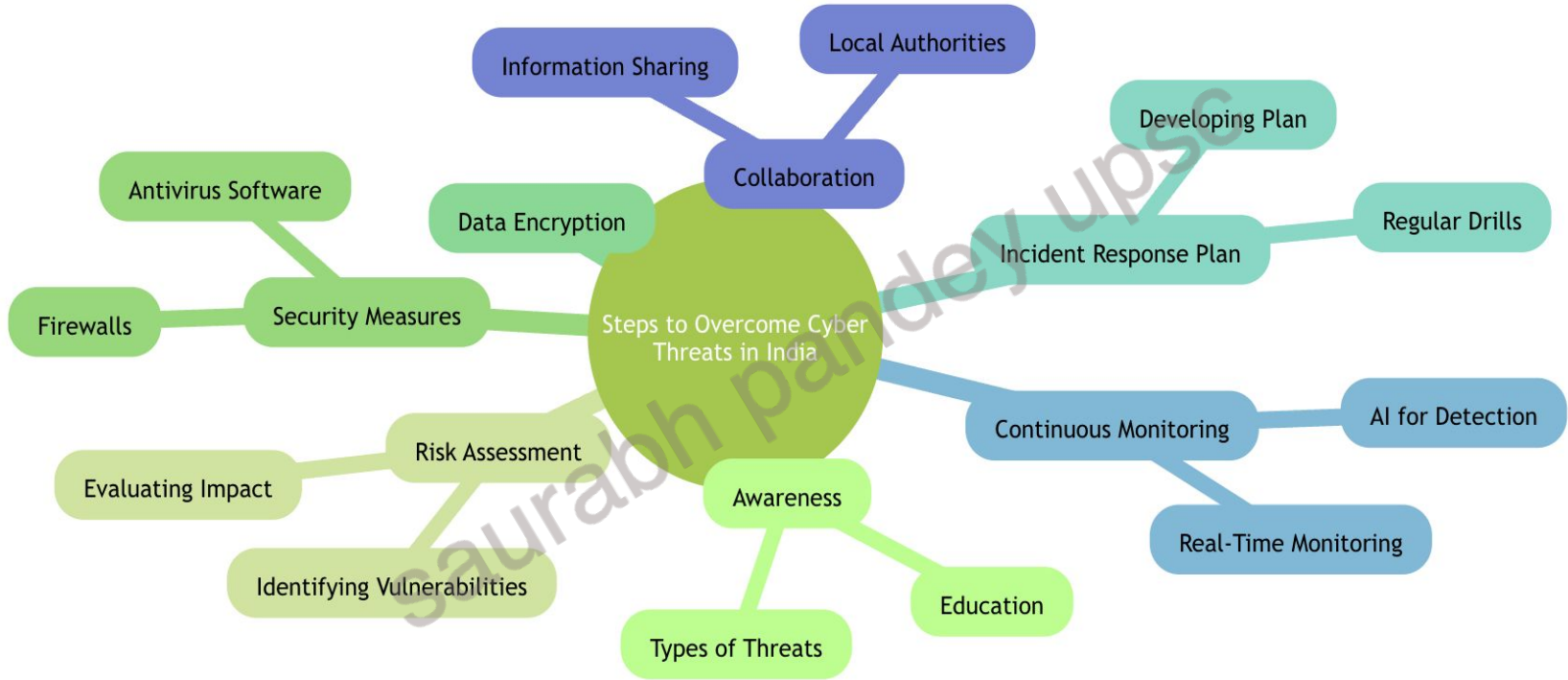
Implement systems for real-time monitoring of network traffic.
Use AI and machine learning for threat detection.

Collaboration with Authorities

Work with local and national cybersecurity agencies.

