INDIAN INSTITUTE OF PUBLIC ADMINISTRATION
कर्मसु कौशलम्

एन सी ई आर टी
NCERT

NCERT

National Council Of Educational Research And Training

New Emerging technology:

Threats and Opportunities in Current Scenario

DR. SURABHI PANDEY

PHD(CLOUD SECURITY)M.PHIL MCA, MCM,

MASTER IN DATA SCIENCE

Agenda Points

Journey of Digital Infrastructure to Digital Transformation

Digital India 2.0

New Emerging Technologies

Services and Security of Digital World

Securing the Cyber ecosystem

Way forward

India's Digital Transformation journey over the last 75 years

Trends that initiated India’s Digital way forward

Trend1 The desire of replacing manpower with “smart” power

Trend2 The mission of becoming a “paperless, faceless, cashless” economy

Trend3 The vision of selling an “experience” not just a product or service

Top 10 EMERGING TECHNOLOGIES?

Artificial Intelligence

Quantum computing

Blockchain technology

IOT

RPA

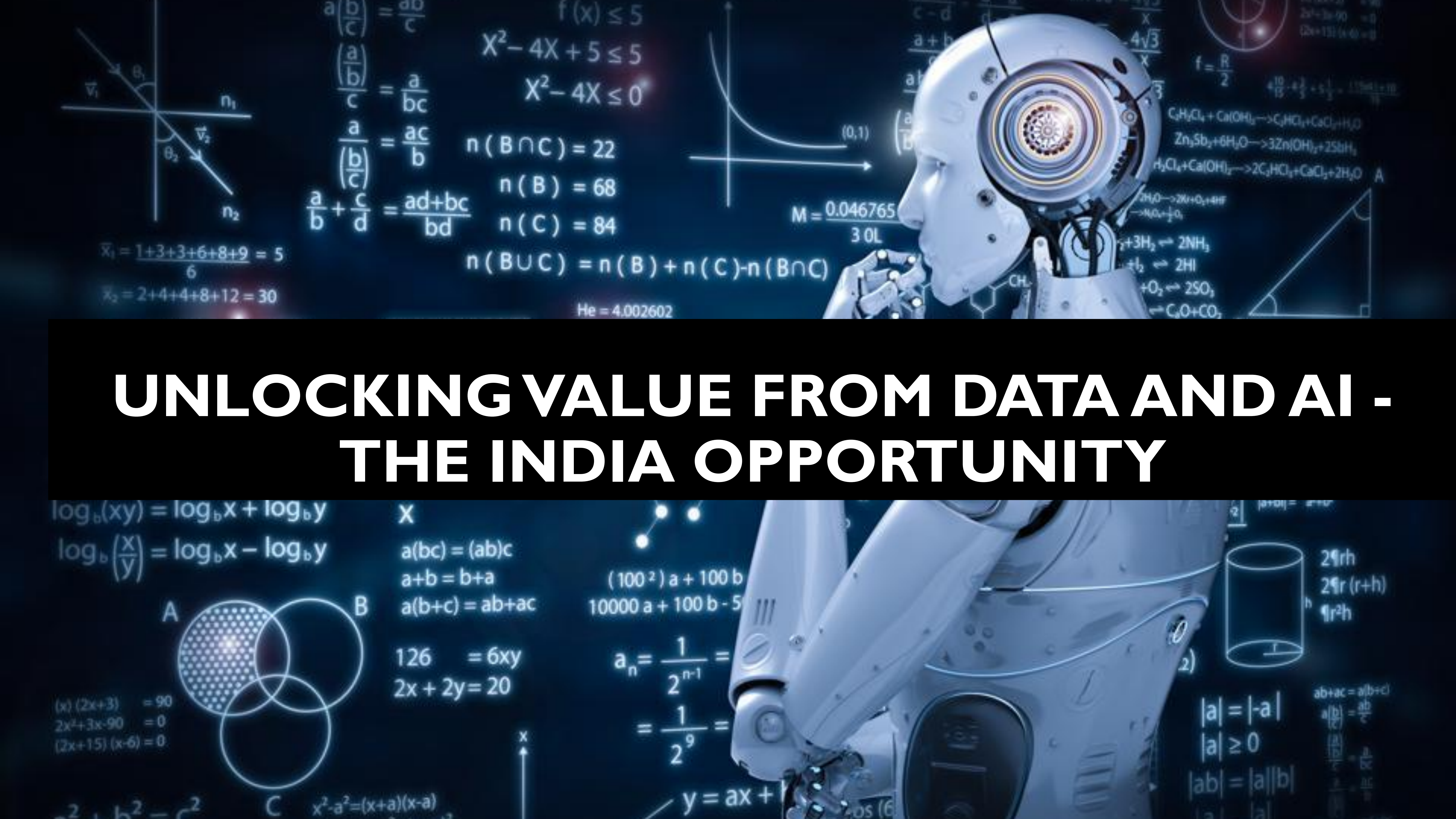
Voice assistance

Cloud computing

Augmented reality

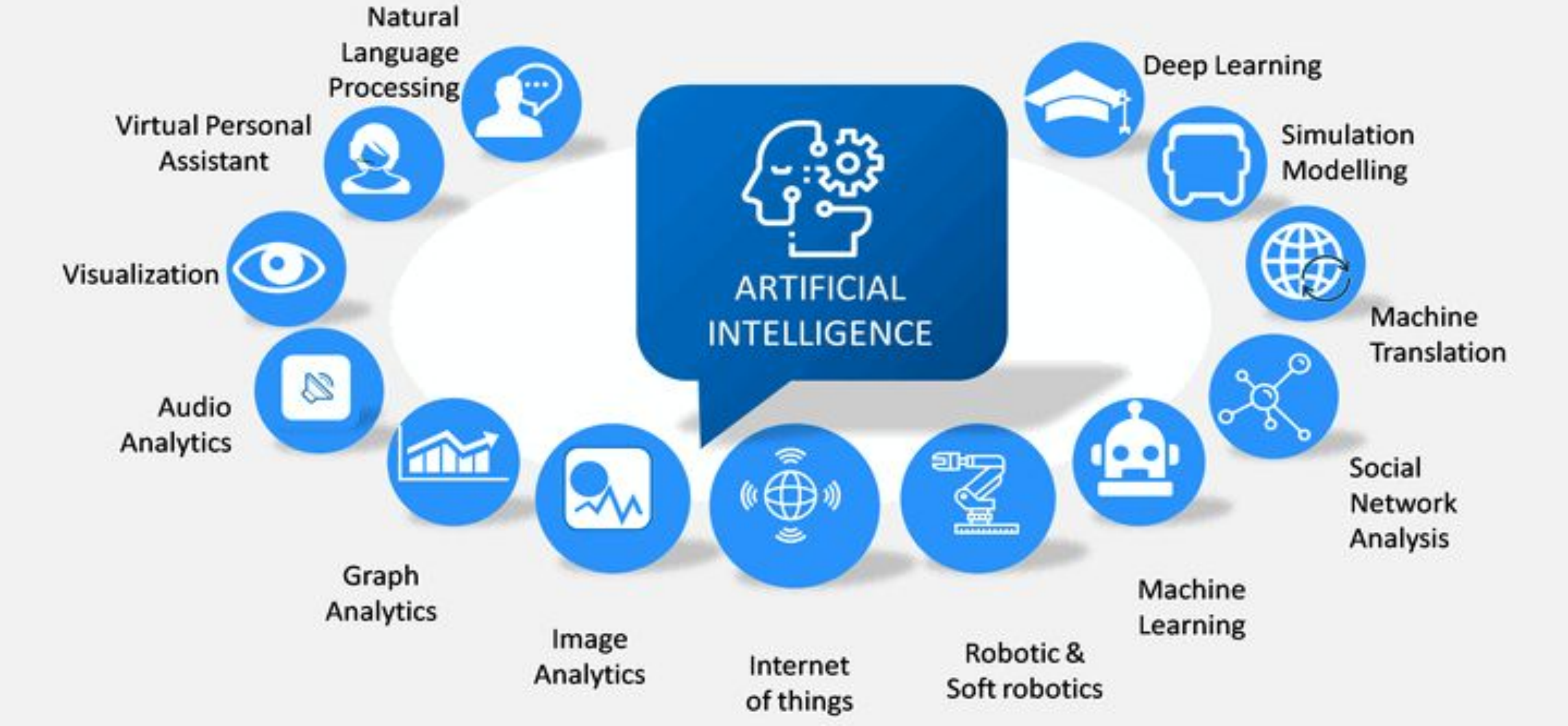
Genetic prediction

5G



