PLUTUS
IAS

CURRENT AFFAIRS

Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

Date –9 November 2024

ALIGARH MUSLIM UNIVERSITY'S MINORITY STATUS: A LANDMARK DECISION AWAITS FROM SUPREME COURT

Posted at **09 Nov 2024** in Current Affairs by Ritik singh 0 Comments
0Likes

SYLLABUS MAPPING:

GS-2 Polity- Aligarh Muslim University's Minority Status: A Landmark Decision Awaits from Supreme Court

FOR PRELIMS:

How does the minority status of AMU impact its governance and admission policies?

FOR MAINS:

Discuss the legal and constitutional arguments surrounding the minority status of Aligarh Muslim University. How does this case challenge the principles of secularism and equality in India?

WHY IN THE NEWS?

A Bench led by the Chief Justice of India (CJI) is set to deliver its verdict on whether Aligarh Muslim University (AMU) is entitled to claim minority status under Article 30 of the Indian Constitution on the CJI's final working day in office.

MINORITY INSTITUTIONS-CONSTITUTIONAL MANDATES:

Article 30 of the Indian Constitution ensures the rights of minorities, whether based on religion or language, to establish and administer educational institutions of their choice. This provision is crucial in the ongoing legal discussions surrounding institutions like Aligarh Muslim University (AMU) and their claim for minority status.

Key Provisions of Article 30:

1. Right to Establish and Administer: Religious and linguistic minorities can establish and manage educational institutions without state interference (Article 30(1)).

2. Non-Discrimination in Aid: The state cannot deny aid to minority institutions solely because they are managed by minorities (Article 30(2)).

Types of Minority Institutions:

Religious Minority Institutions: Established and managed by religious minorities, e.g., Aligarh Muslim University (AMU) (Muslim) and St. Xavier’s College (Christian).

Linguistic Minority Institutions: Run by linguistic minorities to preserve and promote their language, e.g., institutions serving Tamil, Telugu, or Marathi-speaking communities.

MINORITY INSTITUTIONS FEATURE VS OTHER INSTITUTIONS:

1. Constitutional Autonomy:

Minority Institutions: Protected under Article 30; have the right to manage their own affairs, including admissions and curriculum, with preference for their community.

Other Institutions: Governed by state and national regulations, with less autonomy in admissions, governance, and curriculum design.

2. Admissions and Community Preference:

Minority Institutions: Can prioritize admissions for students from their own religious or linguistic community.

Other Institutions: Follow merit-based admissions, with reservations for SC/ST/OBC students but no community-based preferences.

3. Cultural and Religious Identity:

Minority Institutions: Focus on preserving the religious, cultural, or linguistic identity of the minority community (e.g., Islamic studies in Muslim-run colleges).

Other Institutions: Have a secular ethos, focusing on inclusive, national standards without promoting any specific religious or cultural identity.

4. State Regulation and Financial Support:

Minority Institutions: Enjoy limited state interference but are eligible for state funding; often rely on private donations and community support.

Other Institutions: Subject to more state regulation; rely on public funding and tuition fees for financial sustainability.

5. Reservation and Social Justice Policies:

Minority Institutions: Can implement their own community-based reservations but must still comply with constitutional equality norms.

Other Institutions: Must follow government-mandated reservation policies for SC/ST/OBCs, ensuring social justice and inclusive access to education.

ISSUE HIGHLIGHTS BY SUPREME COURT:

1. Minority Status under Article 30:

The core issue is whether Aligarh Muslim University (AMU) can claim minority status as a Muslim-run institution despite being established by an Act of Parliament.

The Court is examining whether an institution created by Parliament can still be considered a minority institution under Article 30 of the Constitution, which guarantees minority communities the right to establish and manage educational institutions.

2. Definition of ‘Minority’:

The Court is considering whether minority status should be determined state-wise or nationally, as minorities are defined differently in various states. The ruling will affect how other institutions across India claim minority status based on their community and geographical context.

Impact on Other Institutions:

The decision will set a precedent for other minority-run educational institutions like Jamia Millia Islamia and St. Xavier's College, influencing their admissions, autonomy, and funding policies.

3. Role of Parliament vs. Minority Rights:

The case raises questions about whether Parliament's legislative powers (e.g., the AMU Act) override minority rights under the Constitution, especially regarding self-governance and religious autonomy of institutions.

