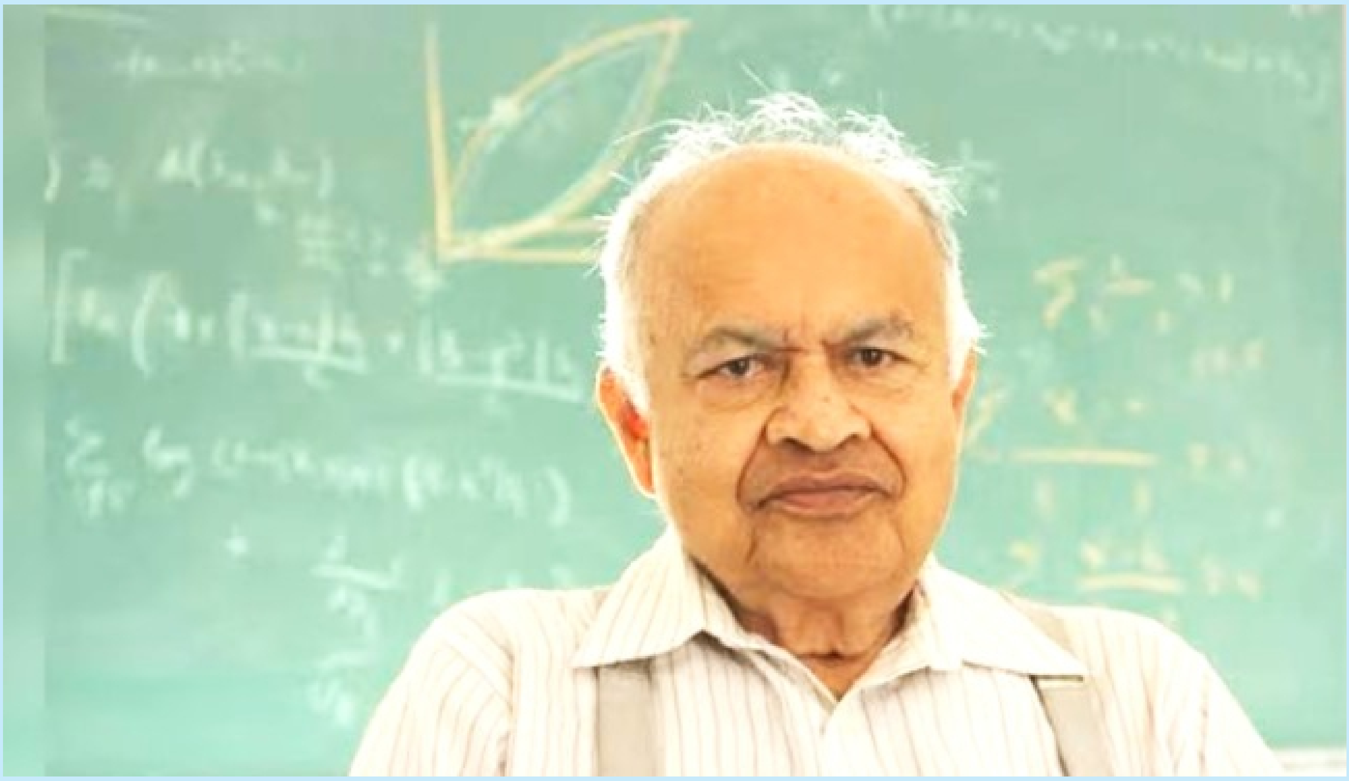
ISSN 2348-084X

COLLEGE POST

the higher education journal

VOL. 25, No. 1 April - June, 2025



Jayant Vishnu Narlikar (19 July 1938 - 20 May 2025)
An astrophysicist who performed research on alternative cosmology.
Big Bang or Steady State Cosmos Theory.

About cover see page 12

seed...

seed...

CHEST

Online Courses on Ethics, Values & Life Skills

Course -1

Introduction to Ethics – 2 Credits

Module -1: DEFINITION AND MAJOR THEORIES
Unit 1: The definition
Unit 2:Major Theories of Ethics and Brief description of theories
Unit 3: Ethical Framework and Approaches
Unit 4:Key Distinction between Ethics, Morals, and Values

Module - 2: SCOPE OF ETHICS AND ETHICS IN DIFFERENT DISCIPLINESAND PROFESSIONAL ETHICS
Unit 1: ScopeUnit 2: Scope of Ethics in Different Disciplines
Unit 3: Professional EthicsUnit 4: Challenges of Application

Module – 3: ETHICSIN MODERN TIMES
Unit 1: Ethics in Modern TimesUnit 2: Future Challenges

Course - 2

Introduction To Values – 2 Credits

Module - 1: VALUE ORIENTATION
Unit 1: The Definition Unit 2: Norms and ValuesUnit 3: Perennial Values

Module - 2: VALUES IN MODERN SOCIETY
Unit 1:Modernization and ModernityUnit 2:The Rationalistic or Liberal Model
Unit 3:The Revivalist or the Orthodox ModelUnit 4:The Radical or the Revolutionary Model

Module - 3: TYPES OF CONTEMPORARY SOCIETIES
Unit 1:Traditional SocietiesUnit2:Transitional SocietiesUnit 3:Modern Societies
Unit 4:Post-Modern SocietiesUnit 5: Indian Unity and Diversity Value
Unit 6: UGC Guidelines Value Pravesh 2.0 Unit 7:Changing Societies under the Tech. Revo.

Course- 3

LIFE SKILLS- 2Credits:Self Development, Management, Rights &Duties, Personal Safety and Security-

Module - 1: SELF DEVELOPMENT
Unit 1: Emotional IntelligenceUnit 2:Self-EsteemUnit 3: Yoga Unit 4: Skills for Quality LifeUnit 5: The True North Principles Unit 6: The Potentiality Of The Four Human Endowments

Module - 2:WORK, HABITS, ENVIRONMENT PROTECTION &FUNDAMENTAL RIGHTS & DUTIES
Unit 1:Work,Unit 2:Sense of Duty,Unit 3:Habits of Thrift, Unit 4:Environment, Unit 4.1:Environment Protection Policy,Unit 5:Fundamental Rights and Dutiesof The Citizens

Module - 3: NATIONAL SECURITY, PERSONAL SAFETY AND SECURITY
Unit 1: National Security Unit 2: Personal Security Unit 3: Body Heat: As Temperatures Rise, Please Add SaltUnit 3.1: Prevent Electrical Fires at HomeUnit 3.2: Security Travel TipsUnit 3.2.1: Travel Tips Unit 4: Sexual Harassment: What Every Working Woman needs to knowUnit 5: How Burglars Choose Their VictimsUnit 6: Ten Ways to Protect Your HomeUnit 7: Credit Card & Cyber Security Precautions Unit 7.1: Negative Impact of Excess use of Mobile Phone Unit 8: Prudent Precautions against Terrorism.

IMPORTANT NOTE -
Courses will be offered in collaboration with the institutions. Also, students can directly enroll for the Courses. Certificate will be provided jointly by SEED-CHEST and Collaborating Institute.

CONTACT DETAILS:-
E-mail - seedicf@gmail.com
Phone - 9868820215
Landline- 011-43008598

Society for Education and Economic Development, New Delhi

EDITORIAL

THE 5.0 INDUSTRIAL REVOLUTION AND CHALLENGES BEFORE HIGHER EDUCATION: ARE WE READY?

As the world continues to adapt to the transformations of Industry 4.0, a more profound shift is already upon us - the 5.0 Industrial Revolution. Driven by powerful General Purpose Technologies (GPTs) like generative AI, this new phase is rapidly redefining how we work, think, and live. The arrival of tools like ChatGPT, developed by OpenAI, has brought the once-theoretical question "Can machines think?" into the realm of lived experience. The more pressing question now is: Can humans think beyond what machines can?

The release of ChatGPT marked a milestone in human-machine interaction. Within months, new AI models emerged with capabilities far beyond basic text processing, handling multimodal and real-time data. Competitors such as Grok AI and DeepSeek added to this technological wave, pushing the capabilities of AI while making them more affordable and accessible. Nations like India are now racing to acquire the necessary infrastructure - including Graphics Processing Units (GPUs) - to compete in this rapidly evolving ecosystem.

This technological leap poses serious challenges to higher education systems, which often struggle to evolve at the pace of innovation. The conventional university model, built on the dissemination and interpretation of archival knowledge, is quickly becoming outdated.

AI now performs tasks that were once central to the academic experience - searching, summarizing, and explaining complex information - in a matter of seconds. Faculty are understandably skeptical of assignments generated with AI assistance, as they circumvent the cognitive labor that is essential to intellectual development. Yet, these same tools are already being used by researchers to process vast datasets and solve complex problems, such as protein folding in biomedical science.

The emerging consensus is that machines should handle data-heavy and routine cognitive tasks, while human beings focus on higher-order thinking - including creativity, critical analysis, ethics, and communication.

To remain relevant in the age of Industry 5.0, higher education must undergo transformative change along three key dimensions:

1. Transition Beyond Archival Learning

Curricula must shift from static knowledge transfer to active, experiential, and inquiry-based learning. Students must be equipped to analyze real-time data, think critically, and adapt to rapidly changing contexts. This demands pedagogical innovation and deep curricular reform.

2. Build Digital Ethics and Combat Misinformation

AI systems are capable of spreading misinformation as quickly as they share the truth. Educators must prepare students to recognize digital bias, question AI-generated content, and construct ethical frameworks for responsible technology use. Ethics and communication skills must become foundational elements of every academic program - not just electives for a select few.

3. Train for Human-Machine Collaboration

The greatest opportunity of this revolution lies in collaborative problem-solving. Higher education must prepare students to work alongside intelligent machines to address global challenges - whether social, environmental, or emotional. This collaboration requires new skill sets, new attitudes, and a new pedagogy.

Efforts to regulate or contain this revolution will likely prove insufficient. The digital revolution, unlike earlier industrial ones, is not grounded in physical systems - it is powered by algorithms that are learning and evolving in real-time. The regulatory frameworks of the past may not apply.

....contd on page 28

CONTENTS

Editor

G.D. Sharma

Co-editor

Baldev Mahajan

REVAMPING THE INDIAN COLLEGES FORUM (ICF)

Following the 25th Silver Jubilee Conference, activities of the Indian Colleges Forum (ICF) witnessed a temporary slowdown-primarily due to the COVID-19 pandemic and various organizational changes. However, during this period, several notable initiatives were undertaken, including:

- A Leadership Development Programme
- Workshops on the use of Artificial Intelligence, Blockchain Technology, and Quantum Computing
- Convocation ceremonies for participants of the IDEL-HE programme
- Regular publication of College Post, ICF's journal on higher education
- "• Meetings with State Secretaries of ICF

Despite these efforts, a need was felt to revamp and restructure the Forum to align with evolving academic and administrative needs.

MEMBER COLLEGE ENGAGEMENT AND DATA UPDATE

A formal communication was sent to all member colleges, detailing their membership history and outlining the proposed course of action. Colleges were requested to update their institutional profiles via a Google Form created for this purpose. While several institutions have submitted their data, many are yet to do so. The updated profiles of responding colleges have been uploaded to the official website: http://indiancollegesforum.com.

FORMATION OF STATE-LEVEL EXECUTIVE COMMITTEES

In line with ICF's constitution, the next step involved constituting State-Level Executive Committees (ECs). Member colleges were invited to submit three nominations/preferences for their respective State ECs. Where preferences were not received, the senior-most registered member colleges were nominated.

Following this process, State ECs have been successfully constituted and their first meetings held in the following states:

- Assam (Upper and Lower)
- Chhattisgarh
- Delhi
- Gujarat
- Jammu & Kashmir
- Kerala
- Karnataka
- Meghalaya
- Maharashtra
- Tamil Nadu
- Uttar Pradesh
- West Bengal

Meetings for other states are currently in progress.

The list of State ECs and minutes of their inaugural meetings have been uploaded on the ICF website.

TOWARDS A NATIONAL-LEVEL EXECUTIVE COMMITTEE

A meeting of the Secretaries of all State-Level ECs is being planned to formally constitute the National Executive Committee of ICF.

During the first round of State EC meetings, several key issues were raised, particularly:

- Implementation of NEP 2020
- Orientation and training of institutional heads
- Execution of the Four-Year Undergraduate Programme (FYUGP)
- Quality assessment and accreditation processes
- Concerns regarding infrastructure, faculty recruitment, and curricular design for the fourth year

These issues will be addressed in forthcoming meetings with EC Secretaries and through focused interactions with state-level office bearers and members.

WEBINAR ON FOUR-YEAR UNDERGRADUATE PROGRAMME: RETROSPECT AND PROSPECTS

On 27th May 2025, Grace Valley College, in partnership with other institutions and under the aegis of the Kerala State EC of ICF, organized a webinar on the theme: Four-Year Undergraduate Programme - Retrospect and Prospects.

The webinar was inaugurated by Dr. G.D. Sharma, President of SEED-ICF, who highlighted both the importance and challenges of implementing the fourth year of undergraduate education. He stressed the need to:

- Conduct surveys of students opting for the fourth year, considering the option to exit after three years
- Upgrade infrastructure and faculty capacities in line with increased student numbers
- Implement outcome-based evaluation systems
- Offer programmes in soft skills and ability enhancement

To support institutions, SEED-CHEST has introduced:

- Three 2-credit programmes on Ethics, Values, and Life Skills
- Two 4-credit programmes on Communication Skills and Critical Thinking

MES Keveeyam College, Valanchery has successfully implemented the Ethics and Values programme, with over 100 students certified last year and another 100 currently enrolled. These courses are hosted on the LMS Canvas platform and are conducted online.

Dr. Sharma urged the Secretary of the Kerala State EC to share the proceedings of the webinar for publication in College Post, so that insights and best practices can benefit colleges nationwide.

THE RISE OF AI-GENERATED MALWARE: UNDERSTANDING THREATS, REAL EXAMPLES, AND HOW WE CAN DEFEND OURSELVES

PROFESSOR RAMESH C. SHARMA *

With the advancement of technology, in particular General Purpose Technology - AI, which has applications in various fields of Industry, academia, human health, and so on, there is a corresponding challenge of cyber-attacks by use of various malware. The paper deals with issues of Cyber Security in a very elaborate manner by citing several examples of possible malware challenges and cautions that are required to be taken and Institutionalized.

ABSTRACT

Artificial Intelligence (AI) is fundamentally transforming the cybersecurity landscape, equipping both defenders and attackers with unprecedented capabilities. A growing concern is the rise of AI-generated malware-malicious software designed or enhanced by machine learning models that can autonomously adapt, evade traditional defenses, and execute highly personalized attacks. Unlike conventional threats, AI-powered malware demonstrates polymorphic behavior, mimics legitimate applications, and can exploit vulnerabilities within AI systems themselves. Recent cases involving tools such as FraudGPT, WormGPT, and BlackMamba, along with operations by state-linked actors like Forest Blizzard and Kimsuky, highlight the severity and sophistication of this threat. In response, cybersecurity systems are increasingly relying on AI-driven solutions including behavioral analytics, adversarial machine learning, and autonomous threat detection. Sector-specific vulnerabilities in healthcare, education, and finance further underscore the need for multi-layered defensive strategies. Measures such as biometric authentication, federated learning, deception technologies, and explainable AI are becoming essential in safeguarding digital infrastructure. As the dual-use nature of AI accelerates the cyber arms race, organizations must implement proactive, adaptive, and ethically guided frameworks to manage the evolving threat landscape.

> *Measures such as biometric authentication, federated learning, deception technologies, and explainable AI are becoming essential in safeguarding digital infrastructure. As the dual-use nature of AI accelerates the cyber arms race, organizations must implement proactive, adaptive, and ethically guided frameworks to manage the evolving threat landscape.*

KEYWORDS

AI malware, cybersecurity, polymorphic malware, adversarial AI, threat detection, FraudGPT, WormGPT, behavioral analytics, autonomous threat response, sector-specific risks

UNDERSTANDING THE BASICS - WHAT IS AI AND WHAT IS CYBERSECURITY?

Before diving into the evolving threats and defenses in today's digital world, it's important to clearly understand two key concepts: Artificial Intelligence (AI) and Cybersecurity. These terms are often used in expert circles, but here they are broken down in simple, human language for clarity and context.

What is Artificial Intelligence (AI)?

Artificial Intelligence, or AI, refers to the ability of machines-usually computers or software systems-to perform tasks that typically require human intelligence. These tasks can include:

- Recognizing patterns (like spotting a face or reading handwriting)
- Making decisions (like suggesting a movie or approving a bank transaction)
- Learning from experience (like improving results based on user feedback)
- Understanding language (as seen in chatbots or translation apps)

AI systems often rely on machine learning (ML)-a subset of AI where computers "learn" from large amounts of data instead of being explicitly programmed for each task. When these systems use neural networks to process complex data like images or speech, it's called deep learning.

Examples of AI in everyday life:

- ChatGPT answering questions in real time
- Netflix recommending shows
- Google Maps predicting traffic
- Facial recognition on phones

In cybersecurity, AI is used to:

- Detect unusual patterns in network traffic
- Automate the response to threats
- Analyze millions of data points in seconds

But as powerful as AI is, it can be used just as effectively by attackers-creating an arms race between good and bad actors.