Share information about potential threats and incidents. The importance of cybersecurity continues to rise, especially in countries like India with a growing digital landscape

Figure 1.1: Mindmap



National Cyber Security Policy 2013

- **Policy Objectives:** The National Cyber Security Policy 2013 aims to establish a secure computing environment, foster trust in electronic transactions, and guide the implementation of robust cybersecurity measures across sectors.
- **Framework for Safeguarding:** The policy outlines a comprehensive framework to fortify the nation's cyber infrastructure and protect against cyber-attacks, emphasizing the importance of secure communication and electronic transactions.
- **Evolution of Cyber Threats:** The policy acknowledges the dynamic nature of cyber threats and provides a strategic approach to address emerging challenges in the

Cybersecurity Awareness and Education

- **Cyber Literacy:** Promoting cyber awareness and education initiatives is critical for empowering individuals with the knowledge and skills to protect themselves from cyber threats and contribute to a secure digital ecosystem.
- **Role of Educational Institutions:** Integrating cybersecurity education into academic curricula equips students with the necessary skills and knowledge to pursue careers in cybersecurity and contribute to national cyber resilience.
- **Youth Empowerment:** Fostering a culture of cyber awareness and resilience among the youth is essential for nurturing the next generation of cybersecurity professionals and advocates.

Topic- What is Short Selling?



Overview

Definition: Short selling is an investment strategy that involves selling borrowed shares of a stock with the intention of buying them back later at a lower price.

Purpose: Investors short sell to profit from an anticipated decline in the stock's price.

Steps of Short Selling

Borrowing Shares: Obtain shares from a broker.

Selling Borrowed Shares: Sell them on the market at the current price.

Waiting for Price Drop: Hold the position until the stock price decreases.

Buying Back Shares: Purchase the same number of shares at the lower price.

Returning Shares: Return the borrowed shares to the broker and keep the difference as profit.

Risks Involved

Unlimited Loss Potential: If the stock price rises instead of falls, losses can be unlimited since there's no cap on how high a stock price can go.

Margin Calls: Brokers may require additional funds if the stock price rises significantly.

Market Impact

Volatility: Short selling can contribute to market volatility, especially in bear markets.

Market Correction: Some argue it helps correct overvalued stocks.

Regulatory Aspects

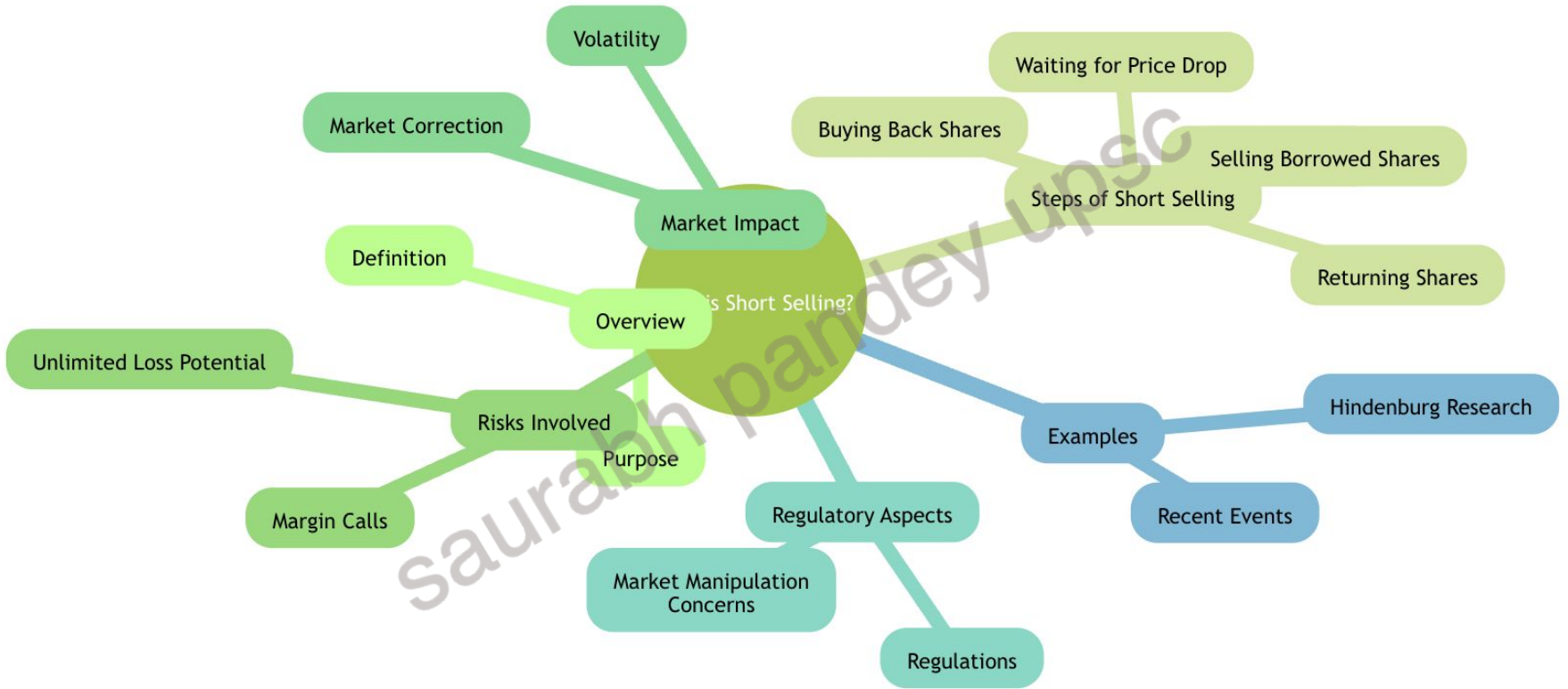
Regulations: Different countries have various regulations regarding short selling, including restrictions and reporting requirements.