UNLOCKING VALUE FROM DATA AND AI - THE INDIA OPPORTUNITY

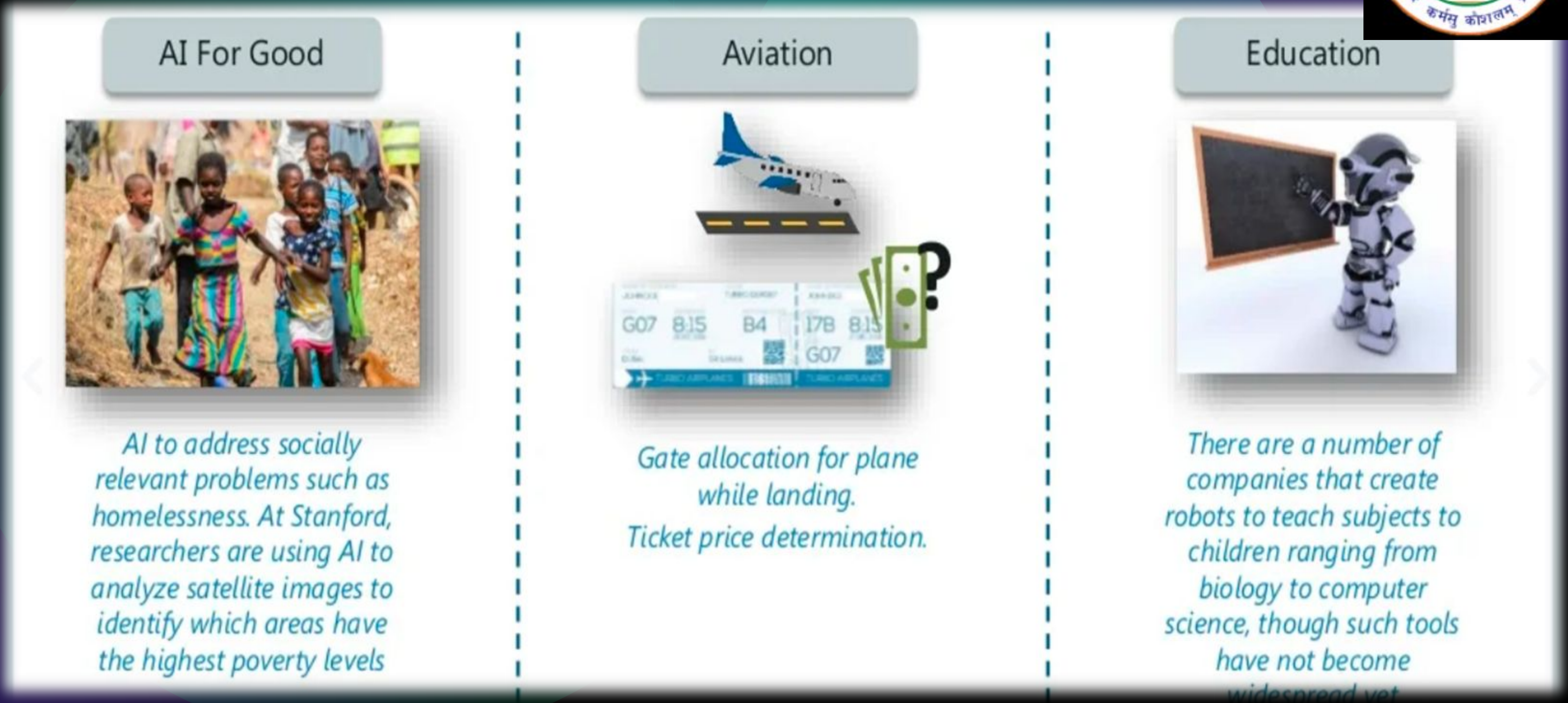
ARTIFICAL INTELLIGENCE APPLICATIONs



AI AND MACHINE LEARNING USE

Delhi Police is using AI in the implementation of the **SAFE CITY PROJECT.**

Use Case of Artificial Intelliger



AI For Good

AI to address socially relevant problems such as homelessness. At Stanford, researchers are using AI to analyze satellite images to identify which areas have the highest poverty levels

Aviation

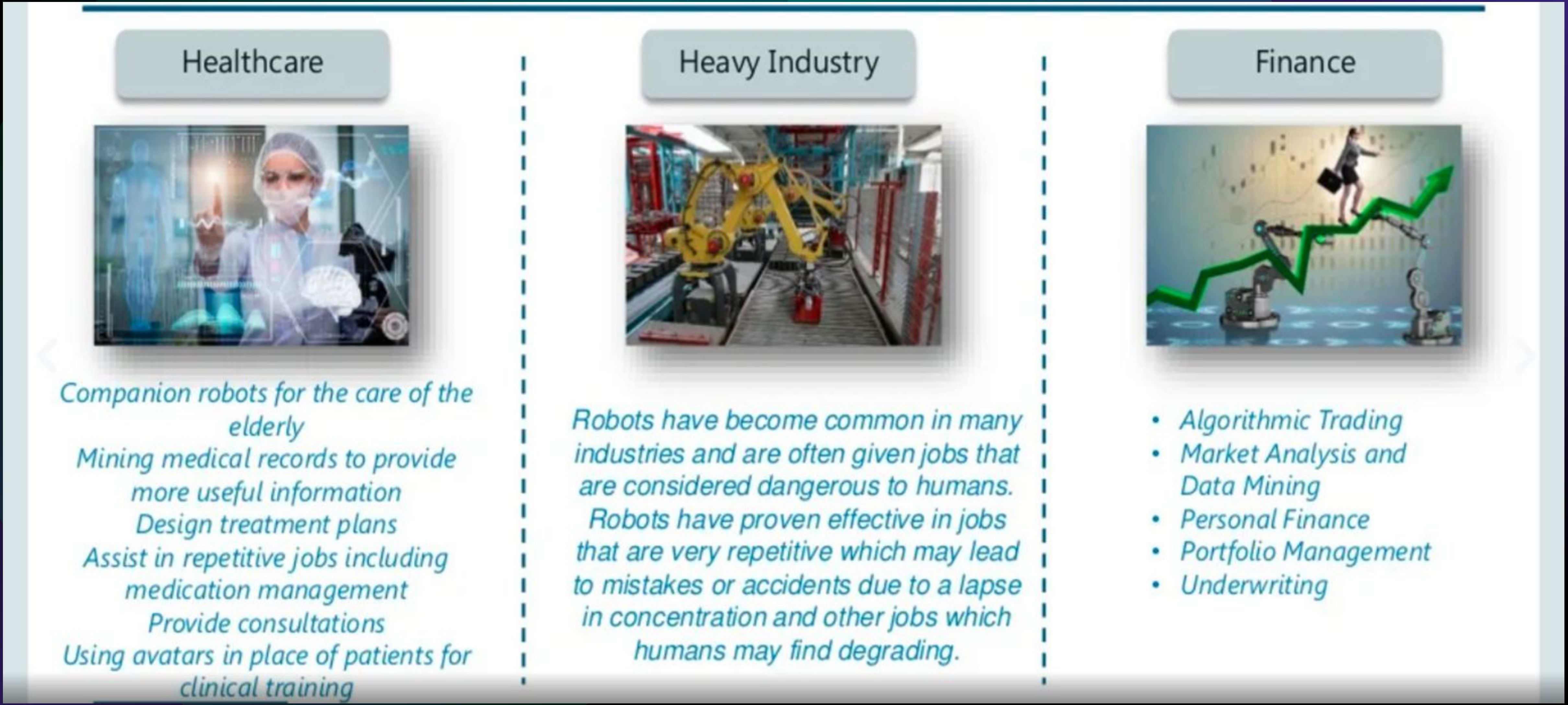
Gate allocation for plane while landing.