What is Cybersecurity?

Cybersecurity refers to the practice of protecting computer systems, networks, software, and data from unauthorized access, attacks, or damage. In a world where everything from healthcare to education runs on digital infrastructure,

* Dr B R Ambedkar University Delhi, New Delhi

cybersecurity has become a foundational pillar of modern life.

The main goals of cybersecurity are to:

- Prevent unauthorized access to data or systems
- Detect threats like viruses, phishing, or data breaches
- Respond quickly to attacks to minimize damage
- Recover from incidents and prevent them from happening again

Traditional cybersecurity methods include:

- Firewalls (which block unauthorized access)
- Antivirus software (which detects known malicious files)
- Password protection and access control

But traditional tools are now being stretched thin. Cybercriminals are evolving, using smart tools, automation, and AI to launch attacks that adapt and learn-faster than most legacy systems can respond. That's where AI-enhanced cybersecurity comes in.

Why This Matters Now?

With AI being used on both sides of the digital battlefield-by defenders and attackers-the definitions of "smart systems" and "secure systems" are beginning to overlap. AI doesn't just power our apps and devices; it's shaping the future of how we protect them.

Understanding these concepts isn't just for tech experts. Faculty, educators, policymakers, and institutional leaders all need a basic grasp of what AI and cybersecurity mean today-because the risks (and responsibilities) now touch every part of society.

INTRODUCTION - WHEN MACHINES LEARN TO ATTACK

In the digital age, almost everything we do-whether banking, learning, or even seeing a doctor-depends on technology. As these systems become smarter and faster thanks to artificial intelligence (AI), so do the threats that target them. AI is no longer just a tool for innovation. It's now being used by both security experts and cybercriminals alike. And that has changed the rules of the game.

Cybersecurity, which once relied on basic antivirus software and firewalls, is now facing a new enemy: AI-generated malware. This is not your typical computer virus. It learns, evolves, and adapts on its own-making it much harder to stop. These threats are more than just a technical challenge; they represent a turning point in how we think about digital safety.

This article unpacks what AI-generated malware is, why it's so dangerous, and how real-world tools like FraudGPT, WormGPT, and BlackMamba are reshaping cyberattacks. We'll look at how malware can now mimic human behavior, rewrite its own code to dodge detection (this is called polymorphic malware), and even fool smart AI systems themselves.

But it's not all doom and gloom. The same AI that powers malware is also helping defenders fight back with behavioral analytics, adversarial machine learning, and autonomous threat response systems. As we explore these developments, we'll also look at what different sectors-like healthcare, finance, and education-can do to stay one step ahead.

If we want to protect our data, our systems, and ultimately our people, we need to understand how AI is transforming cybersecurity from both sides. This isn't just a technical issue-it's a human one.

AI as Defender: Enhancing Cyber Resilience

While artificial intelligence has introduced new cyber risks, it has also become one of the most powerful allies in defending against them. Modern cybersecurity no longer depends solely on firewalls and signature-based antivirus tools. Today, AI strengthens defenses by detecting threats earlier, responding faster, and adapting to new patterns that traditional systems often miss.

1. Smarter Threat Detection through Behavioral Analytics

One of AI's most valuable contributions is its ability to learn what "normal" looks like in a digital environment-and flag anything that deviates from it. This is known as behavioral analytics. Tools based on User and Entity Behavior Analytics (UEBA) monitor how users typically interact with systems. If an employee who normally logs in at 9 AM suddenly accesses sensitive files at 3 AM from an unfamiliar location, AI systems can raise alerts in real time.

Unlike rule-based systems that rely on pre-defined attack signatures, behavioral AI adapts continuously. It spots subtle patterns that humans might miss, making it highly effective against unknown or evolving threats like zero-day exploits.

2. Predictive Capabilities and Proactive Defense

AI doesn't just react-it predicts. By analyzing massive amounts of historical breach data, machine learning models can identify early warning signs of future attacks. For instance, certain combinations of login failures, system errors, and network anomalies may signal an incoming breach. AI uses these correlations to proactively tighten security before damage occurs.

3. Automated Incident Response and Self-Healing Networks

Responding to threats quickly is critical. In traditional security systems, it could take hours or even days to analyze and contain an attack. AI compresses that timeline dramatically. Tools like IBM Watson for Cybersecurity can analyze millions of data points in seconds to identify root causes and suggest responses. Even more advanced are self-healing networks, such as those powered by DarktraceAntigena. These systems don't wait for human intervention. They can isolate compromised devices, slow suspicious traffic, or shut down attack paths on their own-buying time for IT teams to investigate without disrupting overall services.

4. AI-Driven Phishing and Fraud Prevention

Phishing emails remain one of the most common entry points for malware. Traditional spam filters can be fooled by grammatically correct, well-crafted messages-especially when they're generated by AI tools. Fortunately, AI can fight back with equal force.

Using Natural Language Processing (NLP), modern email security systems scan incoming messages for context, urgency triggers, and suspicious links-even if there are no obvious typos or red flags. NLP models can detect subtle linguistic patterns associated with deception, outperforming conventional filters with over 95% accuracy. On the user end, biometric authentication technologies-such as facial recognition or voiceprint systems-are also powered by AI. These tools reduce reliance on passwords and protect against credential theft and account hijacking.

5. Building Adaptive, Multi-Layered Security

AI-powered cybersecurity is not about replacing human professionals-it's about enhancing their ability to make faster, smarter decisions. A well-structured security system combines AI tools with human oversight, continuous learning, and ethical controls.

Technologies like Explainable AI (XAI) are now helping analysts understand why an AI made a particular decision-an essential factor when making policy or responding to legal scrutiny.

The bottom line is this: the smarter the threats become, the smarter the defenses need to be. And thanks to AI, cybersecurity is no longer a game of catch-up-it's becoming a game of anticipation.

AI AS ATTACKER: THE DARK SIDE OF INTELLIGENCE

While artificial intelligence is helping organizations build stronger defenses, it is also arming cybercriminals with tools that were once unthinkable. With little technical expertise, even novice attackers can now use AI to generate convincing phishing scams, bypass security systems, and automate large-scale intrusions. The dark web is already home to AI tools purpose-built for cybercrime, marking a dangerous shift in how digital threats are created and deployed.

1. AI-Generated Malware: Smarter, Stealthier, and Shape-Shifting

Traditional malware typically follows a set script. Once discovered, it can be identified and blocked by security software using a "signature"-a unique piece of code. But AI-generated malware doesn't play by these rules. It adapts.

One of the most striking examples is BlackMamba, an AI-powered keylogger that rewrites its own code in real time using natural language models like ChatGPT. This kind of polymorphic malware changes its structure every time it infects a new system, making traditional detection methods almost useless.

Another case is Morris II, a worm that spreads by manipulating AI systems themselves. It exploits vulnerabilities in large language models by sending specially crafted prompts, causing the AI to execute harmful commands-without any need for downloads or suspicious attachments.

These intelligent threats learn from their environment. They analyze the defenses in place and evolve their behavior to avoid them. This is malware with a mind of its own.

2. Hyper-Targeted Social Engineering Attacks

Social engineering has long been a hacker's favorite weapon-convincing people to click, download, or hand over sensitive information. With AI, this tactic has become far more dangerous.

Tools like FraudGPT and WormGPT, sold on cybercrime forums, use stolen data from social media and professional platforms to create spear-phishing emails tailored to individual victims. These messages aren't riddled with typos-they're clean, context-aware, and eerily personal. They may reference a real colleague, an upcoming meeting, or even mimic the writing style of someone the victim trusts.

Even more disturbing is the rise of deepfake phishing. AI can now clone a voice with just a short audio sample or generate a realistic fake video of a person saying something they never said. In one real case, scammers used an AI-generated voice to impersonate a company executive and steal $25 million through a fake transfer request.

3. AI Botnets and Zero-Day Exploits

Botnets-networks of compromised devices used to launch coordinated attacks-are becoming more intelligent thanks to machine learning. A new generation of AI-enhanced Mirai variants can scan the internet for vulnerable devices, adapt attack patterns on the fly, and carry out massive DDoS (Distributed Denial of Service) campaigns with minimal oversight.

AI also accelerates the discovery of zero-day vulnerabilities-flaws in software that no one else knows about yet. By analyzing open-source code, patch cycles, and system behaviors, AI can identify weak points before they're patched-giving attackers a crucial advantage.

4. Adversarial Machine Learning: Turning AI Against Itself

In a more advanced twist, hackers are now targeting the AI systems that protect us. This technique, known as adversarial machine learning, involves fooling AI models into making the wrong decisions.

For example:

- Adding harmless-looking text to a spam email can trick a filter into marking it as "safe."
- Corrupting a training dataset can teach an AI to overlook real threats, allowing malware to pass undetected.

This strategy doesn't just attack systems-it attacks their intelligence.

The New Reality

Cyberattacks powered by AI are faster, harder to trace, and more adaptive than anything seen before. They can move from intrusion to damage in seconds, operate without human intervention, and even learn from failed attempts. With tools like FraudGPT now accessible on the dark web, the barrier to entry for cybercrime has dramatically lowered-making it possible for a lone actor with minimal coding skills to launch devastating campaigns.

The cyber battlefield is no longer limited to lines of code. It's now a contest between intelligent systems-one trying to break in, the other trying to stop it.

REAL-WORLD EXAMPLES OF AI-GENERATED MALWARE

AI-generated malware is no longer confined to research labs or speculative forecasts. It has already appeared in the wild, deployed by cybercriminal groups and state-sponsored actors alike. These cases demonstrate just how deeply artificial intelligence is being integrated into cybercrime-automating attacks, personalizing deception, and bypassing even advanced defense systems.

1. FraudGPT and WormGPT: AI for Hire on the Dark Web

Among the most concerning developments is the rise of FraudGPT and WormGPT-custom AI models trained specifically for criminal purposes. Unlike ethical language models that include safety filters, these tools are designed to assist in phishing, scamming, and malware creation.

Key capabilities include:

- Writing highly convincing spear-phishing emails with perfect grammar
- Generating polymorphic ransomware code
- Helping attackers bypass CAPTCHA systems
- Offering scripts to exploit common software vulnerabilities

In one reported case, FraudGPT was used in a business email compromise (BEC) attack that stole $243,000 by impersonating a finance executive with a fake invoice request. These tools are available as paid subscriptions on dark web marketplaces, complete with user support and feature updates-turning cybercrime into a service economy.

2. BlackMamba: An AI-Powered Polymorphic Keylogger

BlackMamba is an experimental but fully functional malware prototype that uses generative AI to rewrite its code dynamically. Built with integration to ChatGPT-like models, it changes its behavior every time it runs-making it immune to traditional signature-based detection.

Once deployed, it acts as a keylogger, capturing keystrokes and sending them to the attacker. What makes it so dangerous is its ability to hide in plain sight, blending into legitimate processes and avoiding detection from common endpoint protection platforms. Security researchers used it to demonstrate how AI models, if misused, can serve as a live malware engine.

3. Morris II Worm: Exploiting AI Assistants

Inspired by the infamous Morris worm of 1988, Morris II is a newer type of AI-driven malware that propagates using prompt injection-a technique that manipulates large language models (LLMs) to behave in unintended ways. This worm doesn't spread by exploiting operating system flaws, but by targeting AI assistants embedded in apps, customer service bots, and email responders. It delivers malicious prompts that trick the AI into executing harmful commands, sending out spam, or leaking sensitive data. This case emphasizes a new class of vulnerabilities: AI prompt-level attacks, where the system does exactly what the attacker tells it to do-because it was trained to follow instructions.

4. Forest Blizzard and Emerald Sleet: Nation-State Threat Actors Using AI

AI isn't just being used by freelance hackers. Nation-state actors are increasingly adopting AI to improve their digital espionage capabilities.

- Forest Blizzard (linked to Russia) has reportedly used AI to craft phishing emails impersonating government agencies, designed to deliver custom backdoors such as Masepie for data theft.
- Emerald Sleet (associated with North Korea's Kimsuky group) has executed multi-stage attacks using platforms like Dropbox and PowerShell, enhanced with AI-encrypted payloads to evade detection. The use of AES encryption by an AI-guided dropper complicates analysis, as each payload appears unique.

These advanced persistent threat (APT) groups demonstrate how AI can assist in reconnaissance, payload creation, and obfuscation-making them harder to track and neutralize.

5. HP's AI-Generated Dropper Case

In 2024, HP cybersecurity researchers identified a French-language VBScript dropper containing commented sections that showed signs of AI generation. The malware delivered AsyncRAT, a remote access tool, and included phrasing and structure consistent with large language model output. This marked one of the first publicly analyzed malware samples suspected to have been written by a generative AI-blurring the line between human and machine authorship in cyber threats.

Lessons from the Field

These cases make one thing clear: AI is not a future risk-it is a present reality. From freelance attackers using AI-as-a-service to nation-states enhancing their offensive capabilities, the threat landscape is rapidly evolving. The most effective defenses now require systems that can recognize behavioral anomalies, predict attack vectors, and even anticipate how malicious AI might think.

DEFENSIVE STRATEGIES: HOW TO COUNTER AI-GENERATED MALWARE

As AI-generated malware grows smarter, faster, and more evasive, traditional cybersecurity approaches-like signature matching or manual monitoring-are no longer sufficient. Today's defenses must be just as intelligent, adaptive, and automated as the threats they face. This section outlines the most effective strategies currently being used to detect, deflect, and defeat AI-powered cyberattacks.

1. Behavioral Analytics and AI-Powered Threat Detection

One of the strongest weapons against AI malware is AI itself. Modern defense tools now rely on behavioral analytics, a technique that uses machine learning to understand what normal behavior looks like for each user, device, and system. Once this baseline is established, the system can detect even the smallest deviations-whether it's an employee logging in from an unusual location, or a process behaving in ways it never has before.

Platforms like Cortex XDR from Palo Alto Networks use real-time behavioral analysis to spot suspicious patterns, including those created by polymorphic malware. These tools can detect abnormal API calls, hidden network connections, and even minor timing anomalies-flagging attacks that would go unnoticed by rule-based systems.

2. Adversarial Machine Learning: Fighting AI with AI

AI models can also be used to test and challenge each other-a concept known as adversarial machine learning. In this setup, defensive AI systems are trained not only to recognize malicious behavior but also to predict how malicious AI might evolve.

For instance:

- Defensive models simulate attacks by generating "hostile" inputs (like prompt injections or altered malware code) to see how well the system responds.
- These simulations help expose vulnerabilities in a controlled environment before real attackers can exploit them.

Organizations like MITRE and OpenAI are exploring adversarial robustness testing to help build systems that can withstand AI-targeted attacks over time.

3. Deception Technology and Honeypots

Not all cybersecurity is about direct confrontation. Sometimes the best defense is distraction.

Deception technologies-such as honeypots or decoy files-create fake environments that look like real systems but serve one purpose: to lure attackers. Once malware engages with the decoy, it reveals its tactics and behavior in a controlled space, allowing analysts to study and block it without risk to actual infrastructure.

Advanced honeypots can mimic high-value systems like databases or internal admin portals, wasting the attacker's time and collecting data on their methods.

4. Deepfake and Phishing Awareness Training

While AI tools can automate and detect phishing attacks, human awareness remains crucial-especially with the rise of AI-generated deepfakes and voice cloning. Employee training programs must now go beyond basic cybersecurity hygiene and include modules on:

- How to spot suspicious emails that use perfect grammar and personalized content.
- Recognizing inconsistencies in video or audio communications.
- Verifying unusual requests-even if they appear to come from a known person.

Institutions can conduct red-team phishing simulations using AI to test how staff respond under pressure and adapt future training accordingly.

5. Zero Trust Architecture and Identity Verification

The concept of Zero Trust is simple: trust nothing by default. In a world where malware can imitate legitimate users and software, verifying every access request-no matter where it comes from-is essential.

This strategy includes:

- Multi-factor authentication (MFA) to verify identity beyond passwords.
- Behavioral biometrics, such as typing patterns or mouse movements, which are difficult for AI to replicate.
- Micro-segmentation, which isolates systems and limits how far an attacker can move even if they breach one part of the network.

By assuming that any device, user, or software could be compromised, Zero Trust creates layers of security that make it much harder for threats to spread.

6. Explainable AI (XAI) and Transparency

One major concern with deploying AI for defense is its "black box" nature-security teams often don't understand why an AI made a particular decision. That's where Explainable AI (XAI) comes in.

XAI tools provide clear reasoning behind AI actions, making it easier for human analysts to audit, adjust, and trust AI-driven defenses. This also helps during post-attack investigations, legal compliance checks, and training exercises.

As cybersecurity becomes increasingly AI-powered, explainability ensures that human judgment remains in the loop.

Staying One Step Ahead

Defending against AI-generated malware isn't just about installing the right tools. It's about creating an ecosystem that learns continuously, adapts quickly, and remains resilient in the face of intelligent adversaries.