4. Secularism vs. Religious Autonomy:

The Court must balance India's secular framework with the religious autonomy of institutions, ensuring that minority institutions can maintain their cultural and religious identity while adhering to national educational standards.

ROLE OF STATE IN MINORITY INSTITUTIONS STATUS:

1. AMU Cannot Claim Minority Status:

The Government argues that AMU, established by an Act of Parliament in 1920, is a public university and not a minority institution under Article 30. It contends that Article 30 applies to private institutions founded by minority communities, not public ones.

2. Secular Education Framework:

The Government stresses the secular character of education in India, asserting that all public institutions, including AMU, must adhere to national educational standards and cannot claim religious-based exemptions.

3. Reservations and Inclusive Policies:

AMU, as a state-funded institution, must comply with reservation policies for SCs, STs, and OBCs. The Government argues that granting AMU minority status could undermine affirmative action and create inequalities in admissions.

4. Public Accountability and Regulation:

The Government emphasizes that public universities like AMU should remain subject to government oversight, including in matters like curriculum, admissions, and faculty recruitment, ensuring uniformity and accountability across the education system.

5. Setting a Precedent for Other Institutions:

The Government fears that recognizing AMU's minority status could set a precedent for other public universities to seek similar exemptions, leading to unequal treatment in admissions and funding.

CONCLUSION:

The Supreme Court is set to decide whether Aligarh Muslim University (AMU) can claim minority status under Article 30 of the Indian Constitution. The case hinges on whether Article 30, which protects the rights of minorities to establish and manage educational institutions, applies to a public university like AMU, established by an Act of Parliament, or only to private institutions. The Government argues that AMU, as a state-funded institution, must follow national policies, including reservation and secular standards, and cannot claim religious exemptions. It warns that granting AMU minority status could lead to unequal treatment and undermine inclusive education policies.

PRELIMS QUESTION:

Q. Which of the following is a provision of Article 30 of the Indian Constitution?

A. The right to free education for all children

B. Protection of minority-run institutions from state interference

C. Guarantee of reservation in educational institutions
D. Right to form trade unions for minority communities
Answer: B

MAINS QUESTION:

Q. Critically assess whether minority institutions like AMU should be allowed to prioritize admissions for students from their own community while still adhering to national educational standards and constitutional principles.
(250 words, 15 marks)

Ritik singh

“SIDE-CHANNEL ATTACKS: EMERGING THREATS TO INDIA’S CYBERSECURITY AND INTERNAL SECURITY”

This article covers “Daily Current Affairs” and topic details A side-channel attack”

SYLLABUS MAPPING:

GS-3: Internal Security: Challenges to internal security through communication networks; the role of media and social networking sites in internal security challenges; basics of cyber security.

FOR PRELIMS:

What are the side Channel attacks, their types, and terminologies related to the side-channel attacks?

FOR MAINS:

What are the threats from the Side- side-channel attack to the internal security, challenges in the tackling of the side-channel attack, and government measures to tackle the side-channel attack?

WHY IN THE NEWS?

New Agreement for Cybersecurity R&D: The Centre for Development of Telematics (C-DOT) has signed an agreement with C R Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS) to develop an advanced cybersecurity solution, the Side Channel Leakage Capture Infrastructure and Analysis (SCLCIA). This collaboration aims to strengthen India’s defense against side-channel attacks.

WHAT IS A SIDE-CHANNEL ATTACK?

A side-channel attack is a cyber-attack where attackers exploit unintended information leaks from a system—such as power usage, timing, or electromagnetic emissions—rather than directly targeting the software or hardware. By observing physical indicators of a system's operations, attackers can extract sensitive data, making these attacks particularly stealthy and dangerous, especially in high-security environments.

Mechanism: These attacks primarily target cryptographic systems, as they handle sensitive data that can be indirectly observed. By analyzing "side channels" like energy emissions, sound, or light, attackers can uncover confidential data, such as encryption keys or passwords, without altering or infiltrating the system's code, often evading traditional detection methods.

EXAMPLES OF SIDE-CHANNEL ATTACKS

Power Analysis Attack: Observes variations in power consumption by a device to deduce operations such as encryption key generation.

Timing Attack: Measures the time taken to execute specific computations to determine sensitive information, such as cryptographic keys.

Electromagnetic (EM) Attack: Uses electromagnetic emissions from a device to reconstruct operations and potentially infer data being processed.