Ticket price determination.

Education

There are a number of companies that create robots to teach subjects to children ranging from biology to computer science, though such tools have not become widespread yet.

Use Case of Artificial Intelligence



Healthcare

Companion robots for the care of the elderly

Mining medical records to provide more useful information

Design treatment plans

Assist in repetitive jobs including medication management

Provide consultations

Using avatars in place of patients for clinical training

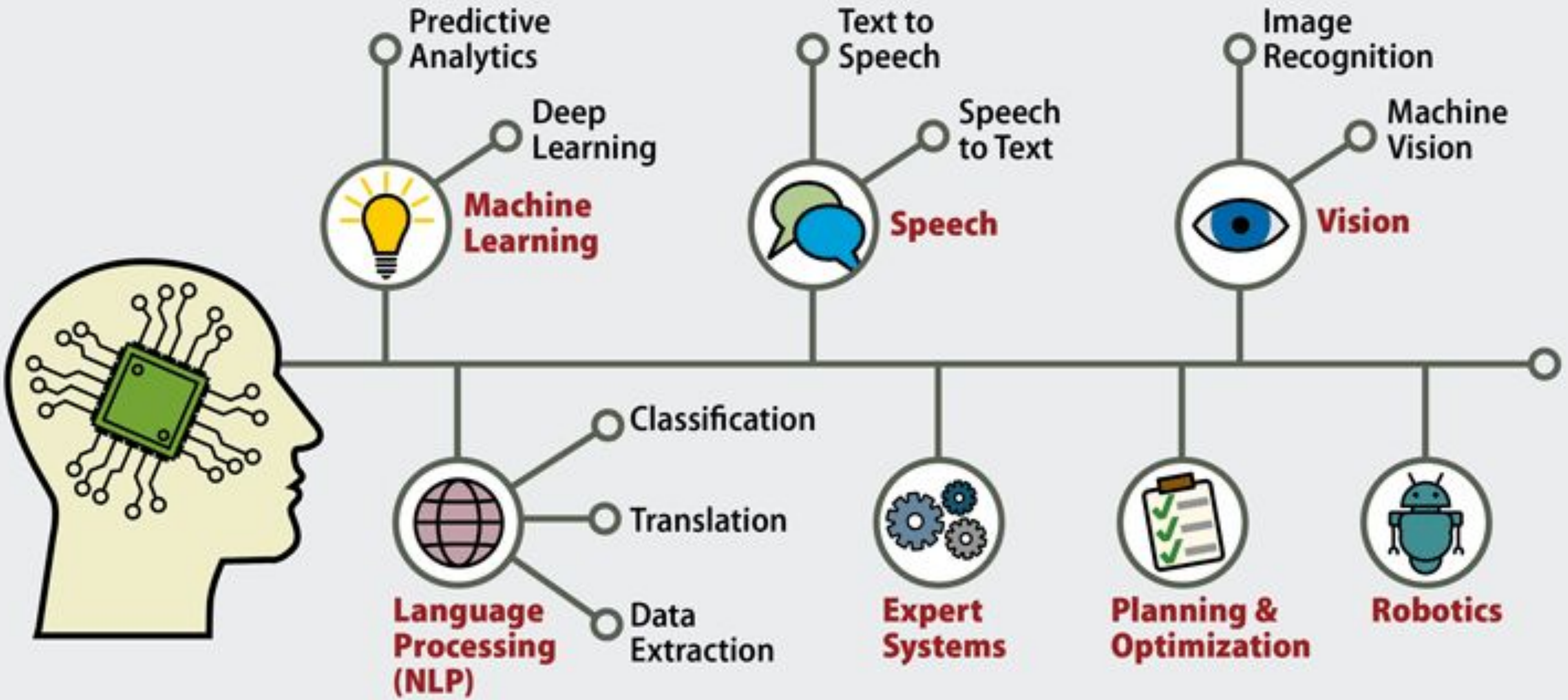
Heavy Industry

Robots have become common in many industries and are often given jobs that are considered dangerous to humans. Robots have proven effective in jobs that are very repetitive which may lead to mistakes or accidents due to a lapse in concentration and other jobs which humans may find degrading.

Finance

- Algorithmic Trading
- Market Analysis and Data Mining
- Personal Finance
- Portfolio Management
- Underwriting