Market Manipulation Concerns: Authorities monitor for illegal short selling practices.

Examples

Hindenburg Research: Known for short selling and exposing corporate frauds and making profits from market downturns.

Recent Events: News on regulatory changes related to short selling in countries like China.



Topic-Court of Arbitration for Sports



Overview

Function: Resolves disputes in sports

Establishment: Founded in 1984

Headquarters: Lausanne, Switzerland

Role: International arbitration for sports-related disputes

Key Components

Types of Disputes:

Doping cases 🏆

Contractual disputes 📄

Eligibility issues 🏅

Process:

Filing appeals

Arbitration hearings

Final decisions

Legal Precedents: Sets legal standards for future cases

Recent Cases

Jordan Chiles: Dispute over a bronze medal 🏅

Vinesh Phogat: Wrestling eligibility case 🤼

Impact on Olympics: Influence on athlete participation and outcomes 🏆

Governance

Structure:

President

Arbitrators from various countries 🌍

Legal professionals with sports expertise ⚖️

Funding:

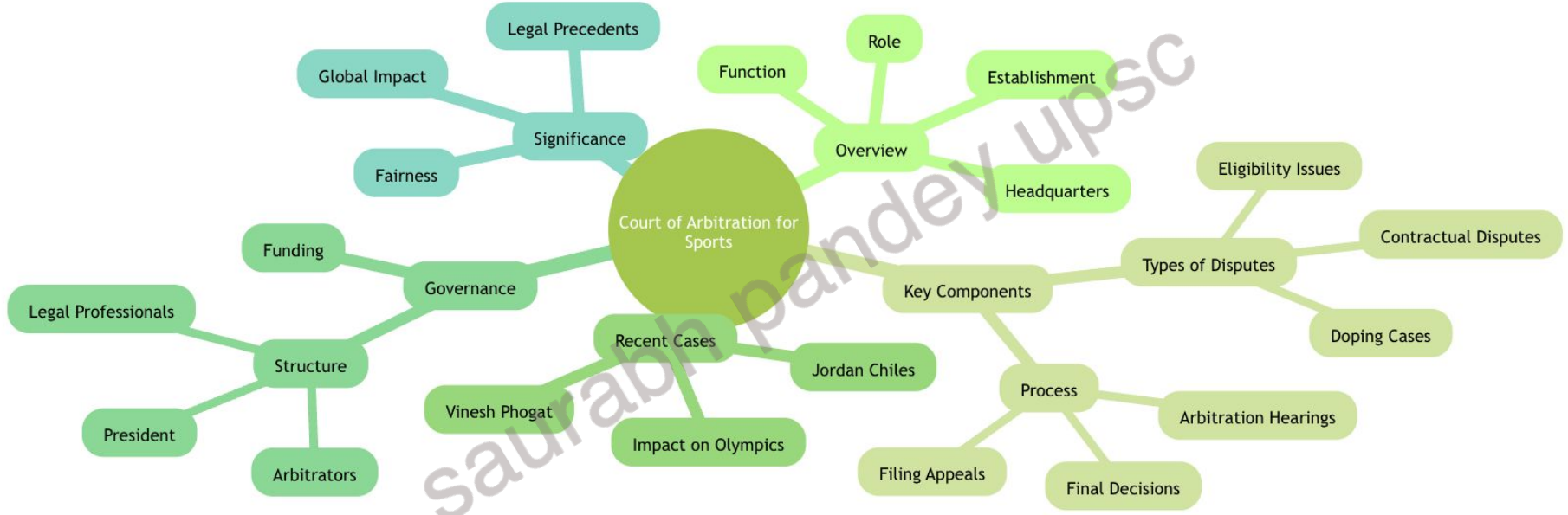
Membership fees

Service fees for arbitration

Significance

Fairness: Ensures fair play and integrity in sports

Global Impact: Decisions affect athletes worldwide 🌐



Topic-Overview of AUKUS



AUKUS: A trilateral security pact between (*Australia, the UK, and the US*). 🤝

Purpose: To enhance security cooperation, particularly in the Indo-Pacific region. 🌐

Focus Areas:

Nuclear submarine technology. ⚓

Cybersecurity enhancements. 🔒

Artificial Intelligence (AI) collaboration. 🤖

Key Components of AUKUS

Membership:

Initial countries: Australia, UK, US.

Potential expansions: Interest from Japan, South Korea, and New Zealand. 

Strategic Goals:

Counteracting China's influence in the region. 

Strengthening global alliances against shared security challenges. 

Current Developments

Cooperation with Quad:

Possible collaboration with Quad-member Japan. 

Concerns raised regarding China's response to these alliances. 

Technological Advancements:

Formation of the AUKUS Cloud Alliance for data center optimization. 

Development of advanced military technologies. 

saurabh pandey upsc

Challenges Ahead

Public Opposition:

Activism against AUKUS from peace groups. 

International Relations:

Need for careful diplomacy to avoid escalating tensions with nations like China. 