The most effective strategies combine:

- Intelligent technology (behavioral analytics, deception, adversarial AI),
- Informed people (deepfake awareness, phishing training),
- And forward-looking policies (zero trust, transparency, and auditing).

With these in place, organizations stand a much better chance of keeping up with threats that think, learn, and attack like never before.

SECTOR-SPECIFIC RISKS AND MITIGATIONS: AI CYBERSECURITY IN CRITICAL DOMAINS

While AI-generated malware poses a global risk, its impact can vary dramatically depending on the sector it targets. Each industry has unique systems, vulnerabilities, and regulatory requirements, making tailored defense strategies essential. This section outlines how AI-powered threats are affecting three high-impact domains-healthcare, education, and finance-and what institutions in each space can do to stay secure.

1. Healthcare: Smart Hospitals, Fragile Targets

Risks

Healthcare systems are increasingly connected-using AI to assist with diagnostics, manage patient records, and operate medical devices. However, this connectivity comes at a price:

- AI-enhanced medical device hijacking: Attackers can manipulate firmware in devices like IV pumps or MRI machines, potentially endangering lives.
- Deepfake medical records: Generative Adversarial Networks (GANs) can fabricate lab results, diagnoses, or entire patient histories-enabling insurance fraud or even misdiagnosis.

Hospitals are especially vulnerable because many still use legacy systems not designed for today's threat landscape.

Mitigations

- Anomaly detection for medical IoT: AI tools like Cynerio continuously monitor connected devices, alerting staff to irregular data flows or unauthorized access.
- HIPAA-compliant AI auditing: Healthcare providers must routinely check diagnostic models for data bias, drift, or adversarial manipulation.
- Regular patching and software updates are critical, especially in older medical equipment that lacks built-in security.

2. Education: The Digital Classroom Under Siege

Risks

As schools and universities adopt smart boards, AI-assisted grading tools, and virtual learning platforms, they face an expanding attack surface:

- AI-graded essay exploitations: Attackers submit prompts that exploit vulnerabilities in grading systems powered by tools like ChatGPT APIs, enabling remote code execution (RCE).
- IoT botnets in schools: Unsecured devices like smart projectors or Wi-Fi-connected HVAC systems can be hijacked and added to DDoS networks.

Educational institutions often lack dedicated cybersecurity teams, making them easy targets for experimentation by amateur hackers or botnet operators.

Mitigations

- Network segmentation: Isolate student networks from administrative and financial systems using Virtual LANs (VLANs). This limits the spread of any successful breach.
- AI literacy training: Faculty and staff should be trained to recognize AI-generated phishing emails, especially deepfake voice messages pretending to be principals, finance officers, or tech staff.
- Secure device procurement policies: Any IoT or smart device entering the school ecosystem must meet baseline security standards and receive regular firmware updates.

3. Finance: AI in the Hands of Digital Thieves

Risks

Financial institutions are prime targets for AI-powered attacks due to the volume and value of the data they handle:

- Synthetic identity fraud: Generative AI can create entirely fake identities-complete with facial images, transaction histories, and even fake LinkedIn profiles-for use in loan fraud, credit abuse, and tax evasion.
- Algorithmic market manipulation: Malicious bots use reinforcement learning to study market behavior, spoof trades, and trigger artificial volatility-without triggering traditional fraud detection systems.

These attacks are not only hard to detect-they're hard to trace back to a human culprit.

Mitigations

- Explainable AI (XAI): Financial services must use interpretable machine learning tools like Fiddler AI to audit black-box algorithms, ensuring that AI-driven trades or loan decisions are lawful and fair.
- Behavioral biometrics: Tools like NuDetect from Mastercardanalyze user behavior (e.g., typing speed, cursor movement) to distinguish between real customers and AI-generated identities.
- AI stress testing and red-teaming: Simulated attacks help test how trading systems respond under adversarial AI pressure-ensuring operational resilience during targeted manipulation campaigns.

Tailored Cyber Hygiene Is No Longer Optional

AI-generated malware does not discriminate, but its methods of attack are highly sector-sensitive. A one-size-fits-all approach won't work.

Instead, cybersecurity in the AI era demands:

- Context-aware risk analysis
- Domain-specific safeguards
- Continuous awareness training across all levels of staff

Institutions that understand their unique vulnerabilities-and respond with proactive, AI-literate strategies-are far more likely to withstand the next wave of intelligent cyberattacks.

EMERGING SOLUTIONS AND FUTURE OUTLOOK: STAYING AHEAD OF AI THREATS

The rapid rise of AI-generated malware has pushed defenders to think beyond traditional security tools. As cybercriminals exploit generative models and automation to scale their attacks, cybersecurity professionals are developing advanced countermeasures that blend technology, policy, and ethics. This section explores the most promising innovations shaping the future of cyber defense-and what institutions must do now to prepare for what's coming next.

1. Quantum-Resistant AI Cryptography

The looming threat of quantum computing-machines powerful enough to break current encryption-adds another layer of urgency to the cybersecurity challenge. If combined with AI, quantum-powered attacks could decipher passwords, decrypt secure communications, and dismantle conventional cryptographic systems within seconds.

To counter this, researchers are developing quantum-resistant cryptographic algorithms, often based on lattice theory. These are now being paired with machine learning models to protect sensitive information even in a post-quantum future.

One such family of algorithms, CRYSTALS-Kyber, has been approved by NIST (National Institute of Standards and Technology) and is being adopted in pilot programs to secure AI communication pipelines. This integration ensures that AI models handling authentication or transaction verification remain secure even if quantum capabilities fall into the wrong hands.

2. Federated Learning for Privacy-Preserving Threat Intelligence

A major limitation in cybersecurity is the siloed nature of threat data. Organizations are often hesitant to share security breaches or attack patterns, fearing reputational damage or legal exposure. This limits the collective ability to learn from attacks across sectors.

Federated Learning offers a solution. Instead of sharing raw data, organizations like hospitals or banks can train AI models collaboratively on decentralized data sets. Each participant's data stays private, while the collective intelligence improves. Tools like OWASP's FLAPI framework make this possible by coordinating learning across different nodes while preserving data confidentiality.

This model is especially valuable for:

- Detecting rare attack signatures that only appear in certain industries
- Training AI models on diverse data without regulatory hurdles
- Building a global, distributed immune system for cyber defense

3. AI Risk Governance and Ethical Frameworks

As AI plays a growing role in both offense and defense, governance and ethical oversight become critical. Misuse of AI by either side-whether a rogue attacker or a poorly configured defense system-can lead to legal liabilities, discrimination, or infrastructure failure.

Policymakers are now working to close these gaps:

- The EU AI Act classifies cybersecurity as a high-risk AI domain, mandating transparency, explainability, and robust auditing.
- Organizations like ISO and IEEE are publishing AI security standards that guide the design and deployment of responsible systems.
- Explainable AI (XAI) is becoming a requirement, especially in finance and healthcare, where users must understand how and why decisions are made.

In the coming years, institutions may be required to implement AI ethics boards, conduct regular audits, and maintain public records of AI model usage-just as they currently do for financial disclosures or data breaches.

4. Simulated Threat Environments and Cyber AI Labs

A growing trend among advanced organizations is the use of AI cyber ranges or simulated environments-virtual laboratories where security teams can test responses to AI-powered attacks in real time.

These simulations allow organizations to:

- Evaluate the resilience of their defenses against polymorphic malware
- Train AI models to recognize novel attacks in a controlled setting
- Prepare staff for multi-vector threats that unfold at machine speed

Companies like IBM, Microsoft, and NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) are already using AI cyber ranges to develop coordinated global response strategies.

5. Closing the AI Knowledge Gap

The final frontier in emerging solutions isn't a tool-it's education. The effectiveness of even the most advanced defense systems depends on the people who manage and use them. Across every industry, there's a growing need for:

- AI-literate professionals who understand the risks and responsibilities of deploying intelligent systems
- Faculty development programs that integrate AI ethics, threat modeling, and adversarial testing into mainstream education
- Public-private partnerships to ensure that defensive AI research stays ahead of cybercriminal innovation

Cybersecurity is no longer just a technical field-it is a cross-disciplinary challenge requiring collaboration between engineers, educators, policymakers, and everyday users.

CONCLUSION AND ACTIONABLE TAKEAWAYS: BUILDING CYBER RESILIENCE IN THE AGE OF AI

Artificial intelligence has ushered in a new chapter in the history of cybersecurity-one marked by speed, scale, and sophistication on both sides of the battlefield. AI-generated malware is not just a futuristic concept; it is an urgent and evolving reality. From polymorphic viruses and deepfake phishing scams to autonomous botnets and data-poisoning attacks, malicious actors now wield AI with dangerous precision.

But defenders are not powerless. AI is also empowering cybersecurity professionals with the ability to detect unknown threats, automate incident response, and stay ahead of adversaries through predictive modeling and behavioral analytics. The challenge now lies in closing the gap between offensive and defensive innovation-through smarter systems, better education, and stronger ethical frameworks.

For Institutions and Enterprises

- Adopt AI-native security platforms: Tools like Cortex XDR, CrowdStrike Falcon, and DarktraceAntigena offer real-time threat detection, autonomous response, and behavioral analytics.
- Simulate AI-driven attacks regularly: Red-teaming exercises involving AI-generated phishing or malware can help prepare your staff for real-world scenarios.
- Implement a Zero Trust security model: Enforce multi-factor authentication, least-privilege access, and network segmentation to prevent lateral movement after a breach.
- Invest in Explainable AI (XAI): Ensure that your security systems offer transparent decision-making, especially in high-risk environments like finance and healthcare.

For Critical Sectors

- Healthcare: Prioritize patching and monitoring of legacy medical devices; conduct regular audits on AI diagnostic tools to ensure accuracy and fairness.
- Education: Train faculty and IT staff in identifying AI-based phishing attempts; segment smart devices and learning systems from administrative infrastructure.
- Finance: Monitor for synthetic identities using behavioral biometrics; test financial algorithms against AI-enabled spoofing and manipulation.

For Policymakers and Educators

- Support regulation with teeth and vision: Frameworks like the EU AI Act are essential for promoting transparency, ethical AI use, and security compliance.
- Build AI-capable workforce pipelines: Faculty development programs must now include modules on cybersecurity, AI ethics, adversarial testing, and digital threat modeling.
- Promote collaborative intelligence sharing: Encourage partnerships between public agencies, academic institutions, and private industry through federated learning and threat intelligence hubs.

FINAL THOUGHT

The battle between AI-powered attackers and defenders has already begun-and it will only intensify. The institutions that will thrive in this environment are those that see AI not just as a tool, but as a shared responsibility. By combining intelligent systems with human judgment, ethical oversight, and a culture of continuous learning, the cyber world can remain not just secure-but resilient, adaptive, and forward-looking.The future of cybersecurity won't be defined by which side has the most powerful AI. It will be defined by who uses it more wisely. Emerging technologies like federated learning, explainable AI, and quantum-safe cryptography hold great promise-but they require foresight, coordination, and ethical grounding.To stay ahead of intelligent threats, institutions must invest not just in smarter tools, but in smarter cultures of vigilance, learning, and trust. The goal is no longer just to respond to cyberattacks-it is to anticipate, resist, and outthink them.

WHAT TO TEACH: FUTURE-READY CURRICULUM FOR INDUSTRY 5.0

Er. Kapil Murdia *

Industry 5.0 has thrown several challenges to various fields, and in particular education of youth at K-12 and higher education. Since processes of production and services are likely to change and a good part of basic cognitive skills-based jobs are likely to be performed by machines, youth would need to acquire new skills. The paper defines key features of Industry 5.0 and highlights areas of academic interventions.

ABSTRACT

As the world transitions into the fifth industrial revolution, a profound reimagining of education is essential. Industry 5.0 emphasizes a human-centric, collaborative paradigm where advanced technologies like AI, IoT, and robotics enhance-not replace-human capabilities. This article explores the emerging educational imperatives aligned with Industry 5.0, introducing Education 5.0 as a learner-centered, interdisciplinary, and values-driven model. It outlines key curriculum strategies and skillsets necessary to prepare learners to thrive in a technologically advanced and ethically complex future.

1. INTRODUCTION

Education is undergoing a transformative shift propelled by rapid technological evolution and deeper insights into how humans learn. Education 5.0 encapsulates this change-a learner-centered, digitally enriched framework that prioritizes personalization, creativity, emotional intelligence, and ethical reasoning.

Unlike the rigid, standardized models of the past, Education 5.0 moves away from rote memorization and passive content absorption. It encourages active, interdisciplinary learning, cultivating critical thinking and socio-emotional skills essential in an age of automation and artificial intelligence. At its core, Education 5.0 aims to integrate emerging technologies-such as AI, blockchain, and extended reality-with the irreplaceable qualities of human cognition and compassion.

> *Unlike the rigid, standardized models of the past, Education 5.0 moves away from rote memorization and passive content absorption. It encourages active, interdisciplinary learning, cultivating critical thinking and socio-emotional skills essential in an age of automation and artificial intelligence.*

2. KEY PILLARS OF EDUCATION 5.0

The fundamental components of Education 5.0 include:

- Personalized Learning: Leveraging AI-powered platforms to adapt learning paths based on individual pace and preference.
- Critical Thinking and Problem Solving: Emphasizing analytical thinking, creative reasoning, and decision-making over rote content.
- Digital Fluency: Familiarity with digital ecosystems, including AI, IoT, blockchain, and virtual/augmented reality.
- Socio-Emotional Intelligence: Encouraging empathy, collaboration, and resilience alongside academic competence.
- Interdisciplinary Integration: Bridging STEM, humanities, and the arts for holistic, meaningful education.

3. UNDERSTANDING INDUSTRY 5.0: THE HUMAN-CENTRIC REVOLUTION

Industry 5.0 represents a shift from automation-dominated paradigms to human-machine collaboration. It focuses on leveraging intelligent systems to augment human capabilities rather than replace them.

Key Characteristics of Industry 5.0:

- Collaborative Robotics (Cobots): Intelligent machines designed to work safely and efficiently alongside humans.
- Internet of Things (IoT) and Edge Computing: Real-time data analytics empower decentralized and adaptive decision-making.
- 3D Printing and Additive Manufacturing: Enables flexible, on-demand production with reduced environmental footprint.
- Sustainable Technologies: Promotes circular economy models, green innovations, and ethical manufacturing.

Industry 5.0, unlike its predecessors, prioritizes human dignity, creativity, and ecological responsibility within technological systems.

4. FROM INDUSTRY 5.0 TO EDUCATION 5.0: CLOSING THE SKILLS GAP

As workplaces evolve, traditional educational paradigms struggle to remain relevant. Emerging roles now demand a blend of technical proficiency, creative intelligence, ethical judgment, and emotional resilience.

Skills Required in the Industry 5.0 Era:

- Expertise in AI collaboration, data analytics, and sustainable systems.
- New occupations in AI ethics, cybersecurity, human-machine interface design, and innovation management.

* *Technology Expert and Design Thinker*

- The need for cross-disciplinary fluency and lifelong learning abilities.

Education 5.0 offers a timely response to these demands, reshaping learning environments to promote purpose-driven, adaptive, and experiential education.

5. FUTURE SKILLS FRAMEWORK FOR INDUSTRY 5.0

1. AI and Automation Fluency
- Engaging with intelligent systems as co-workers.
- Using data and automation to enhance efficiency and creativity.
2. Ethical and Human-Centered Thinking
- Fostering responsible technology development.
- Navigating ethical dilemmas in digital environments.
3. Emotional Intelligence and Collaboration
- Strengthening interpersonal skills in mixed (human and machine) teams.
- Leading with empathy and inclusivity.
4. Sustainability and Environmental Ethics
- Promoting green innovation and circular economy principles.
- Embedding climate literacy and ecological responsibility.
5. Lifelong Learning and Agility
- Encouraging self-directed, modular, and micro-credential-based learning.
- Instilling entrepreneurial mindsets and innovation culture.

6. EDUCATIONAL IMPERATIVES FOR A FUTURE-READY CURRICULUM

1. Personalized Learning Models
- Utilize AI for custom learning trajectories.
- Replace standardized testing with project-based and competency-driven assessment.
2. Experiential and Immersive Pedagogies
- Employ AR/VR for contextual, real-world simulations.
- Foster industry-academia collaboration for internships and apprenticeships.
3. AI Integration in Teaching and Learning
- Use AI for formative feedback, career guidance, and adaptive content delivery.
- Expand global access through multilingual AI and learning analytics.
4. Embedding Sustainability and Digital Ethics
- Educate on ecological footprints, sustainability metrics, and green entrepreneurship.
- Inculcate digital ethics, data privacy, and responsible AI practices.

7. CONCLUSION: EMPOWERING A HUMAN-CENTERED, TECH-DRIVEN FUTURE

Education 5.0 is not merely a response to technological advancement-it is a proactive vision for a more humane, inclusive, and sustainable future. It aligns curriculum, pedagogy, and purpose with the demands of Industry 5.0, ensuring learners are equipped to innovate responsibly, collaborate effectively, and lead ethically in a dynamic world.