Acoustic Cryptanalysis: Analyzes sounds made by computer components (like CPU or hard drives) to infer data being processed or commands being executed.

Cache Timing Attack: Exploits cache usage patterns in multi-core processors, where shared cache access may leak data between cores.

Optical Side-Channel Attack: Observes light emitted from devices, such as LEDs on network devices or routers, which can reveal information about network traffic or device status.

THREAT TO INDIA'S INTERNAL SECURITY FROM SIDE-CHANNEL ATTACKS

Threat to Critical Infrastructure:

Side-channel attacks can reveal vulnerabilities in critical infrastructure, such as power grids, telecom networks, and transportation systems.

If attackers gain sensitive operational data from these systems, they could disrupt services, impacting internal security, public safety, and economic stability.

National Defense Risks:

Defense systems heavily rely on cryptographic protocols for secure communications and data processing.

Side-channel attacks on defense technologies, including encryption devices, can lead to data leaks, facilitating espionage and potentially compromising national security.

Financial System Vulnerabilities:

The financial sector’s use of encryption mechanisms for transactions makes it vulnerable to side-channel attacks.

Leaked cryptographic keys can enable unauthorized access to confidential financial data, heightening the risk of fraud, financial instability, and reduced public trust in digital banking.

Intelligence and Government Communications:

Side-channel vulnerabilities in government and intelligence agency equipment could lead to sensitive information leaks.

Breaches in encryption protocols used in government communications may expose strategies, intelligence, and classified data to adversaries, making it critical to secure these channels.

IoT and Smart City Risks:

Increased IoT adoption in critical sectors, such as smart cities, healthcare, and traffic systems, introduces more points of vulnerability.

Side-channel attacks on IoT devices in these areas can lead to large-scale disruptions. For instance, compromised data from traffic or healthcare IoT devices could threaten public safety and security.

Supply Chain and Infrastructure Weaknesses:

India’s digitalization drive often relies on foreign technology imports, which may lack adequate protection against side-channel attacks.

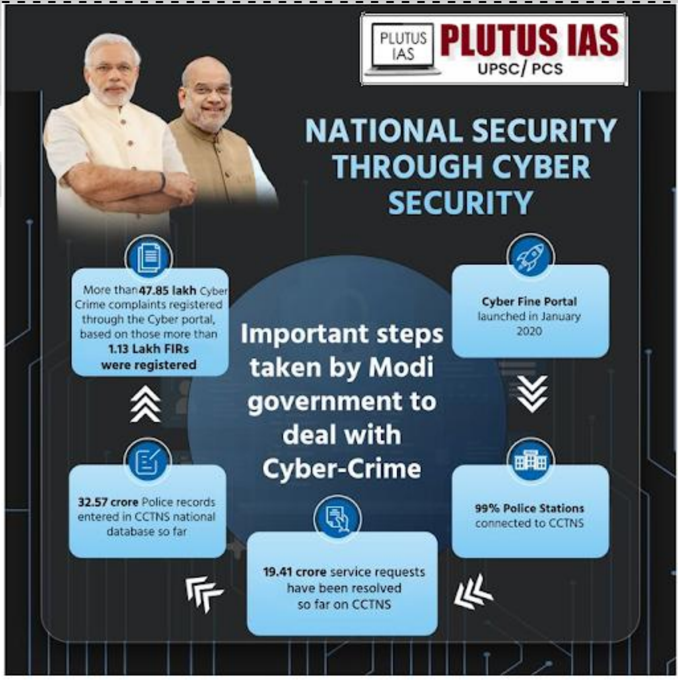
Foreign technology components could expose internal systems without robust security measures, making indigenous solutions critical to safeguard national infrastructure.

Economic Impact and Data Sovereignty:

Frequent side-channel data breaches can lead to intellectual property theft and hinder economic growth.

Weak protections against these attacks threaten India’s digital economy and data sovereignty, as uncontrolled access to critical national data by external entities could jeopardize internal security and control over key information assets.