Artificial Intelligence



Machine Learning
- Predictive Analytics
- Deep Learning

Speech
- Text to Speech
- Speech to Text

Vision
- Image Recognition
- Machine Vision

Language Processing (NLP)
- Classification
- Translation
- Data Extraction

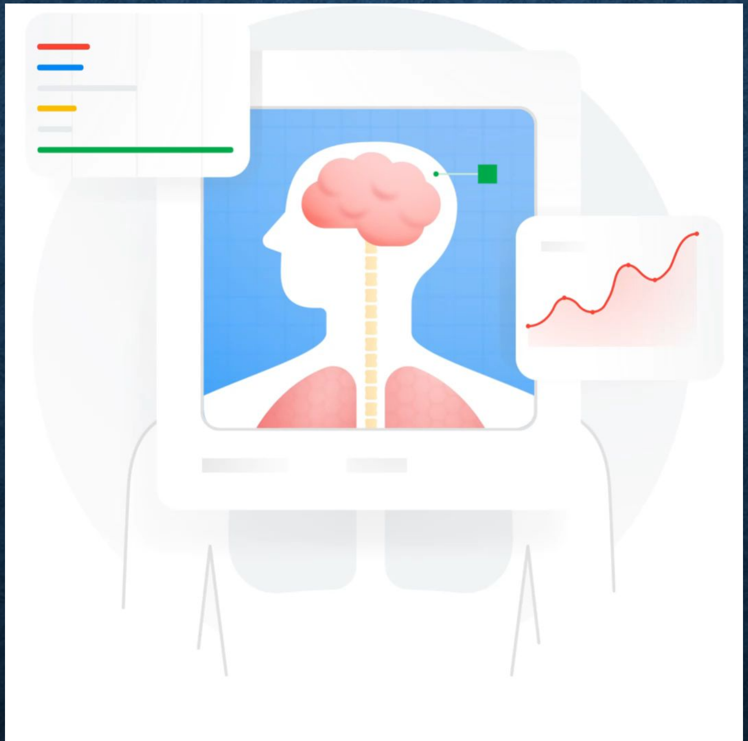
Expert Systems

Planning & Optimization

Robotics

The future of healthcare with artificial intelligence

Improving access to skin disease information



AI advancement in radiotherapy planning

A promising step forward for predicting lung cancer

CHALLENGES IN ARTIFICIAL INTELLIGENCE

- **Lack of enabling data ecosystems**

- **Low intensity of AI research**

i. Core research in fundamental technologies

ii. Transforming core research into market applications

- **High resource cost and low awareness for adopting AI in business processes**

Common Artificial Intelligence Challenges

54% of enterprises are dealing with a huge shortage of skilled **AI talent**

42% of enterprises struggle to align their AI strategies to the **business context**

44% of enterprises are challenged by **data management** issues in terms of data governance, acquisition, and bias

33% of enterprise struggle with the cost-intensive implementation of AI and **lack funds**

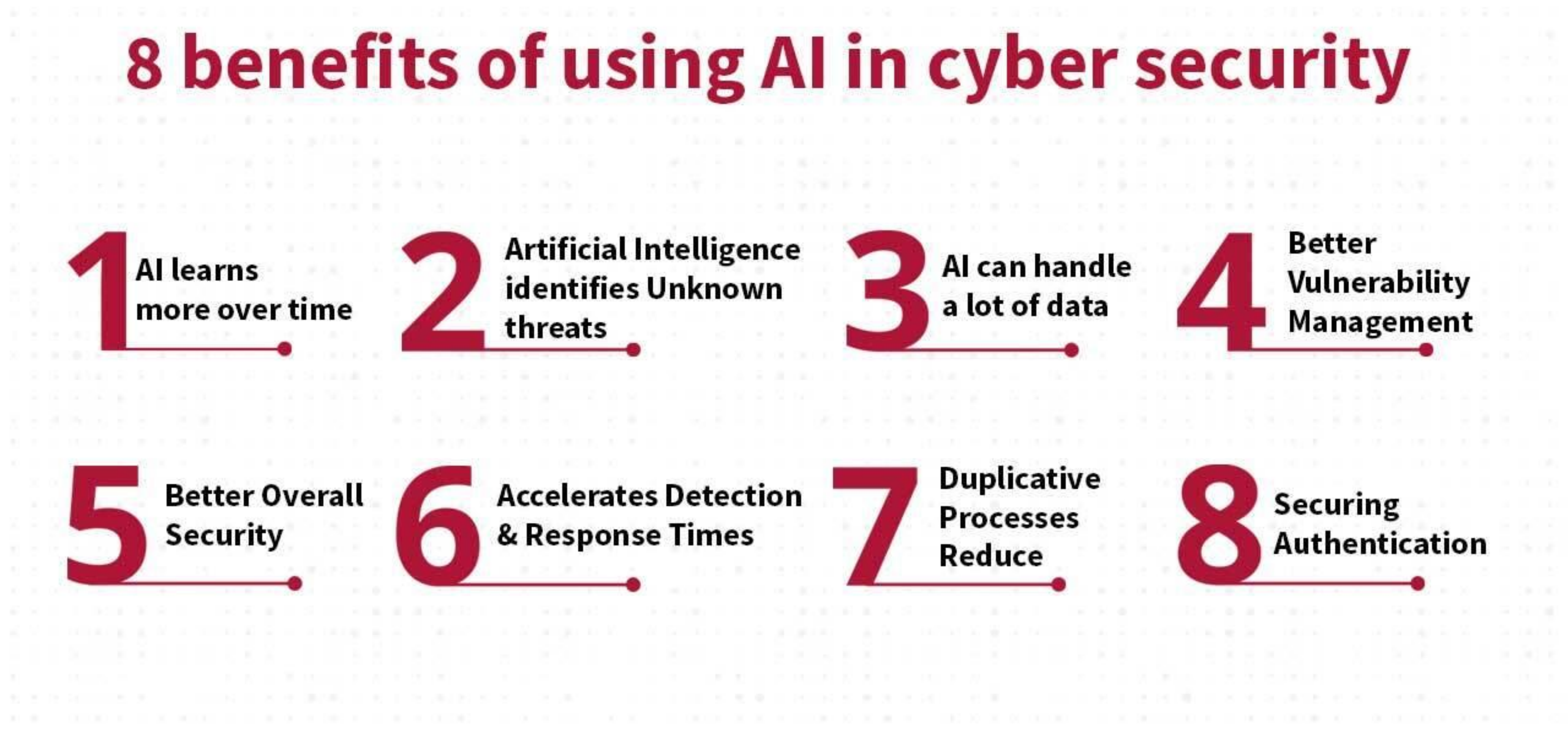
82% of enterprises fail to scale AI and achieve meaningful business outcomes

Source: Everest Group survey with IT heads across 200 global enterprises in North America and Europe on their AI adoption

OPPORTUNITIES AND WAY FORWARD IN ARTIFICIAL INTELLIGENCE

- India forms the IT backbone of the world. The country’s companies and talent are the natural contenders to add ‘intelligence’ to all the digitization.