By embracing Education 5.0, institutions can ensure that education not only keeps pace with technological progress but also remains anchored in the values that define our humanity.

REFERENCES

1. https://youtu.be/17xa6iT51AE
2. https://www.youtube.com/watch?v=DW4h3Q5dNCU
3. European Commission (2021). Industry 5.0: Towards a sustainable, human-centric and resilient European industry.
4. UNESCO (2022). Reimagining our futures together: A new social contract for education.
5. Schwab, K. (2017). The Fourth Industrial Revolution. World Economic Forum.

About Cover Page

JAYANT VISHNU NARLIKAR (1938-2025)

Early Life & Education

Born on 19 July 1938 in Kolhapur, Maharashtra, into an erudite family-his father, Vishnu Vasudev Narlikar, was a mathematics professor at BHU and his mother, Sumati, a Sanskrit scholar. Completed his B.Sc. at Banaras Hindu University in 1957 and pursued mathematics at Cambridge University, where he became Senior Wrangler, Tyson Medallist, and earned his Ph.D. under Fred Hoyle by 1963.

Scientific Contributions

Co-developed the Hoyle-Narlikar theory of gravity, merging Einstein's relativity with Mach's principle and serving as a cornerstone of the quasi-steady-state cosmology-an alternative to the Big Bang model. In 1972, he joined TIFR and led the Theoretical Astrophysics Group. Later, he founded and directed the Inter-University Centre for Astronomy and Astrophysics (IUCAA) in Pune (1988-2003), shaping it into a world-class research institution. From 1999-2003, he led ISRO-supported stratospheric experiments (up to ~41?km), recovering viable microorganisms and supporting the panspermia hypothesis.

Science Outreach & Writing

A tireless science communicator, he authored over 50 books and numerous articles-ranging from hardcore cosmology to vibrant Marathi and English science fiction. He also produced TV appearances (e.g., on Doordarshan and Carl Sagan's Cosmos) and narrated complex ideas with clarity. His Marathi autobiography, Chaar Nagarantale Mazhe Vishva, earned the Sahitya Akademi Award (2014).

HIGHER EDUCATION IN THE UNITED ARAB EMIRATES: GOVERNANCE, ACADEMIC OFFERINGS, COST REGULATION, QUALITY CONTROL, AND EXIT MECHANISMS

O.P. Bohra *

Of late UAE has developed a hub of higher education in the Middle East. Many Indian institutions of higher education have set up campuses there. Many Indian students are studying in the UAE. The article explores several dimensions of higher education at UEA.

ABSTRACT

The United Arab Emirates (UAE) has developed a multi-tiered, internationally benchmarked framework for regulating and assuring the quality of higher education across its federal and emirate systems. This article presents a detailed overview of policy, status, fee structures, regulatory norms, quality assurance mechanisms, and institutional closures over the last decade. With increasing foreign branch campuses and ambitious national education goals, the UAE continues to refine its educational governance to align with global standards and regional aspirations.

GOVENANCE:

1. POLICY FRAMEWORK FOR FOREIGN EDUCATIONAL INSTITUTIONS IN THE UAE

The United Arab Emirates (UAE) has rapidly evolved into a global center for transnational education by adopting progressive policies that attract prestigious foreign universities and international education providers. This section outlines the regulatory framework and strategic developments enabling this transformation.

> *The United Arab Emirates (UAE) has rapidly evolved into a global center for transnational education by adopting progressive policies that attract prestigious foreign universities and international education providers.*

1.1 Establishment of Foreign University Campuses

Licensing and Accreditation Authorities

- The Commission for Academic Accreditation (CAA), operating under the Ministry of Education (MoE), is the federal authority responsible for granting:
  - o Institutional licensure
  - o Program accreditation

  This applies to universities operating in both the mainland and free zones across the UAE.
- In the Dubai free zones-notably Dubai International Academic City (DIAC) and Dubai Knowledge Park-the Knowledge and Human Development Authority (KHDA) regulates:
  - o Academic authorization
  - o Program registration
  - o Quality assurance via its University Quality Assurance International Board (UQAIB)

  The UQAIB ensures that foreign university branches deliver programs equivalent in content and quality to their parent institutions.

Recent Regulatory Developments

- A landmark Memorandum of Understanding (MoU) signed in March 2025 between the Ministry of Higher Education and Scientific Research (MoHESR) and the KHDA aims to:
  - o Streamline licensing processes
  - o Reduce approval timelines from several months to a few weeks
  - o Harmonize regulations for free-zone and mainland institutions
- Between 2000 and 2025, the number of licensed foreign university campuses in the UAE increased dramatically-from approximately 8 to over 120, spanning Abu Dhabi, Dubai, Sharjah, and various academic free zones.

Entry Requirements and Procedures

To operate legally within the UAE, foreign universities must:

- Secure institutional licensure and program accreditation from the CAA
- Obtain KHDA authorization for free-zone operations, which includes:
  - o Campus and facility inspections
  - o Verification of faculty qualifications
  - o Scrutiny of academic offerings and delivery modes.

2. RECOGNITION OF FOREIGN DEGREES IN THE UAE

To support international academic mobility and workforce integration, the UAE has overhauled its foreign degree recognition system to ensure efficiency, transparency, and alignment with international standards.

*Former Faculty member, University of Wollongong, UEA (opbohra51@gmail.com)

2.1 Certificate Equivalency Reform

The Ministry of Education has replaced the traditional degree attestation system with a more streamlined Certificate Equivalency framework, marked by:

- Reduction in documentation requirements (from 14 to 4 documents)
- Removal of mandatory physical attendance or credit transfer restrictions
- Inclusion of online and distance-learning degrees, provided the delivery method is verifiable

2.2 Verification Process

A two-step verification system, administered via Dataflow or Quadra Bay, is now in place:

1. Degree Authentication: Verification of credentials from the issuing institution
2. Certificate Issuance: The Ministry provides a formal Certificate of Recognition within approximately 30 working days. Fees for recognition are:

- AED 100 for Bachelor's
- AED 150 for Master's
- AED 200 for Doctorate degrees

Applicants may appeal decisions within 90 days of issuance.

2.3 Conditions and Scope

- Degrees must originate from accredited foreign institutions, including those offering online or blended formats
- The system does not recognize:
  - o Vocational certificates
  - o Short-term courses
- Degrees in regulated professions (e.g., medicine, engineering, law) may require additional evaluation or licensure

3. STRATEGIC GOALS AND IMPACTS

The UAE's higher education policy is guided by long-term national strategies and an ambition to establish itself as a global knowledge economy.

Key Objectives

- Attract leading global universities to establish branch campuses (e.g., Murdoch University, Middlesex University, Heriot-Watt University)
- Increase international student enrollment by offering a cost-effective and high-quality alternative to traditional study destinations
- Streamline and digitize regulation to promote ease of access, institutional agility, and academic excellence.

These initiatives align closely with the Dubai Education Strategy 2033 and broader national frameworks such as UAE Vision 2031, which emphasize the role of education in sustainable development and global competitiveness.

Academic Offerings:

2. Higher Education Institutions in the United Arab Emirates

Universities and Degree-Granting Institutions

The United Arab Emirates (UAE) has emerged as a regional leader in transnational higher education, with a rapidly expanding network of universities and educational institutions. As of 2024, the higher education landscape is marked by a strong presence of both national and international institutions, driven by supportive regulatory frameworks and the country's vision to become a global knowledge hub.

Institutional Overview

- 123 universities are licensed by the federal Commission for Academic Accreditation (CAA) under the Ministry of Education.
- Of these, 67 universities have received full program-level accreditation by the CAA.
- The UAE hosts over 130 private and international higher education institutions (HEIs) operating across its emirates.
- Dubai alone accommodates approximately 30 to 60 foreign branch campuses, with 39 institutions formally recognized by the Knowledge and Human Development Authority (KHDA).

This diverse ecosystem includes:

- National universities, such as:
  - o United Arab Emirates University (UAEU)
  - o Zayed University
  - o Higher Colleges of Technology (HCT)
- International branch campuses, including:
  - o University of Wollongong in Dubai
  - o Heriot-Watt University Dubai
  - o Birla Institute of Technology and Science (BITS) Pilani, Dubai Campus
  - o Murdoch University Dubai, among others

While consolidated national data remains decentralized, the KHDA in Dubai provides detailed and reliable insights into institutional distributions, especially within Dubai's academic free zones, such as Dubai International Academic City (DIAC) and Dubai Knowledge Park.

Institutional Summary Table (as of 2024)

Category	*Approximate Count*	*Geographic Coverage*
CAA-licensed universities	123	Nationwide
CAA-accredited universities	67	Nationwide
Private & international HEIs	>130	Nationwide
Foreign branch campuses	30-60	Dubai
Private K-12 schools	227	Dubai
Early childhood centers	274	Dubai
Vocational/training centers	1,167	Dubai

Key Observations

1. Steady Expansion: The higher education sector in the UAE continues to expand, with a strategic emphasis on internationalization. Free zones in Dubai have been particularly instrumental in attracting foreign universities.
2. Globalization of Education: Foreign branch campuses now represent nearly half of all operating universities in the country, reinforcing the UAE's role as a regional and international hub for transnational education.
3. Comprehensive Infrastructure: Growth is not limited to higher education. The K-12, early childhood, and vocational training sectors-especially in Dubai-demonstrate a well-rounded approach to educational development across all levels.

This multi-tiered educational framework not only reflects the UAE's commitment to academic excellence and internationalization but also aligns with national strategies such as UAE Vision 2031 and Dubai Economic Agenda (D33), which prioritize knowledge-based economic transformation through educational investment and innovation.

3. TYPES OF COURSES AND STUDENT DEMOGRAPHICS IN UAE HIGHER EDUCATION

The United Arab Emirates (UAE) has developed a vibrant higher education ecosystem that attracts a globally diverse student body. With its expanding portfolio of academic programs and branch campuses, the UAE offers a wide array of courses tailored to meet global and regional labor market needs. This section examines the most sought-after disciplines, enrollment patterns, and demographic composition of international students.

3.1 Popular Fields of Study

International students in the UAE predominantly pursue programs aligned with global industry demands and national development goals. Based on comprehensive enrollment data from major academic zones such as Dubai International Academic City (DIAC), the most popular fields include:

- Business and Management (55-60%)
  Specializations: Finance, Marketing, Human Resource Management, International Business
- Engineering (11%)
  Subfields: Civil, Mechanical, Electrical, Aerospace, and Construction Engineering
- Information Technology and Computer Science (9%)
- Health Sciences

Includes: Medicine, Nursing, Public Health

- Other Notable Fields

Tourism and Hospitality, Media and Communication, Architecture, Renewable Energy, and Humanities

DIAC alone hosts over 500 academic programs across bachelor's, master's, and doctoral levels-demonstrating the depth and breadth of the UAE's academic offerings.

3.2 Country-Wise Student Composition

The UAE's international student population is highly diverse, representing over 150 nationalities. However, several countries account for a significant proportion of enrollments:

India remains the largest source of international students, particularly in Dubai, followed by substantial cohorts from Pakistan and MENA countries. Students from China and East Asia represent a growing segment, especially at globally branded campuses.

3.3 Student Levels and Academic Profiles

The distribution of students across academic levels reflects global trends and institutional capacity (as in table below):

- Undergraduate students: 50-60% of total enrollment
- Postgraduate (Master's) students: 30-40%
- Doctoral candidates: A smaller segment, primarily concentrated in research-focused universities

Campus Snapshots

- University of Wollongong in Dubai
  Hosts ~3,700 students from 108 countries, offering a balanced undergraduate and postgraduate program mix
- Heriot-Watt University Dubai
  Enrolls ~5,000 students from 115 nationalities, with 50+ programs spanning business, engineering, and IT

Country	Approximate Share	Common Fields of Study
India	43% of new enrollments in Dubai; 17% UAE-wide	Business, Engineering, IT, Management
Pakistan	5-10%	Business, Engineering, IT
Russia	5%	Business, Engineering, Management
Saudi Arabia	3%	Business, Engineering
Egypt, Jordan, Oman, Syria	5,000+ students each	Business, Engineering, IT
Others (e.g., China, East Asia)	Emerging segments	Diverse fields; growing representation

- The British University in Dubai (BUiD)

A research-oriented institution offering bachelor's degrees in fields such as law, finance, engineering, and artificial intelligence, along with postgraduate and doctoral research opportunities

The UAE's higher education sector not only mirrors global academic demand but also adapts strategically to regional priorities. Business, engineering, and IT remain the top academic choices among international students, particularly those from South Asia and the MENA region. With its expanding educational infrastructure and internationally accredited programs, the UAE continues to strengthen its position as a preferred destination for quality transnational education.

Cost Controls:

4. TUITION FEES AND REGULATORY FRAMEWORK IN UAE HIGHER EDUCATION

The cost of higher education in the United Arab Emirates (UAE) reflects its market-oriented model, especially within the private and transnational education sector. While tuition is generally unregulated, a robust quality assurance and licensing framework ensures transparency and institutional accountability.

4.1 Tuition Fee Structure in Higher Education Institutions

Tuition fees in UAE universities vary significantly based on the program, institution, and emirate. Most universities operate on a per-credit-hour or annual tuition basis. The average tuition ranges as follows:

- Private and International Branch Campuses (e.g., Middlesex University, Heriot-Watt, University of Wollongong):
  - o AED 30,000 to AED 70,000+ per academic year for undergraduate and taught master's programs
- High-cost programs such as Medicine and Engineering:
  - o AED 100,000 or more annually, with limited scholarship opportunities for medical programs
- Postgraduate and professional programs:
  - o Fees typically higher for MBA, specialized engineering, or AI/technology fields

Note: The fee structure often includes tuition, examination charges, and learning resources, though some services are charged separately.

4.2 Additional Fees and Financial Obligations

Besides tuition, students may incur several other mandatory and optional costs. These include (as in table below):

Institutions are required to disclose all charges upfront. Practices such as hidden fees or forced participation in optional activities are strictly prohibited.

4.3 VAT and Financial Regulation

- A 5% Value-Added Tax (VAT) applies to tuition at private higher education institutions, unless the institution is fully or majority government-funded.
- Universities are not subject to federal tuition caps; however, they must obtain and maintain licensure from the Commission for Academic Accreditation (CAA) and, for Dubai-based institutions, additional oversight by the Knowledge and Human Development Authority (KHDA).
- While these bodies focus on academic quality and institutional integrity rather than price control, they contribute to overall consumer protection.

4.4 Regulatory Oversight and Legal Framework

The regulation of education-related fees is embedded in a multi-layered legal framework:

- Federal Decree Law No. 18 of 2020: Governs private education institutions nationwide.
- Dubai: The KHDA enforces the School Fees Framework, which aligns fee increases with the Education Cost Index (ECI) and school inspection ratings.
- Abu Dhabi: The Abu Dhabi Department of Education and Knowledge (ADEK) implements a similar regulatory approach.
- Sharjah: Oversight is provided by the Sharjah Private Education Authority (SPEA).
- Students of Determination: Institutions cannot charge extra fees unless individualized services are provided, and even then, charges must reflect actual costs.

4.5 Summary and Observations

- University tuition is market-driven, generally ranging from AED 30,000 to AED 70,000, and may exceed AED 100,000 for high-demand fields like medicine.
- VAT applies unless the institution is government-supported.

Fee Type	*Typical Amount*	*Notes*
Application Fee	Up to AED 500	Refundable if admission is not offered
Registration Deposit	?10% of annual tuition	Deductible from tuition
Re-registration Fee	?5% (or AED 500 max)	For continuing students
Mandatory Service Fees	Up to AED 20,500/year	Covers labs, books, medical, and admin costs
Optional Extras	AED 3,000-5,000	Transport, uniforms, trips (opt-in only)

- Licensing and oversight by the CAA (federal) and KHDA (Dubai) ensure quality assurance and fee transparency.
- Fee components are categorized into mandatory and optional types, with strong regulatory emphasis on clarity and fairness.
- No centralized fee cap exists for higher education, but clear rules on registration deposits, optional charges, and disclosure promote financial accountability.

This detailed regulatory environment-while not imposing strict fee controls-offers a balance between institutional autonomy and consumer protection. The UAE's tuition framework, supplemented by oversight mechanisms, plays a key role in sustaining the country's attractiveness as a regional higher education hub.

Quality Regulation:

5. QUALITY ASSURANCE FRAMEWORK AND INSTITUTIONAL CLOSURES IN UAE HIGHER EDUCATION

The United Arab Emirates (UAE) has built a rigorous, multilayered quality assurance system to regulate and elevate standards across its higher education landscape. This framework operates at both federal and emirate levels and incorporates global benchmarks to position the UAE as a regional education and innovation hub. It also includes robust mechanisms for managing institutional closures, ensuring minimal disruption to learners.