GOVERNMENT OF INDIA’S INITIATIVES FOR CYBERSECURITY



PLUTUS IAS
UPSC/ PCS

NATIONAL SECURITY THROUGH CYBER SECURITY

Important steps taken by Modi government to deal with Cyber-Crime

More than 47.85 lakh Cyber Crime complaints registered through the Cyber portal, based on those more than 1.13 Lakh FIRs were registered

Cyber Fine Portal launched in January 2020

99% Police Stations connected to CCTNS

19.41 crore service requests have been resolved so far on CCTNS

32.57 crore Police records entered in CCTNS national database so far

National Cyber Security Policy: Outlines comprehensive strategies to protect cyberspace infrastructure, prevent cyber attacks, and enable effective responses.
Indian Cyber Crime Coordination Centre (I4C): Provides a framework for law enforcement agencies to collaborate and combat cyber crimes across India.
Computer Emergency Response Team (CERT-In): Acts as the national cyber incident response agency, operating a 24/7 help desk, issuing threat alerts, coordinating responses, and collaborating internationally for threat information sharing.
C**yber Swachhta Kendra:** Operated by CERT-In, this initiative focuses on securing India’s digital environment by identifying and removing cybersecurity threats.
Cyber Surakshit Bharat Initiative: Promotes cybersecurity awareness, particularly among IT staff and Chief Information Security Officers (CISOs), to enhance cyber hygiene in government and critical sectors.
Research and Development Programs: Supports R&D in cybersecurity fields like cryptography, network security, cyber forensics, and capacity building, aiming to advance secure technology and forensic tools domestically.
Capacity Development and Training: Establishes specialized training centers for cybercrime investigation, forensic labs, and virtual training environments across states to strengthen law enforcement capabilities in handling cyber crimes.
International and National Collaboration: Partners with industry bodies (CII, NASSCOM) and international cybersecurity agencies. Cybersecurity cooperation agreements and cyber drills have been conducted with countries like the US, Japan, and South Korea to enhance response and preparedness.

CHALLENGES IN TACKLING SIDE-CHANNEL ATTACKS

Detection Difficulty: These attacks are challenging to detect, as they do not leave traditional cyber footprints and often require sophisticated tools for identification.
High Cost of Countermeasures: Implementing physical protections, such as shielding or noise generators, can be expensive and technically demanding.
Impact on Device Performance: Many protective measures can reduce device performance, posing a challenge in high-performance environments.
Limited Awareness and Training: Many organizations may not fully understand the threat of side-channel attacks, leading to inadequate protection.
Evolving Attack Methods: Attackers continuously develop new techniques, requiring constant adaptation in defenses and countermeasures.
Complex Hardware Requirements: Defending against side-channel attacks often involves hardware-specific solutions, which may not be feasible across all devices or cost-effective.

MEASURES NEEDED TO STRENGTHEN CYBERSECURITY FURTHER

Advanced Wireless Security: Implementing tools to detect rogue access points, disabling SSID broadcasting, using 802.1x for authentication, and restricting personal device access through administrator authorization can enhance wireless security.
Enhanced Incident Response: Building capacity for early warning and quick response to incidents through expanded CERT-In services and increased collaboration with international CERTs.
Cybersecurity Awareness for Citizens: Broader public awareness campaigns, like CERT-In’s “secureyourpc. in” initiative, can educate citizens on personal cybersecurity practices.
Cyber Forensic Tools Development: Further investment in developing advanced cyber forensic tools is needed to improve investigation capabilities, especially for tackling sophisticated cybercrimes.
Strengthening IoT Security: As IoT adoption rises, measures to secure IoT devices in critical sectors (e.g., healthcare, and infrastructure) will be essential to prevent potential side-channel and

other cyber attacks.

Cybersecurity Standards for Import Technology: Given the reliance on foreign technology, establishing standards for imported hardware and software can reduce vulnerabilities, especially in critical infrastructure.

Continuous Capacity Building: More comprehensive training for law enforcement, judiciary, and IT staff across regions will ensure a well-prepared workforce to handle evolving cyber threats.

CONCLUSION:

As India’s digital footprint grows, it holds immense potential for driving economic growth and enhancing social well-being. However, this expansion also brings complex challenges to national security and sovereignty, as digital vulnerabilities can be exploited by cyber threats. A secure cyberspace demands a holistic approach involving not only government initiatives and international collaborations but also heightened public awareness and proactive cybersecurity measures.

PRELIMS QUESTIONS:

Q. The term “Side Channel Leakage Capture Infrastructure” recently seen in the news is related to

A. Money market

B. Climate change

C. Cyber security

D. Investment model

ANSWER: C

MAINS QUESTION:

Q. What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. (2022)

Munde Dhananjay Navnath