- India’s services sector (call centers, BPOs, etc. – roughly 18% of the Indian GDP) have a significant potential opportunity to cater to the coming demand for data cleaning and human-augmented AI training (data labelling, search engine training, content moderation, etc.).



8 benefits of using AI in cyber security

1 AI learns more over time

2 Artificial Intelligence identifies Unknown threats

3 AI can handle a lot of data

4 Better Vulnerability Management

5 Better Overall Security

6 Accelerates Detection & Response Times

7 Duplicative Processes Reduce

8 Securing Authentication

Objectives

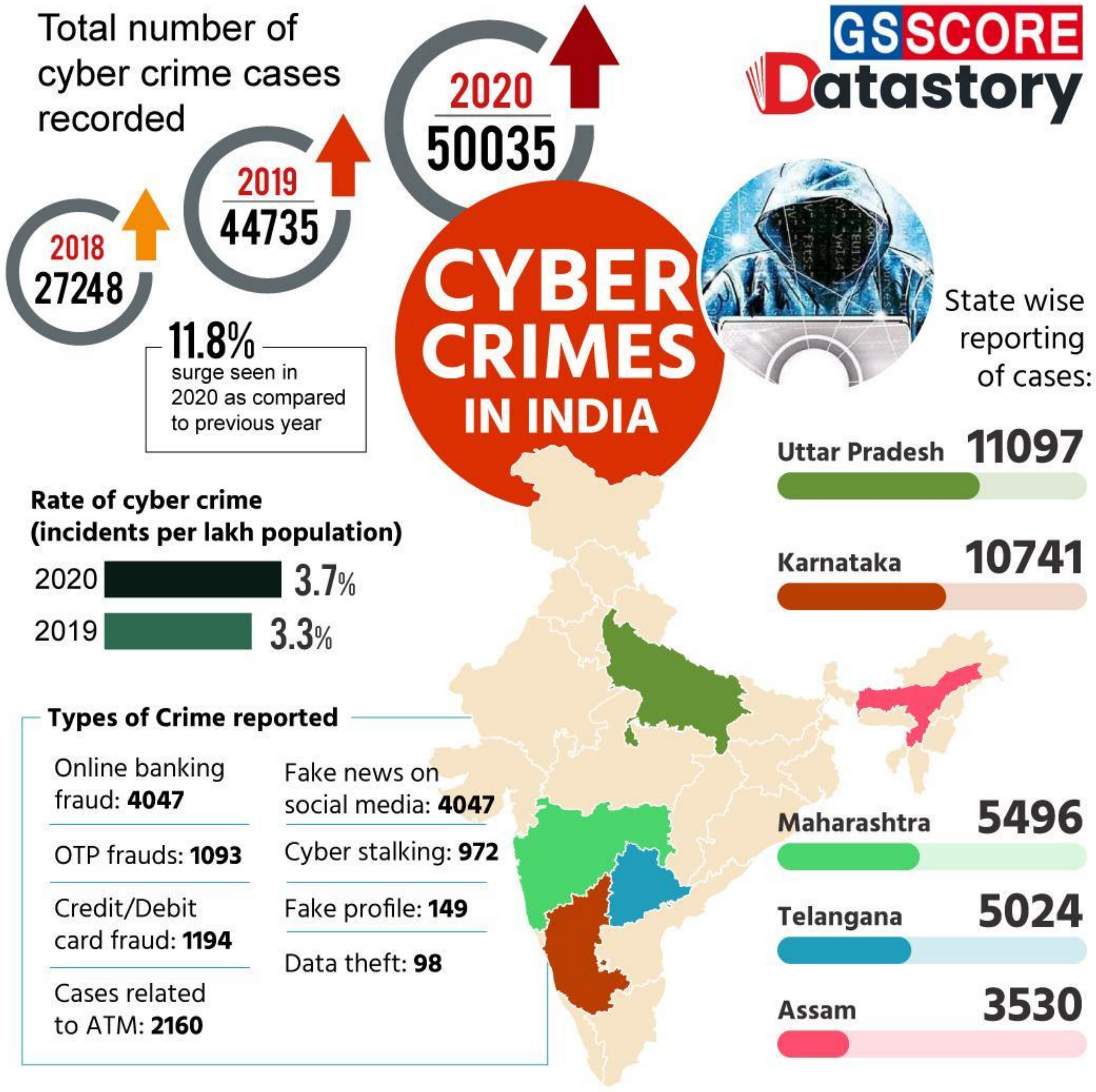
Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

Educational platforms based on Artificial Intelligence technology

- Third Space Learning
- Little Dragon
- Brainy
- CTI
- Carnegie Learning
- ThinkerMath