5.1 Quality Control Measures in Higher Education

Federal Oversight: Commission for Academic Accreditation (CAA)

The CAA, under the UAE Ministry of Education, is responsible for institutional licensing and program accreditation. It evaluates universities on the basis of:

- Governance and Quality Assurance (QA) Systems
- Faculty Qualifications and Research Output
- Student Services and Learning Outcomes
- Infrastructure, Financial Sustainability, and Community Engagement

In 2024, the CAA adopted the Outcome-Based Evaluation Framework (OEF), introducing data-driven accreditation cycles (2-6 years) based on Key Performance Indicators (KPIs) such as:

- Graduate employment rates
- Research productivity
- Academic integrity and student satisfaction

The Certified Reviewer Program, led by trained academics, supports continuous institutional monitoring and quality improvement.

Emirate-Level and Free-Zone Oversight

Several emirate-specific bodies complement federal oversight:

- Dubai: KHDA and UQAIB
    - o The Knowledge and Human Development Authority (KHDA), through its University Quality Assurance International Board (UQAIB), oversees free-zone institutions. It ensures academic equivalence with parent institutions abroad and can enforce probation or institutional closure where necessary.
- Abu Dhabi: ADEK
    - o The Abu Dhabi Department of Education and Knowledge (ADEK) aligns academic programs with the emirate's strategic goals and monitors institutional compliance.
- Sharjah: SPEA
    - o The Sharjah Private Education Authority (SPEA) licenses and inspects private universities, colleges, and K-12 schools, covering over 170,000 students.

Nationwide Quality Management Process

The UAE applies a phased and performance-linked quality assurance cycle:

1. Pre-Licensing Review: Institutions must demonstrate academic rigor, QA structures, faculty competencies, and legal compliance.
2. Accreditation Tiers: Based on performance, institutions undergo reviews every 2 to 7 years.
3. Continuous Monitoring: Requires internal self-studies, student feedback, external peer reviews, and documented improvement plans.
4. Enforcement Mechanisms: Underperforming institutions may face probation, program suspension, or license revocation.

International Quality Benchmarking

UAE regulators maintain affiliations with global QA bodies such as:

- INQAAHE - International Network for Quality Assurance Agencies in Higher Education
- ANQAHE - Arab Network for Quality Assurance
- AACSB, ACEN, WFME, and other accreditation agencies

This global engagement ensures that foreign branch campuses meet the same academic standards as their parent institutions abroad.

Exit Mechanism:

5.2 Institutional Closures: Reasons, Process, and Response

Despite the UAE's growing higher education sector, some institutions have closed over the past decade. These closures were due to non-compliance, financial distress, or declining enrollments. Regulatory bodies have robust protocols to manage such closures and safeguard students.

Key University Closures (2015-2025)

Institution	*Emirate*	*Operating Years*	*Closure Year*	*Reason*
International Horizons College	Dubai	2011-2016	2016	Low enrollment
Ittihad University	RAK	1999-~2016	~2016	Financial challenges
Al Hosn University	Abu Dhabi	2005-2021	2021	Placed on probation, later closed
Al Falah University	Dubai	2015-2022	2022	Accreditation revoked
MODUL University Dubai	Dubai	2016-2020	2020	MOE license revoked
Al Ghurair University	Dubai	-	2022	Sudden closure after probation

Noteworthy Examples

- Murdoch University Dubai: Initially considered closure during the COVID-19 pandemic but transitioned to hybrid delivery with KHDA's support.
- University of Modern Sciences: Closed in 2018 due to non-compliance; students were offered transfers or transcripts through KHDA.
- University of Jazeera: Licensing issues led to suspension; students were supported in transitioning to accredited institutions.

Private School Closures

In the K-12 sector, several private schools have closed due to:

- Financial insolvency
- Consistent low ratings by KHDA/ADEK
- Enrollment drops

These closures are regulated, with parents and students notified in advance and alternate schooling options facilitated.

Regulatory Process for Closures

Closure of higher education institutions requires:

- Formal Approval: From CAA, KHDA, ADEK, or MOE
- Probationary Period: Institutions usually placed under review before closure
- Student Transition Support: Mandatory plans to transfer students, safeguard transcripts, and ensure continuity
- Public Announcements: Issued in advance to minimize academic disruption.

5.3 Summary of Quality Assurance and Institutional Closures

Aspect	*Description*
Quality Assurance	CAA licensure, KPIs, certified reviews, global QA affiliations
Emirate Oversight	KHDA (Dubai), ADEK (Abu Dhabi), SPEA (Sharjah)
Closure Reasons	Low enrollment, non-compliance, financial constraints
Student Safeguards	Transfer support, transcript access, structured closure procedures
Total Closures (2015-25)	6 major institutions, with formal oversight and student transition mechanisms

The UAE's quality assurance framework combines stringent accreditation processes, international alignment, and proactive institutional oversight. While a few institutions have closed in the past decade, these actions were taken transparently and with clear safeguards for student welfare. Through outcome-based regulation and rigorous enforcement, the UAE continues to build a reputation as a credible and globally recognized higher education hub.

TO SUM UP

The UAE has successfully positioned itself as a pioneer in transnational higher education through dynamic regulatory reforms, strategic partnerships, and targeted investment in academic infrastructure. Its supportive policies for foreign institutions and commitment to quality assurance continue to attract world-class universities and students from across the globe, reinforcing the nation's status as an emerging educational powerhouse in the Middle East and beyond.

UAE has established a dynamic, performance-linked quality assurance ecosystem in higher education, rooted in both federal and emirate-level oversight. While tuition is market-driven, transparent fee regulations and service disclosures are mandated. The quality assurance framework emphasizes global benchmarking, outcome-based assessments, and continuous improvement.

Although a handful of institutions have closed over the past decade due to compliance or financial challenges, the UAE's proactive regulatory approach-through CAA, KHDA, ADEK, and SPEA-ensures that closures are managed with transparency and minimal disruption to students. These strategies support the nation's aspiration to become a leading education and innovation hub in the region.

REFERENCES

(Ministry of Education, UAE; Commission for Academic Accreditation; KHDA Annual Reports; ADEK and SPEA Regulatory Bulletins; INQAAHE and ANQAHE documentation.)

FOREIGN UNIVERSITIES' PRESENCE IN INDIA- POLICY AND PRACTICE

Dr. G.D. Sharma *

The Government of India has been encouraging foreign universities to set up campuses in India with an avowed objective of providing world-class education to Indian students in India, making India a hub of international higher education. This paper deals with the policy and practice of setting up of foreign university campus in India and steps taken to internationalize higher education through collaborative arrangements.

ABSTRACT

As a step towards the implementation of NEP-2020, in particular the internationalization of higher education, India developed two sets of policy frameworks for setting up a foreign university campus in India. One is by the Ministry of Finance through an Act passed in 2019 and notified in 2020 for setting up a foreign university campus in a special economic the GIFT city. The other was by the University Grants Commission through notifying regulations for the setting up of foreign universities in India. These frameworks, while enabling foreign universities' campuses, differ significantly with regard to autonomy for institutions. Yet these frameworks have enabled foreign universities to set up campuses or apply to set up campuses in India. The other form of internationalization of higher education in India is encouraging Indian and Foreign Universities' academic collaboration through notifying regulations for such collaboration. The latter form of internationalization seems to have progressed more than the former form.

Initially, two countries, namely the USA and the UK, attracted students for studies on their campuses. Around the mid-1990s and a new concept of recruitment of students for studies on their campus started. Australia was one of the countries that attracted and recruited Indian students.

INTRODUCTION

Internationalization of higher education in India before the mid-1990s was mainly students going to other countries and coming to India for studies, and faculty exchanges. In the mid-1990s, particularly after the concept of liberalization gained ground in India, many foreign education providers started approaching India to set up arrangements in India. Many Indian institutes wanted to set up foreign university programmes in India.

On the global scenario, after the signing of the General Agreement on Trade in Services (GATS) under the World Trade Organization (WTO) framework, many countries signed and became its members. India is also one of the signatories and members of the WTO. Among the 19 services, education is one of the services slated for a multilateral trade agreement. This gave legitimacy to the liberalization of education services.

Initially, two countries, namely the USA and the UK, attracted students for studies on their campuses. Around the mid-1990s and a new concept of recruitment of students for studies on their campus started. Australia was one of the countries that attracted and recruited Indian students. There was somewhat covert recruitment of students in professional courses by China, Russia and Ukraine, and several other countries. The migration of students in these countries was due to the non-availability of seats in India in medical and professional courses and relatively availability of seats in these countries with less cost and competition.

Some students from neighbouring countries also came to India for studies.. But the numbers were small, and a good number of them came under the Indian Technical Programme. Some of the Indian universities also started marketing for the recruitment of foreign students in India.

But there was no foreign university campus in India. Some of the Indian institutions/ education providers have tied up with foreign universities to set up and operate their programmes in India. A couple of such programmes were running in India during the late 1990s and early 2000s. However, these were out of the purview of the Regulatory and Recognition framework in India-mainly done by the University Grants Commission and Ministry of Human Resource Development, now the Ministry of Education, Government of India. Some attempt was made to develop a framework in the form of the Promotion of Indian Universities Abroad and Regulation of Foreign Universities in India. But it remained as a report at the Committee level. However, the committee laid down some norms for allowing foreign universities in India and Indian Universities going abroad. Among the norms for foreign universities coming to India were the Universities Listed at 100 /200 by Times Higher Education or QS ranking. But no campus was set by foreign universities adhering to this norm.

THE POLICY:

The UGC Initiative:

After the National Education, 2020, under internationalization of Higher Education, the UGC also attempted to write letters to more than two dozen universities and encouraging them to set up campuses in India. The UGC also issued guidelines in the year 2021 on the internationalization of higher education. Finally UGC formulated and issued regulations for setting up foreign Universities in India taking support of various

** Former: Professor NIEPA, Secretary, UGC, Director CEC and President SEED* provisions of University Grants Commission Act, 1956 - (which is basically for the universities set up under the three provisions, namely Act of Parliament, Act of Legislation and the Section 3 of UGC allowing research and special subject institutions to act as deemed to be universities).

The UGC issued regulations under its powers conferred by the Act under various sections. In particular, Clause (J) of section 12 read with clauses (f) and (g) of Sub-section (I) of Section 26 of the UGC Act, 1956. These regulations were called as UGC regulations for setting up and operation of foreign Campuses of Foreign Higher Educational Institutions in India, 2023. Some key features of the regulations may be discussed here.

Eligibility: A Foreign University should figure in the overall ranking within the top 500 of global rankings at the time of applying for the setting up campus and should have outstanding expertise in a particular area. The decision-making power was left to the Commission. This is coming down from earlier norms laid down by the committee, i.e., among the top 100 ranked universities by two important ranking bodies, namely, THE and QS rankings. Regulations are silent on rankings by which ranking bodies. The regulations are also further relaxed the norms by allowing Universities to top the 500 Universities ranking in the subject-wise categories of global rankings.

Quality and Recognition: The regulations provide that a foreign university applying for setting up a campus should give an undertaking that the "quality of education imparted by it in the Indian Campus is similar to that of the main campus in the country of origin." The regulation also specifies that "the qualifications awarded to the students in the Indian Campus shall enjoy the same recognition as status as if they were conducted in the its home jurisdiction, that is, they shall be recognized in the country of origin of the foreign Higher Education and shall be equivalent to the corresponding qualifications awarded by the Foreign Higher Educational Institution in the main campus located in the country of origin." It also requires the foreign university to submit the latest accreditation or Quality Assurance report from a recognised body.

Fees and Finances: Regulations provide that "the Foreign Higher Education Institutions shall decide the fee structure, which shall be transparent and reasonable." About the financial status of foreign higher education institutions, it says, "The Foreign Higher Education Institutions shall present their adequacy and other resources required to establish and operate their campus in India. The regulations also provide that cross-border movements of Funds and maintenance of Foreign Currency Accounts, mode of Payments, remittance, repatriation, and sale proceeds shall be by provisions of the Foreign Exchange Management Act, 1999 (42 of 1999) and the rules and regulations thereunder." These provisions also apply to the receipt and utilization of foreign contributions and donations.

Safeguards: Under safeguards, regulations provide for standard safeguards in the event of discontinuation of the programme or closure of the campus, such as relocation of students and prior approval of the commission.

Power to permit and close the Operations: The power to permit rests with UGC, which will be exercised through a standing committee set up by the Commission. As far as closure is concerned, the regulations specify four conditions, namely, a foreign University, (a) fail to adhere to or has violated the provisions of regulations, (b)activities or academic programme against the interest of India, (c) engage in operations other than permitted under the regulations.

Dispute Settlement: For dispute settlement, legal jurisdiction if Indian Courts, and dispute settlement on account of interpretation of provisions and regulations final decision will rest with the Central Government.

These are some key features of the regulations for setting up and operating Foreign Higher Education Institutes in India.

SOME OBSERVATIONS:

The regulations leave a scope of interpretation of eligibility in terms of all global rankings and subject rankings. It has also come down to a 500 band, which does inspire confidence in quality among the students and faculty.

It lacks clarity about the method of ensuring the same quality of education as that of the main campus is provided by the campus in India. It has made no provision for assessment and accreditation by a quality assurance agency in India or global agencies.

As per provisions in the regulation, the decision of closure and cancellation rests with the Central Government. It does not clarify the process to be followed in case of cancellation or closures.

The power to frame regulations for foreign universities under the UGC Act 1956 is a matter of challenge and debate. Although the regulations are issued by the Government of India under the provisions of the Gazette Notification, yet overarching framework does not seem to support it.

THE MINISTRY OF FINANCE INITIATIVE:

Policy of Special Economic Fintech Zone :

Besides approval by UGC, there is a special economic zone concept being used for the setting up of a foreign university campus in India. Gujarat International Finance and Tech City (Gift City) is a location for setting up of foreign university campus. The Government of India passed an Act in 2019 to set up a special financial tech zone. The act is titled as "The International Financial Services Centres Authority Act, 2019. " The act was passed by the Indian Parliament and notified on December 19, 2019. (IFCA) The Act came into force: April 27, 2020. This is the first unified financial regulator in India:

" Combining powers traditionally held by the RBI, SEBI, IRDAI, and PFRDA for IFSC zones only

" Currently operates mainly in GIFT City, Gujarat, which is the only notified IFSC in India.

CONTEXT AND BACKGROUND:

Union Budget 2022-23 Announcement:

On February 1, 2022, the Finance Minister announced the proposal to allow world-class foreign universities to establish campuses in GIFT City, free from domestic regulations, to enhance the availability of skilled human capital for financial services and technology.

OBJECTIVE:

The initiative aims to position GIFT City as a global financial and educational hub, attracting foreign capital and talent while offering a regulatory environment comparable to international financial centers like London and Singapore.

Exemptions from Domestic Regulations:

Unlike foreign universities elsewhere in India, those in GIFT City are not subject to domestic regulations such as the UGC (Promotion and Maintenance of Standards of Academic Collaboration) Regulations, 2016, or AICTE Regulations for Entry and Operation of Foreign Universities, 2005. This light-touch regulatory framework is designed to ease operations and promote liberalization

Legal Framework Adjustments:

Amendments to the IFSCA Act may be required to grant the IFSCA regulatory authority over educational institutions and to formalize exemptions from domestic regulations

Tax Incentives:

Special tax incentives may apply to entities in the GIFT IFSC, potentially boosting enrollment and operations for foreign universities.

Strategic Support:

Firms like Grant Thornton offer consultancy services to help foreign universities develop entry strategies for GIFT City, ensuring compliance and optimizing growth opportunities

Global Appeal:

The regulations aim to attract students from South Asian countries, positioning GIFT City as a regional education hub.

The International Financial Services Centres Authority Act, 2019 (IFCA):

IFSCA is a statutory, autonomous body. It is independent in decision-making. Reports to the Ministry of Finance, but does not operate under RBI, SEBI, or any single regulator. IFCA has its funding mechanisms via fees, charges, and grants from the government.

IFCA Regulatory Framework for setting up a foreign University Campus in Gift City:

The International Financial Services Centres Authority (IFSCA) has established a regulatory framework to facilitate the establishment of foreign universities in Gujarat International Finance Tec-City (GIFT City). Below is an overview of the key guidelines, regulations, and framework issued by the IFSCA for granting permission to universities in GIFT City.

It is titled "International Financial Services Centres Authority (Setting up and Operation of International Branch Campuses and Offshore Education Centres) Regulations, 2022 (IBC-OEC Regulations)". It was notified on October 11, 2022.

Some of the key features of the regulation may be mentioned here.

Purpose: These regulations permit foreign universities and educational institutions to set up International Branch Campuses (IBCs) or Offshore Education Centres (OECs) in GIFT City, Gandhinagar, Gujarat.

Eligibility:

(1) Foreign universities or institutions ranked among the top 500 in the QS World University Rankings or equivalent are eligible to apply.

(2) They must provide an undertaking to establish suitable infrastructure and facilities to offer courses in fields such as financial management, FinTech, science, technology, engineering, and mathematics (STEM)

Course Requirements:

(1) Programs offered must be identical to those provided by the parent entity in its home jurisdiction.

(2) Degrees, diplomas, or certificates conferred must carry the same recognition and status as those issued by the parent entity in its home jurisdiction.