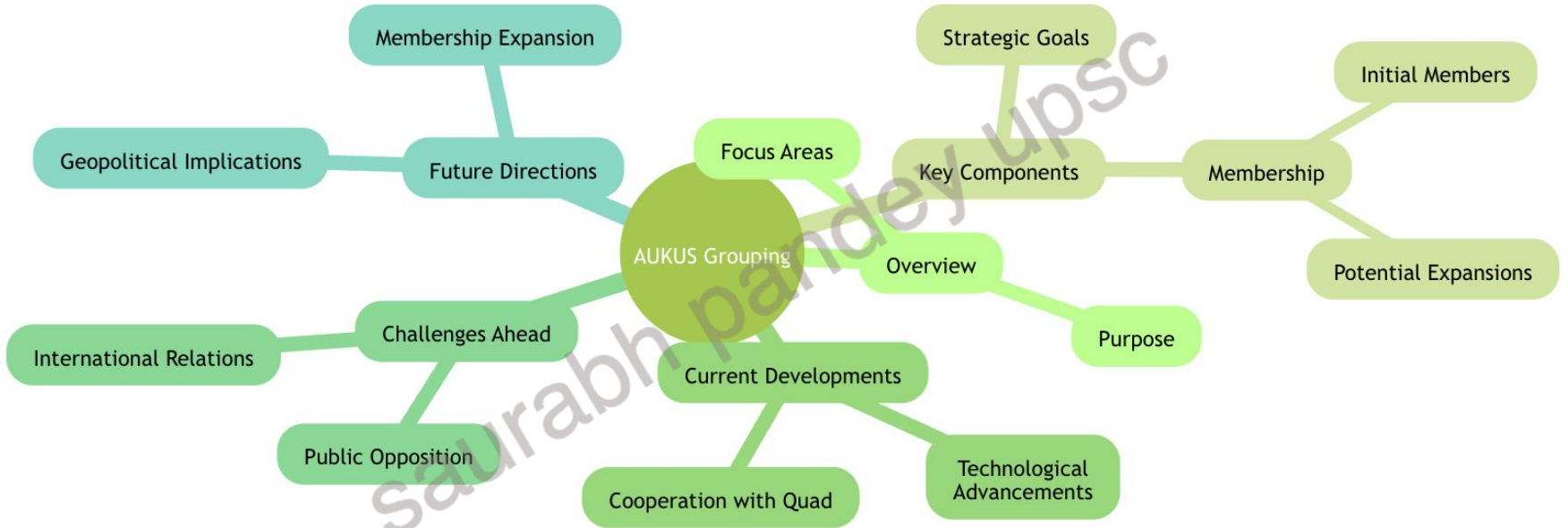
Potential Future Directions

Membership Expansion:

Possible inclusion of other allies such as India or France. 

Geopolitical Implications:

Could AUKUS evolve into a broader Asian NATO-like alliance?



1. AUKUS Grouping is a strategic partnership between Australia, the United Kingdom, and the United States, aimed at enhancing security and defense cooperation in the Indo-Pacific region.

ATTENTION!! BATCH FOR 2025/26 LAUNCHED

connect with sir -9057921649

CURRENT AFFAIRS PLUS (FOR UPSC 2025)

INCLUDES

- PIB Analysis with pdf
- Down to earth
- physics.org
- science daily
- Major newspapers
- With practice test and Mains Mock