Cyber Crimes In India



GS SCORE Datastory

CYBER CRIMES IN INDIA

Total number of cyber crime cases recorded

2018	2019	2020
27248	44735	50035

11.8% surge seen in 2020 as compared to previous year

Rate of cyber crime (incidents per lakh population)

2020	3.7%
2019	3.3%

Types of Crime reported

- Online banking fraud: **4047**
- OTP frauds: **1093**
- Credit/Debit card fraud: **1194**
- Cases related to ATM: **2160**
- Fake news on social media: **4047**
- Cyber stalking: **972**
- Fake profile: **149**
- Data theft: **98**

State wise reporting of cases:

Uttar Pradesh	11097
Karnataka	10741
Maharashtra	5496
Telangana	5024
Assam	3530

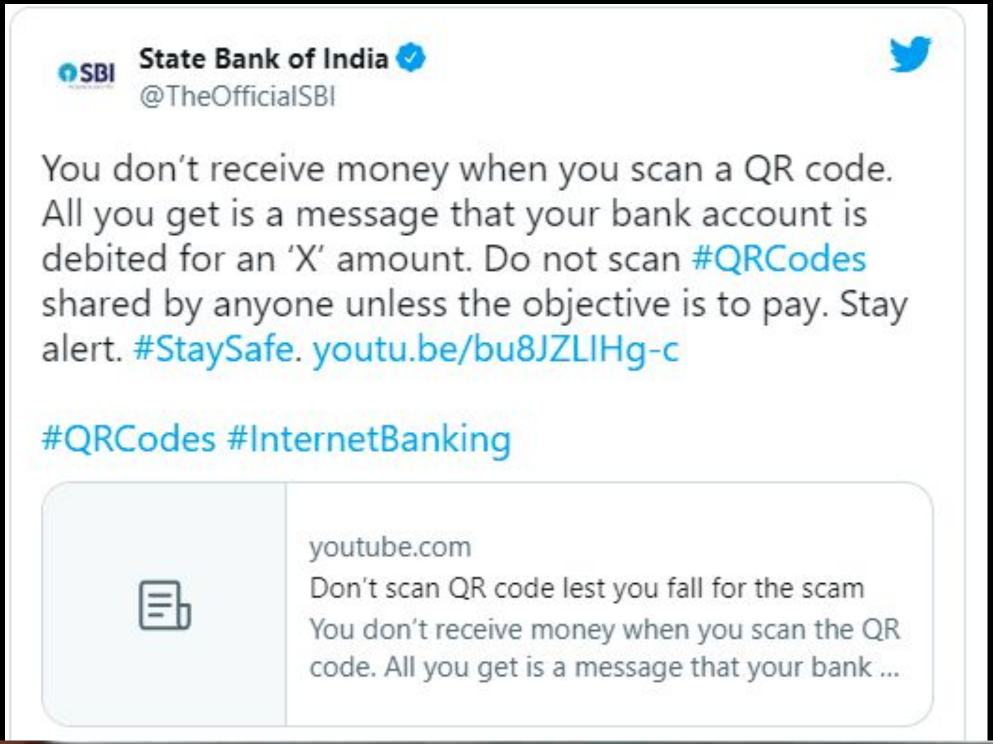
AI Security Use Cases

- Malicious Traffic Identification
- Fraudulent/ Risky User Identification
- Identifying phishing websites
- Identifying Botnet domains
- Identifying Database attacks
- Security intelligence consolidation
- Automated threat disposition
- Threat categorization and attack phase determination
- Data classification
- Account takeover and fraud detection

QR code scams are on the rise.

The goal of QR code fraud is pretty much always the same: getting you to navigate to a page through which cybercriminals can steal your data, money, or both.

> “Remember that QR codes are generally used for paying money, not for receiving it.”



State Bank of India
@TheOfficialSBI

You don’t receive money when you scan a QR code. All you get is a message that your bank account is debited for an ‘X’ amount. Do not scan #QRCodes shared by anyone unless the objective is to pay. Stay alert. #StaySafe. youtu.be/bu8JZLIHg-c

#QRCodes #InternetBanking

youtube.com
Don't scan QR code lest you fall for the scam
You don't receive money when you scan the QR code. All you get is a message that your bank ...

Cryptocurrency Scams: Crypto crime in India on the rise: A look at major scams in recent years

Rs 1,200-crore Morris coin fraud
The latest of the crypto frauds, the Morris coin fraud, was unearthed in 2022. Over 900 investors were allegedly duped of Rs 1,200 crore by a website offering a fake cryptocurrency called Morris coin. They had invested in the 'initial offering' of the fake cryptocurrency.

Despite market fluctuations and an uncertain legal status, cryptocurrencies continue to fascinate Indian investors. The number of crypto users and traders keeps increasing, and worryingly, many seem to be unmindful of the associated risks . These are not limited to market risks; they extend to extreme cyber frauds, involving highly skilled scammers.

How expired web domains help criminal hackers unlock enterprise defenses

https://www.expireddomains.net/godaddy-closeout-domains/

- Managing domain names is a task that enterprises often leave to the marketing department rather than the security team.
- Hijacked domains are used for identity-based attack vectors such as account takeovers or phishing campaigns
- Cyber crooks can use dropped domains for any attack vector that exploits an organization’s identity, such as account takeovers or phishing campaigns that leverage false business invoices.