Autonomy:

(1) Foreign universities in GIFT City are exempt from domestic regulatory oversight by bodies such as the University Grants Commission (UGC), All India Council for Technical Education (AICTE), Higher Education Commission of India, National Assessment and Accreditation Council, and National Board of Accreditation. Only IFSCA guidelines apply.

(2) They have autonomy in admissions, entry-level qualifications, examination patterns, fee structures, curriculum, and accreditation requirements.

Profit Repatriation:

(1) Foreign universities are allowed to repatriate profits without restrictions, aligning with the Foreign Direct Investment (FDI) Policy and the Foreign Exchange Management Act, 1999.

(2) Restrictions under the Liberalised Remittance Scheme (LRS) for domestic students paying fees in

foreign currency may require review to enable smooth operations.

Inspection and Compliance:

(1) The IFSCA retains the right to inspect foreign campuses in GIFT City to ensure compliance with its regulations.

(2) If a program is discontinued, the institution must provide alternatives, such as reallocation, for affected students.

Operational Structure:

Universities may establish standalone campuses or enter collaborative arrangements (e.g., joint ventures) with Indian partners, with the IFSCA framework outlining defined structures for such arrangements.

Application Process:

(1) Entities must engage with the IFSCA's Development Team (via email: development@ifsca.gov.in) for information on opportunities and the process for setting up operations in GIFT City.

(2) A Common Application Form (CAF) with vertical-specific annexures is required for most entities, including foreign universities, except for specific categories like Market Infrastructure Institutions

(3) Approval from the Special Economic Zone (SEZ) authorities is also necessary, involving an application to the Development Commissioner, GIFT SEZ, followed by IFSCA approval.

SOME OBSERVATIONS:

(1) These two policy frameworks of approval and operation of foreign university campuses in India put one set of universities set up in GIFT City under the IFCA framework at a considerable advantage in terms of recognition, autonomy, and financial operations. Tax incentives. This might, over time, may raise the issue of discrimination. This issue could further be extended to discrimination in treatment of Indian and foreign universities.

(2) The IFCA framework is silent about recognition of degrees awarded by foreign universities in India and elsewhere, especially as there is no mention of the process of equivalence of degrees in the Indian or UNESCO-advised framework.

(3) It also does not specify a process to ensure quality of education in Indian Campuses as that of in main campus of the foreign university.

(4) It also mentions system assessment and accreditation nationally or globally.

(5) NEP 2020 also specifies that education institutions should be set up under the provision of "not for profit." In India all education institutes have to set up under the provisions of not for profit. This provision will conflict with foreign universities areset up "for profit."

The Practice:

Under its provisions, IFCA has given permission/license to foreign universities to set up a campus in Gift City. Under the provision of IFCA five universities namely, Deakin University (Australia), University of Wollongong (Australia) and University Queen's University Belfast (United Kingdom), University of Surrey (United Kingdom), Coventry University (United Kingdom), Newcastle University (United Kingdom) have been given approval/ licence to set up campus and operate in GIFT city. These are out of the purview of the University Grants Commission Regulation, 2023.

Besides, the Gift City, another foreign university education hub, appears to be emerging in the Education City of Navi Mumbai or Mumbai. Letter of intents have been given to: (1)Victoria University (Australia), Mumbai or Navi Mumbai, (2) Illinois Institute of Technology (United States), Mumbai or Navi Mumbai, (3) IstitutoEuropeo di Design (Italy), Mumbai or Navi Mumbai, (4) University of York (United Kingdom), Mumbai or Navi Mumbai, (5) University of Aberdeen (United Kingdom), Mumbai. The letters of intent were given to them in June 2025. These universities will operate under the provisions of the Regulations of the University Grants Commission.

Besides these two foreign universities hub the following foreign universities have received approval and are operating or are likely to operate in the near future. There are: University of Southampton (United Kingdom), Gurugram, Haryana, University of Liverpool (United Kingdom), Bengaluru, Karnataka, Western Sydney University (Australia), Greater Noida, Uttar Pradesh, University of Western Australia (Australia), Tamil Nadu, and Maharashtra. The Lincoln University College (Malaysia),Telangana, applied to UGC.

THE STATUS OF FOREIGN UNIVERSITIES IN INDIA:

IFSCA Framework:

Deakin University (Australia) Gift City Campus, Gujarat:

The Background: "Deakin University is a public university known for its strong focus on innovation, digital learning, and industry aligned education. It consistently ranks among Australia's top universities for student satisfaction and graduate employability." **Status:** The first foreign university to establish a campus in India. It has been operational since 2024. University is offering:Master of Financial Technology, Master of Financial Technology (Extension), Graduate Certificate in Financial Technology, Cyber security, and Business Analytics. **Ranking:** It has consistently improved its QS ranking. It was at 266 in 2023 and improved to 233 in 2024, and 192 in 2025. **Fee Structure:** Fees for two-year programmes are Rs. 21.4 lakhs, total tuition cost, and Rs. 2.5 Lakhs approximate living cost per annum. The present intake capacity is 50-60 students initially and will increase to 100.

University of Wollongong (Australia), GIFT City, Gujarat

The Background: It was established as an independent institution in 1975. Its origins date back to 1951 as a division of the NSW University of Technology. Located in

Wollongong, New South Wales. It has grown into a globally respected institution with a strong regional presence and international footprint, including campuses in Dubai, Malaysia, India, Hong Kong, and Singapore.

Status: The University officially received its license in May 2023, following a meeting between UOW's Vice-Chancellor and Prime Minister Modi, and the campus was inaugurated in November 2024.

The University has been operational since November 2024. This is the second foreign university to open a campus in India. The university has started admissions for its July 2025 session.

It offers programmes in: Finance, STEM (Science, Technology, Engineering, Mathematics).

First classes started in November 2024, with the first cohorts currently studying the Master's in FinTech/Data Analytics and Graduate Certificates.

These programs typically run for 12-18 months, so the first Master's degrees are expected to be officially awarded in mid-to-late 2026, assuming on-time completion.

Ranking: The University has improved its ranking over the last three years in the QS ranking. It was 167 in 2023 and improved to 162 in 2024, but slightly declined to 167 in 2025. In the THE Ranking, it has consistently remained in the band of 201-2050. It ranks 11 in Australia. Its fee structure is:

Program	Approx. Fee (INR)	Scholarships Available
Graduate Certificate (6 months)nts	8-9 lakh	25% first trimester in Augural waiver
Master's (Data Analytics / FinTech)	8-9 lakh total	50% first trimester Inaugural; 50% full duration for Women Leaders; Early Bird/Merit

Queen's University Belfast (United Kingdom). GIFT City, Gujarat

The Background: Queen's University Belfast (QUB) was established in 1845 as one of three Queen's Colleges in Ireland to provide higher education to Irish students of all backgrounds. It opened officially in 1849 with 23 professors and 195 students. The university gained independence from the Queen's Colleges system and became The Queen's University of Belfast in 1908. It has since grown into a prestigious Russell Group institution, known for research excellence, innovation, and global engagement.

Status: This is Queen's first international campus outside the UK. The new campus at Gift City will begin operations in January 2026, offering postgraduate programmes in finance, technology, business analytics, and more.
It offers postgraduate master's programs in:

" MSc Finance,MSc Financial Analytics

" MSc Business Analytics,MSc Construction and Project Management.Level: Postgraduate (Master's level, Level 7) . Duration: Typically 1 year full-time (may vary)

These programs are designed to equip students with advanced skills in finance, analytics, project management, and related areas tailored to the needs of the Indian and global markets.

Ranking: The University has improved its ranking in the QS Ranking over the last three years. In 2023, it ranked 233 and improved to 202 but declined slightly in 2025 to 206. In THE ranking, it was 198 in 2023 but slightly declined to 201 in 2024.

Fee Structure: Standard tuition fee: £15,000 (Using £1 = Rs.115.55 exchange rate) per year (for MSc Finance, Financial Analytics, Business Analytics, and Construction & Project Management). Scholarship offer: A £2,000 discount for the 2026 intake, reducing the fee to £13,000. In Indian rupees, it works out to approximately Rs. 15.00 Lakhs.

These are three universities, which have started operations in Gift City, Gujarat, under the approval/ license by IFCA.

The remaining two universities, namely,the University of Surrey (United Kingdom), Coventry University (United Kingdom, and Newcastle University (United Kingdom) in Gift City have yet to start their campus. Their status is as under:

University of Surrey (United Kingdom), GIFT City, Gujarat

Status: Planned for launch between 2026 and 2027. **Program Offerings:** Artificial Intelligence, Finance, Cybersecurity. **Ranking:** QS 262 (2026) THE 201-250 (2025)

Coventry University (United Kingdom), GIFT City, Gujarat

Status: Planning to establish a campus, expected by 2026-2027. **Program Offerings:** Not specified. **Ranking:** QS 526 (2025) in the band of 531-550, THE in the band of 601-800 (2025).

The status of UGC Approved Foreign Universities :

Universities that are given approval by UGC and proposing to set up campuses in Mumbai/Navi Mumbai in Maharashtra have yet to set up their campuses. Their status is as under:

Victoria University (Australia) expected in Mumbai or Navi Mumbai)

Status: Received LoI in 2025, with campus expected to open between 2026 and 2027. **Program Offerings:** Business, IT, and Hospitality, with a focus on flexible learning models. **Ranking:** Ranked 741-750 in QS World University Rankings 2025. Known for practical, hands-on education.

Illinois Institute of Technology (United States). Mumbai or Navi Mumbai, Maharashtra

The first American university to establish a campus in India, **Status:** Received LoI in 2025, with campus expected to open between 2026 and 2027. **Program Offerings:** Engineering, Science, and Technology. **Ranking:** 601-610 in QS World University Rankings 2025.

IstitutoEuropeo di Design (Italy). Mumbai or Navi Mumbai, Maharashtra

Status: Received LoI in 2025, with campus expected to open between 2026 and 2027. **Programs Offering:** Fashion, Visual Arts, and Communication. **Ranking:** Ranked among the top 200 globally in Art & Design, focusing on creativity.

University of York (United Kingdom), Mumbai or Navi Mumbai, Maharashtra

Status: Received LoI in 2025, with admissions expected by December 2026. **Programs Offering:** Not specified, but likely to include STEM and management courses. **Ranking:**169 QS (2026), THE 146 (2025).

University of Aberdeen (United Kingdom): Mumbai, Maharashtra

Status: Received LoI in 2025, with operations expected by 2026-2027. **Program Offerings:** likely to focus on research-intensive programs. The first Scottish university to establish a branch campus in India. **Ranking:** Placed within the 201-250 band internationally

STATUS OF UNIVERSITIES IN GURGAON, HARYANA, NOIDA, UP, BENGALURU, KARNATAKA, TELANGANA, AND TAMIL NADU IS AS UNDER:

University of Southampton (United Kingdom):

Gurugram, Haryana. The first UK University to establish a full-fledged campus in India. **Status:** Received Letter of Intent (LoI) in 2023, with operations expected to commence in August 2025. Teaching will begin in September 2025. **Programs Offering**: Undergraduate programs in Accounting and Finance, Economics, Computer Science, Business Management, and postgraduate courses in International Management and Finance. It is aiming to enrol 5,000-5,500 students over the first 10 years, starting with 150-200. **Ranking:** QS 87 (2026), THE 115 (2025) -Global ranking.

Western Sydney University (Australia), Greater Noida, Uttar Pradesh

Status: Received LoI in 2025, with campus expected to open between 2026 and 2027. **Programs Offering:** Technology and research-focused programs. **Ranking:** 384th globally in QS 2025, with a strong emphasis on technology and research

University of Liverpool (United Kingdom) Bengaluru, Karnataka

Status: Received LoI from UGC in 2025, with operations planned for August 2026. **Programs Offering:** Undergraduate and postgraduate programs in Business Management, Accounting and Finance, Computer Science, Biomedical Sciences, and a unique Game Design course. The fourth foreign university to publicly announce its presence in India, focusing on research-driven education in STEM and Biomedical Sciences, **Ranking:** QS 165 (2025), it improved to 147 in 2026 and moved to the top 150 universities.

Lincoln University College (Malaysia), Telangana

Status: Applied to UGC for approval, under review by a five-member committee. **Program Offerings:** Not specified. Awaiting formal approval to establish a campus. **Ranking:** QS Asia 185

University of Western Australia (Australia), Tamil Nadu, and Maharashtra

Awaiting formal approval, with plans to expand in multiple states. **Status:** Signaled intention to open campuses, with operations expected by 2026-2027. **Programs Offering:** likely to include STEM and management. **Ranking:** 77 QS (2025) THE 149 (2025)

SOME OBSERVATIONS:

Most of the foreign universities that have received approval have yet to set up their campuses and start operations. Some of them may start their operations, if all goes well, by the academic session of 2026-27or even beyond that time.

Some of the universities both in Gift City and approved by UGC rank above the mark of 500 in the global ranking.

Most of the universities are focusing on STEM programmes and very selective courses. None seems to be interested in general science or social science courses.

Whether existing and proposed foreign university campuses will have any impact on an increase in enrolment of Indian students, or inviting foreign students to these campuses, is yet a remote possibility.

Impact on making Indian universities learn from them may be partial and limited to a few new areas of studies, like Fintech, Management, and so on. One cannot expect much impact given the participation of small numbers of Universities and only a few are among top 200.These are some of the avowed objectives for inviting foreign universities to set up their campuses in India. Whether the present status of the presence of foreign universities will help achieve these objectives Is a matter for further study.

FOREIGN AND INDIAN UNIVERSITIES COLLABORATION:

Another form of the presence of foreign universities in India is through the internationalization of higher education as proposed in NEP 2020. Following the provisions of the NEP 2020 the UGC issued Regulations titled "UGC

(Academic Collaboration between Indian and Foreign Higher Educational Institutions to offer Twinning, Joint Degree and Dual Degree Programmes) Regulations, 2021. The objectives and key features of regulations are highlighted here.

The Objectives and Key Features:

The Objectives are to : (a) promote internationalization of higher education in India, (b) enhance global exposure for students, and (c) foster academic excellence through collaboration with reputed foreign institutions.

The Regulations provide for: Twining, Joint and Dual Degree programmes in collaboration with foreign universities. The Key features are :

Twinning Programme: (a) Students complete part of their programme at an Indian HEI and the remaining part at a foreign HEI. (b) The degree is awarded by the Indian HEI, with a certificate indicating credits earned at the foreign institution. (c)Students must complete up to 30% of the programme's credits at the foreign HEI.

Joint Degree Programme: (a) The curriculum is jointly designed by the Indian and foreign HEIs. (b) Students complete parts of the programme at both institutions, and a single degree is awarded jointly by both, with a common certificate bearing the logos of both institutions.

Dual Degree Programme: (a) Degrees are awarded separately by both the Indian and foreign HEIs upon completion of the programme. (b) The curriculum may be designed collaboratively, and students complete requirements for both degrees simultaneously, with separate degree certificates issued by each institution.

Eligibility Criteria:

Indian HEIs: (a) must be accredited by the National Assessment and Accreditation Council (NAAC) with a minimum grade of 3.01 on a 4-point scale or be ranked among the top 100 in the university category of the National Institutional Ranking Framework (NIRF). (b)Alternatively, the Indian HEI must be among the top 1,000 in QS World University Rankings or Times Higher Education (THE) Rankings. (c) Institutions of Eminence (IoE) are automatically eligible.

Foreign HEIs: Must be accredited in their home country or ranked among the top 500 in QS World University Rankings or Times Higher Education Rankings.

Procedure: Both institutions must sign a Memorandum of Understanding (MoU) or agreement to outline the collaboration terms. A detailed MoU or agreement outlining the collaboration terms must be submitted to the UGC for scrutiny.

Programme Structure and Credit Recognition

Credit Transfer: (a) For twinning programmes, credits earned at the foreign HEI are recognized by the Indian HEI for degree conferment, subject to fulfilling academic requirements. (b) At least 50% of the total credits must be earned at the Indian HEI for twinning and joint degree programmes.

Curriculum Design:Joint and dual degree programmes require collaborative curriculum development, ensuring alignment with the standards of both institutions.

Duration: The duration of the programme must comply with the academic requirements specified by the UGC and the collaborating institutions.

Admission and Fee Structure:

Admissions: (a) Indian HEIs are responsible for admissions, following their standard eligibility criteria. (b) Foreign HEIs must adhere to the admission criteria agreed upon in the MoU.

Fees: (a) Indian HEIs can charge fees as per their norms for the portion of the programme conducted in India. (b) Fees for the foreign component are determined by the foreign HEI, and transparency in the fee structure is mandatory.

Degree Recognition: (a) Degrees awarded under these collaborations are equivalent to those awarded by the Indian HEI for similar programmes. (b) Joint degrees are issued with a single certificate bearing the logos of both institutions.(c) Dual degrees result in two separate certificates, one from each institution. (d) Degrees must comply with the nomenclature and standards prescribed by the UGC or other Indian regulatory bodies.

Regulatory Compliance and Approval: (a) No Automatic Approval: (b) Indian HEIs must obtain approval from the UGC for offering joint or dual degree programmes.(c) Twinning programmes require the Indian HEI to inform the UGC but do not need explicit approval, provided the collaboration meets eligibility criteria.