2years
coverage



BY SAURABH
PANDEY SIR

Link in description

Msg -9057921649

Download -
saurabh pandey
cse app

NEW BATCH LAUNCHED

Connect with sir 90579 21649

**Complete Agriculture
optional**

Paper 1 and Paper 2

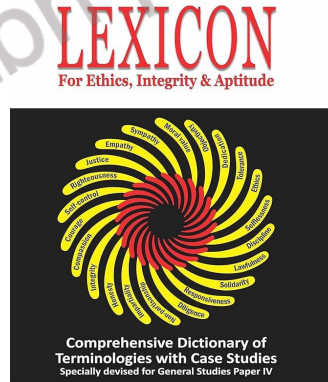
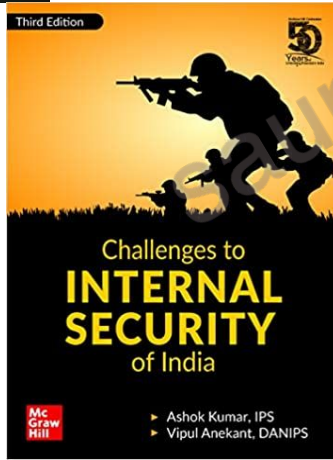
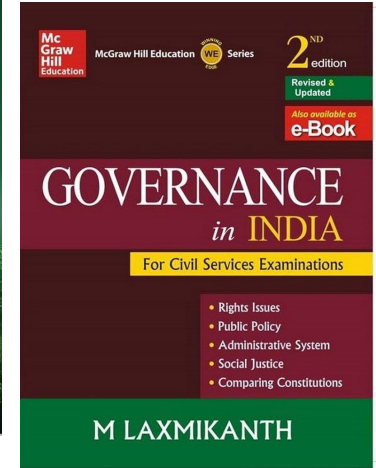
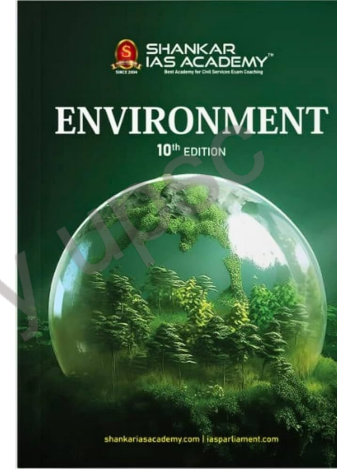
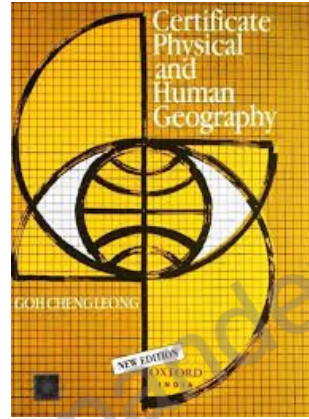
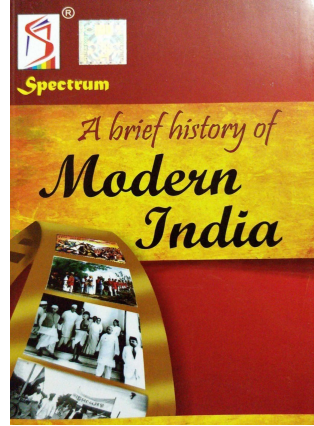
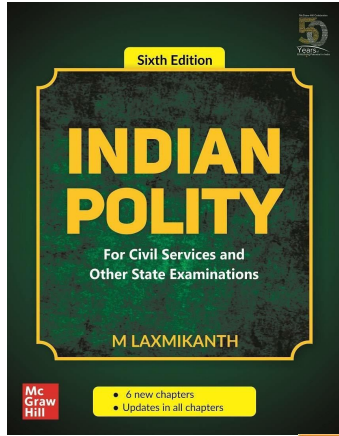
Live classes

Starting 1st July

Score 300+



ALL Advance books for upsc IN ONE COURSE



Chronicle
Nurturing Talent Since 1990

Starting 1st june

Visit -
saurabhpandeyupsc.com

Msg - 9057921649

COMBO COURSE FOR UPSC 2025

ALL Advance books for upsc IN ONE COURSE

Starting 1st july
Visit -
saurabhpandeyupsc.com
Msg - 9057921649



**Save Rs
1000/-**

**ATTENTION!! BATCH FOR 2025/26
LAUNCHED**
connect with sir -9057921649

**CURRENT AFFAIRS PLUS
(FOR UPSC 2025)**

INCLUDES

- PIB Analysis with pdf
- Down to earth
- physics.org
- science daily
- Major newspapers
- With practice test and Mains Mock

starting 1st may 2024

**BY SAURABH
PANDEY SIR**

MAINS GURUJI

Connect with sir 90579 21649

**UPSC MAINS
MENTORSHIP
PROGRAM**

starting
LIVE LY
2024



Batch-1

**BY SAURABH
PANDEY SIR**

**Target 400 + in
GS paper**

**How to approach
Essay ??**

**Only for serious
UPSC ASPIRANTS**

Scan - to get free content



The hindu session pdf

Download the hindu session pdf

Telegram link in description box

Download the hindu pdf - <https://t.me/gesreporter>

Connect with sir
9057921649



Saurabh Pandey upsc

Target Mains -2024/25 -

Q 'AI will make cyberspace more vulnerable'

Elucidate

Connect with sir
9057921649

send your answer - Saurabh pandey
upsc telegram channel