Quality Assurance: Both institutions must ensure compliance with their respective accreditation and quality assurance mechanisms. The UGC may inspect the collaboration to ensure adherence to regulations.

Faculty and Infrastructure: (a) Faculty exchange and collaboration are encouraged to enhance the quality of education. (b) Both institutions must ensure adequate infrastructure, including physical and digital resources, to support the collaborative programmes. (c) Faculty from both HEIs may jointly teach courses, as agreed in the MoU.

Student Mobility and Support:(a) Students participating in twinning or joint degree programmes must spend a specified duration (as per the MoU) at the foreign HEI.(b) Indian HEIs are responsible for facilitating student mobility, including visa support and credit transfer processes. (c) Provisions must be made to ensure students complete the programme even if the collaboration is terminated.

Exclusions :(a) These regulations do not apply to programmes offered through open and distance learning (ODL) or online modes. (b) Collaborations for research, faculty exchange, or non-degree programmes are not covered under these regulations but may be governed by separate agreements.

These are detailed guidelines that seem to have helped the Indian universities to launch the collaboration with foreign universities.

GROWTH IN FOREIGN AND INDIA UNIVERSITIES COLLABORATIONS:

There is phenomenal growth in collaboration with foreign universities. It is reported that there are 400 such collaborations with Indian Universities. In every advertisement of private universities, one could notice the collaboration ofan Indian university with 5-6 countries and 8-10 foreign universities. A random analysis of 9 universities in Gurugram, Haryana, mostly private ones, showed that every university has a collaboration with foreign universities located in various countries. It ranges Universities / Institutes from 5 to 22 countries and 8-41 programmes.

Universities of the USA, UK, Australia, Canada, and France figure in collaboration with most of the Universities located in Gurugram. But the spread is so wide that include Universities from China, Russia, South Korea, Germany, Israel, Brazil, Malaysia, Indonesia, Turkey, Sweden, Switzerland, Spain, Netherlands, Morocco, Taiwan, Vietnam, and so on. Please see figure 1 and 2. `In our view it is more than the presence of foreign university campuses in India, given the present status, one can expect an impact of foreign universities on the academic activities of Indian Universities under these collaboration.

THE NEED OF THE STUDY:

To find out the impact, there a need to study: how these collaborations are working? How are the curricula and processes of teaching, learning, and evaluating students impacted? What is the impact on the quality of Indian Institutions? How many collaboration are for twining, joint, and dual degree programmes? What are their thrust areas? How faculty exchanges are influencing the quality of teaching and research. Is there a two-way interaction, or is it one-way learning only? A study analysing these aspects will help us to know the impact and churn that might be causing in the landscape of Indian higher education and vice versa.

Figure 1. No. of Foreign University Collaboration by Country, Universities in Gurugram

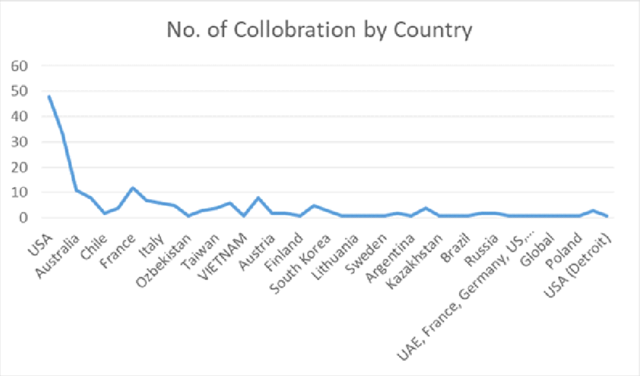
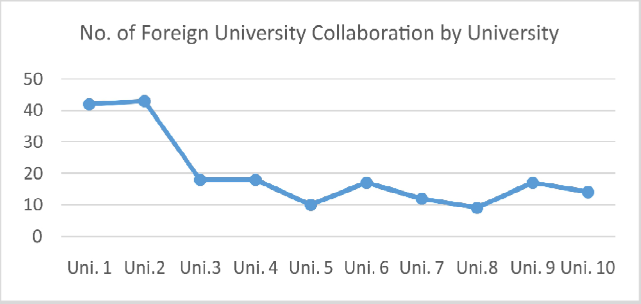


Figure 2. No. of Foreign University Collaboration by Universities in Gurugram



TO SUM UP:

- ¢ Two policy frameworks are working for setting up of foreign university campus in India. Those working under IFSCA framework in Gift City have greater academic, financial and administrative autonomy as compared to those foreign universities approved under the UGC framework. These two policy frameworks might in course of time raise issue of discrimination in treatment of foreign universities. There is a possibility of extension of the issue of discrimination in treatment between foreign and Indian Universities. The issue, therefore, needs to be resolved in the larger interest of students and institutions of higher education.
- ¢ Most of the foreign universities are located in Gift City and proposed to be located in Mumbai or Navy Mumbai's education city.
- ¢ A very few of approved university are in top 200 of QS or THE ranking. Some are even above the mark of 500 QS and THE ranking. Will that inspire confidence among foreign and Indian students seeking to study in foreign university campuses in India.
- ¢ Most of these approved universities have to yet to set up their campuses and start operations. It may not be earlier than couple of years.
- ¢ Collaboration of foreign universities with Indian Universities seems to have progressed well. It may be causing churn and impact on teaching-learning and evaluation process in Indian universities. There is a need of an intensive study of working and impact of these collaboration.
- ¢ More than the presence of foreign university campuses in India, foreign universities collaboration with Indian universities are likely to impact the academic activities of Indian Universities.

SOURCES:

1. University Grants Commission, GoI Regulations mentioned above
2. IFCA and Gift City -information obtained through websites and open AI
3. Foreign university information and data obtained through websites and OpenAI
4. Universities in Gurugram - data obtained through respective websites and Open AI
5. Those interested in knowing other views /aspects of foreign universities may refer to College Post - issues of Jan-March, and April-Sept., 2023.

This column brings out briefs of: Ph.D, M.Phil Researches in Education, Economics of Education, Social, Political, Psychology aspects of education/ economics conducted in University /College departments. It also brings out briefs on researches done by Research Institutions, Industry and NGOs. This column was introduced from April-June, 2016 issue of College Post. Method of reporting the researches completed and in progress was given in that issue. Interested researchers, professors and Heads of institute are requested to send their brief accordingly. Purpose of this column is to high light the researches in education conducted in university and college departments and in any other institution / industry and NGO for the benefit of policy makers, research scholars, thinkers. Readers are welcome to encourage relevant person and institute to send briefs on research done and being done in education/ economics.

This issue brings to you brief on following Researches in Education/Economics.

Ph.D. Thesis- Title: Student Activism, Social Media and Political Education in Indian Democracy, Researcher: Bhageshwari Sharma, Guide: Professor Pankaj Arora, Department: Department of Education, Central Institute of Education, University: University of Delhi, Year of Completion: 2021

Opening Quotation

"What is really needed to make democracy function is not knowledge of facts, but right education."
- Mahatma Gandhi

Objectives of the Study

1. To examine the extent of student engagement with various social media platforms.
2. To analyze students' interest in accessing and sharing socio-political content via social media.
3. To explore the role of social media in student activism and participation in political and social events.
4. To understand the drawbacks and risks associated with the use of social media in socio-political contexts.
5. To explore the interrelationship between students' engagement with social media, activism, and their political education.

Sample and Methodology

Sampling Method: Purposeful sampling
Participants:

- Undergraduate Students (150)
- University Teachers (15)
- Student Activists (15)

Disciplines: Political Science, Journalism, English, Mathematics, Economics, Commerce, and B.A. Programme

Institutions: Five colleges under the University of Delhi

Tools Used: Questionnaires, interviews, and focused group discussions

Key Findings

1. Student Engagement with Social Media

- Social media has become deeply integrated into students' daily routines.
- The primary motivation for internet use among students is to access social media platforms.
- Facebook, WhatsApp, Instagram, YouTube, and Twitter are the most widely used platforms, with Snapchat, TikTok, Google+, and LinkedIn also accessed.
- Smartphones are the dominant devices for social media access due to pre-installed apps and ease of use.
- Students use social media for networking, identity exploration, sharing content, and academic purposes.
- It is also used to follow societal developments, protests, and political news.
- Social media enables students to assert their views and act as "netizens," participating in civic discourse and awareness generation.

2. Students' Interest in Socio-Political Content

- Social media is saturated with political posts, memes, politoons, and campaign content.
- Both individuals and ideological groups use platforms to disseminate political information.
- Political parties leverage social media extensively for campaigning, mobilization, and propaganda.
- Students use it to learn about, express, and engage in socio-political issues, contributing to opinion-building and mobilization.
- However, digital inequality affects participation, limiting access for students without adequate internet connectivity or digital devices.

3. Role of Social Media in Student Activism

- Social media plays a pivotal role in mobilizing students and spreading awareness about protests and movements.
- It facilitates student participation in elections, strikes, and alliances, often forming new activist groups.
- Political parties specifically target students through digital strategies.
- Social media enables ideological exchange and visibility of causes, encouraging both collective and individual activism.
- Students are influenced and inspired by peers and public figures online, deepening engagement with socio-political issues.

4. The Flip Side of Social Media Usage

- Participants acknowledged that social media can be misused to distort realities, promote misinformation, and fuel hate.

- Threats, derogatory comments, and privacy violations are frequent among student activists.
- Sensationalist content can provoke hostility and encourage blind following without fact-checking.
- Respondents stressed the need for digital literacy, critical thinking, and responsible usage.
- Opinions were divided on content regulation-some advocated monitoring to prevent misuse, while others emphasized free speech and individual responsibility.

5. Link between Social Media, Student Activism, and Political Education

- Participants widely recognized social media as a tool that enhances political awareness and education.
- Political education via social media includes exposure to governmental structures, elections, political ideologies, and leaders.
- The multimedia nature of social platforms aids expression and comprehension.
- Discussions, debates, and divergent views on social media foster critical engagement and idea development.
- However, misinformation and the digital divide pose serious challenges to the effectiveness of political education through social media.

LIMITATIONS OF THE STUDY

- The study was limited to undergraduate students from only five colleges of the University of Delhi.
- Teachers involved had backgrounds in Political Science and Media only.
- Data was collected through self-reported methods such as questionnaires and interviews; observational and statistical methods were not employed.
- The study did not assess student participation in formal political events like student union elections through direct observation.

CONCLUDING REMARKS:

This thesis offers a nuanced understanding of how social media shapes student activism and political education within the democratic framework of India, highlighting both the empowering and problematic dimensions of digital engagement.

...contd. from page 1

Ultimately, the most important question is no longer about machine intelligence. It is whether we, as humans, can think ethically, deeply, and wisely enough to shape a future in which intelligent technologies serve humanity rather than replace it.

As an illustrative example, I asked an AI model what challenges Industry 5.0 poses for higher education. It responded, in seconds:

"The 5.0 Industrial Revolution brings profound challenges to higher education by demanding a shift toward more human-centric, sustainable, and technologically integrated learning environments. Institutions must rapidly adapt curricula to stay relevant in a world increasingly shaped by AI, robotics, and biotechnology, while also fostering essential human skills such as creativity, ethics, and emotional intelligence.

Higher education must also ensure equitable access to digital tools, align research with societal needs, and offer lifelong learning through modular programs and micro-credentials. International collaboration and ethical scrutiny are essential to navigating this complex future."

This rapid and articulate summary shows not only what is possible - but also what is at stake.

The 5.0 Industrial Revolution challenges educators, policy-makers, and institutions to act quickly, think critically, and lead ethically. It demands that we rethink how we prepare students - not simply to earn degrees, but to become thoughtful, resilient, and capable human beings in a world of intelligent machines.

As educators, we are tasked not only with adapting to change but with guiding it. That guidance must be grounded in shared human values - and in the unwavering belief that education, when done right, remains our greatest tool for building a just, informed, and humane future.

Book Review..contd. from page 32

"Future digital empires may repeat the history of colonialism-this time with data."

Harari's closing thought is both a warning and a call to action:

"Many things we consider natural and eternal are man-made and mutable… If we make the effort, we can create a better world. This isn't naivety-it's realism. Every old thing was once new. The only constant of history is change."

Nexus is a deep, nuanced exploration of how information-its creation, manipulation, and distribution-has shaped human history and may determine its future. Harari's storytelling is lucid and thought-provoking, moving seamlessly from mythology and history to digital futures. His warnings about the unchecked power of AI, misinformation, and decaying democratic institutions are timely and urgent.

This book is a must-read for anyone seeking to understand the past and future of information networks and their profound impact on human civilization.

By GD Sharma

THE MELTING POT BOILS - EMERGING CHALLENGES FOR INSTITUTIONS AND STUDENTS IN THE USA

In 1908, British-Jewish playwright and political thinker Israel Zangwill premiered his influential play The Melting Pot in Washington, D.C., presenting the idea of America as a place where diverse cultures blend into a unified whole. This metaphor became foundational in describing the cultural assimilation process central to America's identity as a land of opportunity, especially for immigrants. Over the decades, the United States became a beacon for scholars, researchers, and students from across the globe-many of whom contributed significantly to the country's academic and scientific prestige, including Nobel laureates of Indian origin.

Among the top institutions benefiting from this global influx was Harvard University, renowned for its commitment to excellence, diversity, and freedom of thought. However, recent policy shifts under the President Donald Trump have begun to challenge this long-standing tradition.

THE TRUMP ADMINISTRATION'S DISRUPTION OF ACADEMIA

Under Trump's leadership, a series of controversial actions were undertaken that many perceived as hostile to the foundational values of equity, inclusion, and academic freedom in U.S. universities. The administration issued sweeping guidelines aimed at reshaping the higher education landscape, focusing on free speech, ideological neutrality, and a crackdown on perceived anti-Semitism. These directives came with tangible threats: universities that failed to comply risked the withdrawal of federal funding. Immigration policies were also weaponized to control academic institutions' autonomy, especially concerning international students.

A flashpoint in this conflict was Harvard University. While some institutions complied under pressure, Harvard's leadership took a stand.

ACTIONS TAKEN AGAINST HARVARD UNIVERSITY

Between April and May 2025, the Trump administration implemented several punitive measures against Harvard:

- Federal Research Funding Frozen: Approximately $2.2-2.3 billion in federal research grants were suspended, citing alleged violations of civil rights and anti-Semitism.
- Cancellation of Federal Contracts: The General Services Administration ordered the cancellation of about $100 million worth of contracts with Harvard.
- Accreditation Reform: Trump advocated for changes in college accreditation procedures, urging accrediting bodies to scrutinize ideological bias, which he called his "secret weapon."
- Tax Exemption Threats: Trump suggested revoking Harvard's 501(c)(3) nonprofit status via posts on Truth Social.
- Visa Program Revoked: In May 2025, the Department of Homeland Security (DHS) revoked Harvard's certification under the Student and Exchange Visitor Program (SEVP), effectively blocking the university from enrolling foreign students.
- Visa Ban Proclamation: On June 4, a proclamation explicitly blocked the issuance of new F, M, and J visas for students bound for Harvard, and called for a review of existing visas.
- Increased Surveillance: A new mandate required the State Department to intensify social media screening for visa applicants, especially those affiliated with Harvard.

LEGAL BATTLE AND INSTITUTIONAL RESPONSE

In response, Harvard filed multiple lawsuits, invoking First Amendment protections, due process rights, and the Administrative Procedure Act. Federal Judge Allison Burroughs issued temporary restraining orders and preliminary injunctions, effectively keeping Harvard's international student programs operational-at least for the time being.

University President Alan Garber condemned the administration's measures as "illegal retaliatory steps" and reaffirmed Harvard's commitment to academic freedom and global inclusion. The university announced contingency plans to support affected international students and continue its research operations despite federal obstacles.

The final outcome awaits judicial ruling, but the case has already sent tremors through the global academic community, raising fundamental questions about the future of international education in the U.S.

The metaphor of the "melting pot" may still resonate, but it now simmers with complexity, uncertainty, and geopolitical tension. As institutions and students worldwide navigate this evolving terrain, the choices made today will shape the contours of global education for decades to come

****

JAPAN TURNS TO INDIA: A NEW AXIS OF ACADEMIC MOBILITY

While the U.S. landscape appears uncertain, Japan is actively repositioning itself to fill the gap, particularly by courting Indian students to meet its demographic and economic needs. A recent article in University World News by Suvendrini Kakuchi and Yojana Sharma (19 June 2025) highlighted Japan's efforts to internationalize its higher education system, with India playing a pivotal role.

In 2024, Japan's Integrated Innovation Strategy identified India as a priority partner. The Japanese government is now encouraging partnerships between leading universities in both countries and expanding India-specific initiatives.

COACHING INDUSTRY IN INDIA- A POLICY RESPONSE

Government Action on Coaching Industry

On 17th June 2025, the Ministry of Education, Government of India, constituted a nine-member committee chaired by Shri Vineet Joshi, Secretary, Higher Education, to examine critical issues emerging from the rapidly growing coaching industry, particularly those preparing students for competitive examinations.

The committee will examine:

1. The reasons for students' increasing dependence on coaching centers
2. The effectiveness and fairness of competitive entrance examinations
3. The impact of the coaching industry's growth on the education system

It will also assess the gaps in school education that push students toward private coaching-specifically the lack of emphasis on critical thinking, logical reasoning, analytical skills, and innovation, and the dominance of rote learning practices.

A Call for Broader Focus: Demand-Supply Mismatch In addition to the assigned areas, it is recommended that the committee also revisit the professional education as also issues highlighted in a 1995 ground-level study.

Demand-supply Mismatch

While student participation, aspirations, and pass rates have increased over the decades, the growth of institutions offering professional courses has not kept pace. This imbalance triggered a chain of developments:

- Institution-level entrance exams
- Group-based testing across institutions
- Centralized testing at state and eventually national levels

This led to the proliferation of coaching centers and the emergence of entire coaching towns. Unfortunately, it also brought serious side effects, including mental health pressures, student burnout, and suicides.

Recent controversies-such as allegations of question paper leaks and disproportionate selections from specific coaching hubs-further underscore the need for urgent systemic reforms.

Insights from the 1995 Ground-Level Study on the Coaching Industry

Commissioned by the Department of Science and Technology, the 1995 study conducted by the Society for Education and Economic Development (SEED) provided foundational insights into the coaching sector's development.

KEY FINDINGS:

1. Origins and Growth:

- Coaching for engineering and medical entrances began in 1956 (IIT Kharagpur) and 1962 (AIIMS Delhi).
- Expansion remained limited until the late 1980s and early 1990s, when competitive examinations multiplied.
- Coaching institutions evolved from small family-run ventures to professionally managed firms, adopting franchise models for rapid growth.

2. Operational Structure:

- Most coaching centers operate with bare minimum infrastructure, focused on high space utilization without facilities like libraries or student support services.

3. Student Demographics and Perceptions:

- Students largely came from professional, government, and education sector backgrounds.
- A majority attended coaching, particularly high-performing students seeking certainty in admissions.
- While 90% of engineering and 83% of medical students recommended coaching, only 30% (engineering) and 15% (medical) felt it helped them in their current academic studies.

" Concerns were raised over high costs, limited scope, and questionable long-term value.

4. Student Suggestions:

- Success was attributed more to self-study, discipline, and conceptual clarity than to coaching.
- Systemic suggestions included better teaching materials, improved faculty quality, and curriculum reforms to align school learning with competitive exams.

KEY RECOMMENDATIONS FROM THE STUDY:

1. Mandatory Registration of coaching centers under appropriate laws to prevent fraud and protect students.
2. Creation of a national accreditation system to ensure quality, possibly via academic bodies, ISI, or ISO.

CONCLUSION

The coaching industry is both a symptom and a driver of deeper issues in India's education system. Addressing it requires a multi-pronged approach-reforming school education, expanding professional education capacity, regulating coaching centers, and embracing innovative solutions like AI to improve learning. The committee's work, if informed by past research and present innovation, can pave the way for long-term, equitable reforms.

NEUROTECHNOLOGY IMPACTING EDUCATION AND LIFE

By Er. Rahul Agarwal

Advances in neurotechnology are ushering in a new era in understanding and enhancing brain health. These developments not only promise improvements in longevity but also in the overall quality of life. However, as with any powerful technology, they bring with them a host of ethical and privacy concerns-especially when it comes to monitoring brain activity. In response, organizations such as UNESCO and the United Nations are actively examining the implications of neurotechnology to ensure it is used responsibly. Yet, alongside these valid concerns lies immense potential. Let's explore what neurotechnology is and how it is shaping our lives, particularly in healthcare and education.

What is Neurotechnology?

Neurotechnology refers to a diverse array of tools and systems designed to monitor, analyze, and even influence brain function. This interdisciplinary field draws from neuroscience, computer science, engineering, and psychology to develop techniques for understanding and interacting with the brain and nervous system.

Neurotechnology in Healthcare

In medicine, neurotechnology is transforming diagnosis, treatment, and rehabilitation. Tools like EEG (Electroencephalography) and fMRI (functional Magnetic Resonance Imaging) are routinely used to assess brain activity and diagnose neurological conditions such as epilepsy, stroke, and mental health disorders.

Brain-computer interfaces (BCIs) are enabling individuals with paralysis to communicate or control devices using only their thoughts. Meanwhile, neuromodulation therapies-such as Deep Brain Stimulation (DBS) and Transcranial Magnetic Stimulation (TMS)-are being used to treat conditions like Parkinson's disease, depression, and chronic pain.

Neuroprosthetics, including cochlear implants and bionic limbs, are restoring sensory and motor functions for individuals with disabilities. Moreover, digital therapeutics and neurofeedback techniques are supporting the treatment of ADHD, PTSD, and other mental health conditions.

Despite these advances, the field still faces significant challenges in terms of privacy, accessibility, safety, and long-term efficacy.

Neurotechnology in Education

Beyond healthcare, neurotechnology is making inroads into education, learning, gaming, and entertainment. In classrooms and training environments, tools like EEG and fMRI are providing new ways to understand how students learn-and how to optimize the process.

1. **Immersive and Intuitive Learning-** EEG-enhanced Virtual Reality (VR) and Augmented Reality (AR) experiences are making learning more intuitive. By allowing users to interact with virtual environments using thought-based interfaces, these technologies foster deeper engagement and real-time responsiveness.

2. **Understanding Aptitude-** Researchers are exploring how brain structure and activity patterns correlate with an individual's aptitudes. Such insights could eventually support vocational guidance by offering objective assessments of a person's suitability for specific careers or training paths.

3. **Gamified Learning-** By incorporating insights from neuroscience on how the brain learns best, gamified learning makes education more engaging. Points, badges, leaderboards, and rewards can transform mundane lessons into dynamic, motivating experiences that encourage participation and sustained effort.

4. **Enhancing Cognitive Skills-** Techniques such as transcranial direct current stimulation (tDCS) and neurofeedback are being explored to enhance cognitive functions including memory, creativity, and problem-solving-skills critical for success in the 21st century.

5. **Bridging Educational Inequities-** Neurotechnology platforms are being developed to deliver personalized learning experiences, particularly in underserved or remote areas. These tools aim to reduce educational disparities by making quality learning resources accessible to all.

Ethical Considerations and Privacy Concerns

With the growing ability to monitor and manipulate brain activity comes an urgent need for ethical safeguards. As brain-wave data becomes increasingly accessible, concerns about surveillance, consent, and data misuse are intensifying.

Some governments have begun enacting legislation to classify neural data as highly sensitive, requiring stringent protections. The ethical debate continues around the boundaries of neuroenhancement, autonomy, and potential misuse.

CONCLUSION

Neurotechnology holds the promise of revolutionizing education by making it more personalized, immersive, and effective. It can empower students to overcome learning challenges, unlock hidden potential, and foster a culture of lifelong learning. As research progresses, neuroscience-driven education will likely become more adaptive and inclusive, shaping a future where every learner can thrive.

INFORMATION, PEOPLE AND POWER - A STORY NEXUS: A BRIEF HISTORY OF INFORMATION NETWORKS FROM THE STONE AGE TO AI, By Yuval Noah Harari, Fern Press - Penguin Random House, UK, 2024 | pp. 492

On the global knowledge scene, Yuval Noah Harari has emerged as a historian who sees the world in his own distinct and compelling way. An unconventional thinker, Harari is known for works like Sapiens, Homo Deus, and 21 Lessons for the 21st Century. His latest offering, Nexus, continues his tradition of probing grand questions with striking clarity, originality, and narrative power.

Organized into three parts, Nexus examines how human and non-human (inorganic) information networks shape societies, identities, and political systems. The first section, Human Networks, includes five chapters that explore foundational questions: What is Information?, Stories: Unlimited Connections, Documents: The Bite of the Paper Tiger, Error: The Fantasy of Infallibility, and Decisions: A Brief History of Democracy and Totalitarianism.

Harari's core argument, outlined in the prologue, is provocative and timely:

"Humankind gains enormous powers by building large networks of cooperation, but these networks predispose us to use that power unwisely. Our problem is, essentially, a network problem-and more specifically, an information problem."

He challenges conventional wisdom about power, asserting that it is not individual hubris but collective networks that give rise to influence and error. Quoting myths like Phaethon and interpretations of Goethe, Harari critiques the simplistic idea that individuals alone misuse power, reminding us instead that:

"Human power is never the outcome of individual initiative. Power always stems from cooperation between large numbers of humans."

Harari explores how information can mean different things to different people. For him, information is always embedded in symbols-spoken, written, or encoded. He clearly distinguishes disinformation as:

"A deliberate lie, occurring when someone consciously intends to distort our view of reality."

In the chapter on Stories, Harari reiterates a familiar but powerful idea:

"We Sapiens rule the world not because we are so wise, but because we are the only animal that can cooperate flexibly in large numbers."

Stories, he argues, are not mere entertainment-they are the foundation of social order, nationhood, branding, belief systems, and governance. Harari introduces three types of realities:

1. Objective reality - things that exist independently (like rivers and mountains),
2. Subjective reality - individual experiences like pain and love, and
3. Inter-subjective reality - constructs like money, laws, nations, and gods that exist only through shared belief and communication.

In The Noble Lie, he observes that fiction often outpaces truth in uniting people because fiction can be simplified and made emotionally comforting, while truth is often complex and discomforting.

His discussion on democracy is particularly salient. Harari argues:

"Dictatorship is a centralized information network lacking self-correcting mechanisms. Democracy, by contrast, is a distributed information network, rich in self-correcting mechanisms."

He warns against strongmen who dismantle these mechanisms-often starting with attacks on the judiciary and the press. For Harari:

"Democratic networks assume that everyone is fallible-including the winners of elections and the majority."

The second part, Inorganic Networks, comprises three chapters exploring the rise of machine-based information networks. He discusses how computers differ fundamentally from older communication tools like printing presses. In Relentless: The Network Is Always On, he warns that:

"The reputation market has always controlled people through social norms. Many more people commit suicide from shame and guilt than from financial distress."

Unlike organic systems, which require rest, digital networks are tireless and pervasive. This shift introduces new risks:

"Information is not truth. The network might not discover the truth-it might impose a new world order."

Harari argues that the threats posed by AI and computer networks are not just technological-they are deeply political. He writes:

"There is no technological solution to this problem. It is a political challenge. Do we have the political will to deal with it?"

The third part, Computer Politics, deals with the evolving interface between AI and governance. It includes chapters on whether democracies can survive the erosion of shared discourse, whether totalitarian regimes might fully embrace algorithmic control, and whether the world will coalesce into a global data empire-or fragment into digital colonies. He asks unsettling questions:

"Would you still be living in an independent country-or in a data colony?"

He highlights the danger of countries losing sovereignty to digital infrastructure controlled by foreign entities and corporations:

Please read further at page 28

seed...

CHEST

Online Course on Critical Thinking - Foundations, Skills & Applications for – Students & Professionals

Course Code: 02, Credit Hours: 4 Credits, Course Duration: 1 Semester

Curse Overview:

This course aims to develop students' critical thinking skills by encouraging logical reasoning, effective argumentation, and problem-solving. Students will learn to identify fallacies, construct sound arguments, evaluate evidence, and make well-informed decisions in academic, professional, and personal contexts.

Learning Outcomes:

By the end of the course, students will be able to:

- *Recognize the key components of critical thinking and logical reasoning.*
- *Analyse and evaluate arguments for validity, soundness, and clarity.*
- *Identify common logical fallacies and cognitive biases.*
- *Construct well-reasoned arguments and communicate them effectively.*
- *Apply critical thinking skills to solve problems and make decisions in real-world situations.*

Course Modules

Module 1:Introduction to Critical Thinking

Unit 1: Definition and importance of critical thinking
Unit 2: Critical thinking vs. ordinary thinking
Unit 3: Characteristics of a critical thinker.

Module 2:Basics of Logic and Reasoning

Unit 1: Arguments: Premises, conclusions, and structure
Unit 2: Deductive vs. inductive reasoning
Unit 3: Evaluating validity and soundness of arguments

Module 3:Identifying and Avoiding Fallacies

Unit 1: Common logical fallacies: Unit 1.1: Ad hominem
Unit 1.2: Straw man argument
Unit 1.3: False dichotomy
Unit 1.4: Slippery slope Unit 1.5: Hasty generalization
Unit 2: How to detect and address fallacies in arguments

Module 4:Cognitive Biases and Critical Thinking

Unit 1: Understanding cognitive biases: Confirmation bias, anchoring, etc.
Unit 2: The role of perception, memory, & heuristics in reasoning
Unit 3: Techniques to mitigate biases in decision-making

Module 5:Critical Reading and Media Analysis

Unit 1: Evaluating credibility and reliability of sources
Unit 2: Analysing media, news, and online content for bias and manipulation
Unit 3: Recognizing fake news and misinformation

Module 6:Argument Construction and Effective Communication

Unit 1: Structuring arguments: Claims, evidence, and reasoning
Unit 2: Writing and presenting arguments clearly and persuasively
Unit 3: Debates and discussions: Techniques for effective argumentation

Module 7:Problem-Solving and Decision-Making

Unit 1: Strategies for solving complex problems critically
Unit 2: Decision-making frameworks
Unit 3: Ethical reasoning and moral decision-making

Module 8:Applications of Critical Thinking

Unit 1: Applying critical thinking in academics and research
Unit 2: Critical thinking in professional and workplace settings
Unit 3: Case studies: Real-world problems requiring critical thinking

Teaching Methods Online:(i) Contents on LMS(ii) Interactive sessions (iii) Group activities, debates, and role-plays (iv) Case studies and analysis (v) Assignments and presentations

Online Assessment Methods: (i) Reading of Modules: 10% (ii) Quizzes/Tests: 20% (iii) Assignments and Essays: 25% (iv) Group Debate/Presentation: 15% (v) Final Exam: 30%

IMPORTANT NOTE -
Course will be offered in collaboration with the institutions. Also, students can directly enroll for the Courses. Certificate will be provided jointly by SEED-CHEST and Collaborating Institute(s).

CONTACT DETAILS:-
E-mail - seedicf@gmail.com
Phone - 9868820215
Landline- 011-43008598

SOCIETY FOR EDUCATION AND ECONOMIC DEVELOPMENT
Flat No-56 B, DDA SFS Flats, Sector -1 Pocket-1
Dwarka, New Delhi -110075.

College Post R. No. 65288/95
ISBN 978-81-929059-0-7

CHEST

Online Course on Communication Skills

A 4 Credit Course
8 MODULES COURSE WITH SUB-MODULE UNITS
DURATION: 60 HRS. 6-8 WEEKS

Average Per week self-study 8 Hrs.

and contact /test on Virtual mode 2 Hrs.

Course on Canvas Platform

Virtual Meet on Google Meet platform

Course Over View

This course helps participants develop effectivecommunication strategies for variouscontexts, improving verbal, non-verbal, writtencommunication, and skills for conflict Resolution, Negotiationtechniques, collaboration andeffectiveTeamwork.

Course Objectives

- Develop clear and concise verbal communication.
- Enhance active listening skills.
- Master non-verbal communication techniques (e.g., body language, tone).
- Improve writing skills for reports, emails, and formal documents.
- Overcome barriers to effective communication.
- Build confidence for public speaking and presentations.
- Build skills for Conflict Resolution and Negotiation
- Cultivate interpersonal skills for teamwork and leadership.

Course Modules

Module1: Introduction to Communication

- Understanding the basics of communication.
- Components: Sender, message, receiver, and feedback.
- Barriers to communication and how to overcome them.

Module2: Verbal Communication

- Speaking with clarity and confidence.
- Vocabulary building.
- Formal vs. informal communication.
- Handling difficult conversations.

Module3: Non-Verbal Communication

- Role of body language and facial expressions.
- Reading non-verbal cues.
- Using gestures effectively.

Module4: Listening Skills

- Active listening techniques.
- Empathetic listening.
- Improving concentration and retention.

Module5: Written Communication

- Email and business letter etiquette.
- Writing reports, proposals, and resumes.
- Editing and proofreading skills.

Module6: Public Speaking& Presentations

- Overcoming stage fright.
- Structuring effective presentations.
- Engaging your audience.

Module7: Conflict Resolution & Negotiation

- Dealing with conflicts constructively.
- Persuasion and negotiation techniques.

Module8: Communication in Teams

- Building rapport with colleagues.
- Collaboration and effective teamwork.

IMPORTANT NOTE -

Courses will be offered in collaboration with the institutions. Also, students can directly enroll for the Courses. Certificate will be provided jointly by SEED-CHEST and Collaborating Institute.

Published and Edited by Dr. G.D. Sharma on behalf of the Society for Education and Economic Development, from Flat No. 56, Sector-1, Pocket-1, Dwarka, New Delhi-110075, www.seededu.org / www.thecollgepost.in / www.indiancollegesforum.com, Phone 43008598, lasertypeset by Suvidha Computers, 86-A, Adchini, New Delhi-110017.