Exploit-as-a-service: Cybercriminals exploring potential of leasing out zero-day vulnerabilities

- Cybercriminals are starting to consider leasing or rather than just selling zero-day vulnerabilities under a potential ‘exploit-as-a-service’ model for the first time,
- Renting parties could test the proposed zero-day and later decide whether to purchase the exploit on an exclusive or non-exclusive basis.
- The exploit-as-a-service model may offer malicious hackers a new means of diversifying their revenue streams.(click and shoot model)

Metaverse: New Digital world

The metaverse is a set of virtual spaces where you can create and explore with other people who aren't in the same physical space as you. You'll be able to hang out with friends, work, play, learn, shop, create, and more."

American science fiction author Neal Stephenson introduced the metaverse in his 1992 novel, Snow Crash. In the novel (like others in its genre), users use metaverse as an escape from a futuristic, largely dystopian world.

The metaverse can be defined as a simulated digital environment that uses augmented reality (AR), virtual reality (VR), and blockchain, along with concepts from social media, to create spaces for rich user interaction mimicking the real world.

USAF Files Patent for SPACEVERSE Metaverse Trainer

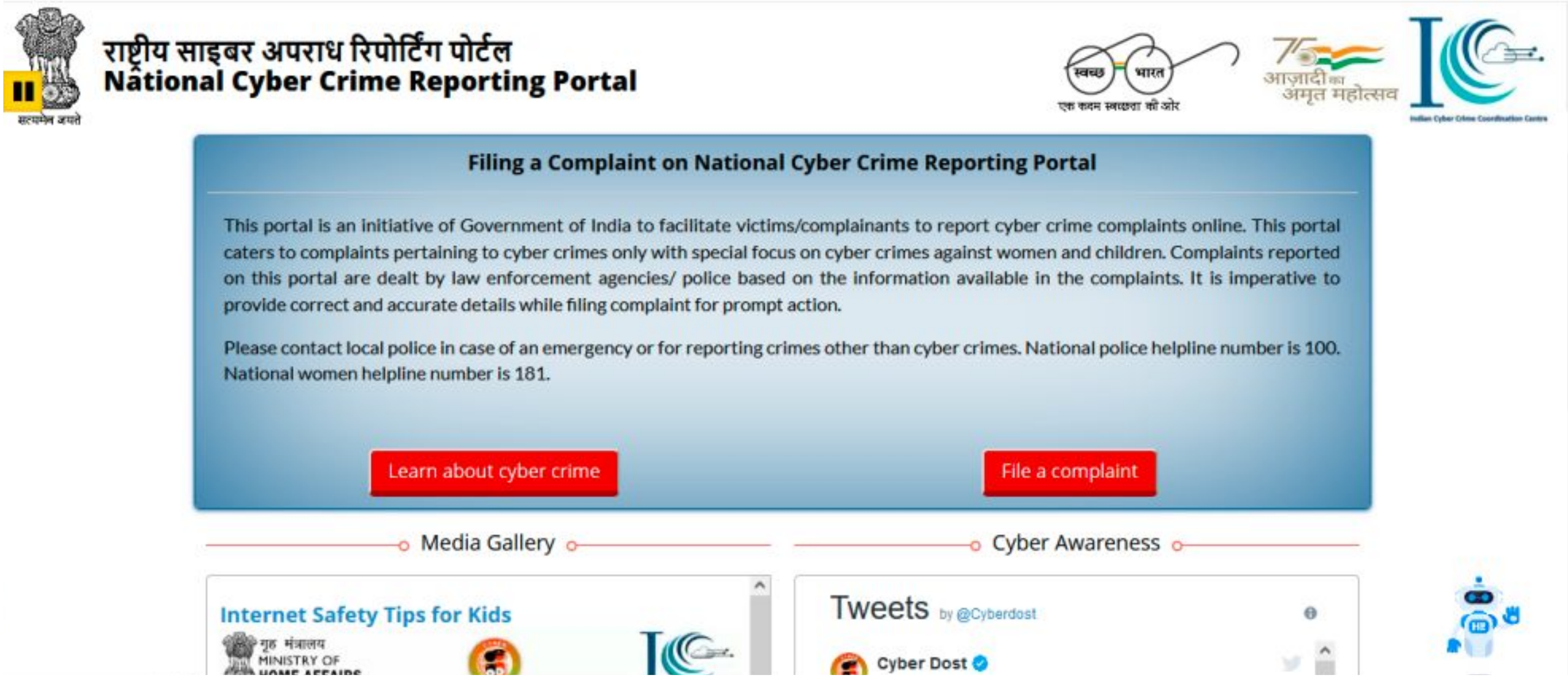
The US Air Force (USAF) filed a trademark on 14 April with the US Patent and Trademark Office, media reports have revealed this week. Citing a tweet from **Mike Kondoudis, USPTO Trademark Attorney**, reports found the USAF aimed to patent a SPACEVERSE for training personnel and staff in extended reality (XR).

"a secure digital metaverse that converges terrestrial and space physical and digital realities and provides synthetic and simulated extended-reality (XR) training, testing, and operations environments"

Top 10 cyber crime trends

- Weaponising operational technology environments
- Remote working brings new challenges
- Geopolitical cyber concerns pose growing risks
- Use of social media for attacks
- Cryptocurrency exchanges to experience an increase in attacks
- Phishing attacks
- API becoming a lucrative target
- Rise of ransomware
- Cloud migration poses threat

I4C www.cybercrime.gov.in , 1930



सत्यमेव जयते
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal
स्वच्छ भारत
एक कदम स्वच्छता की ओर
आज़ादी का अमृत महोत्सव
Indian Cyber Crime Coordination Centre

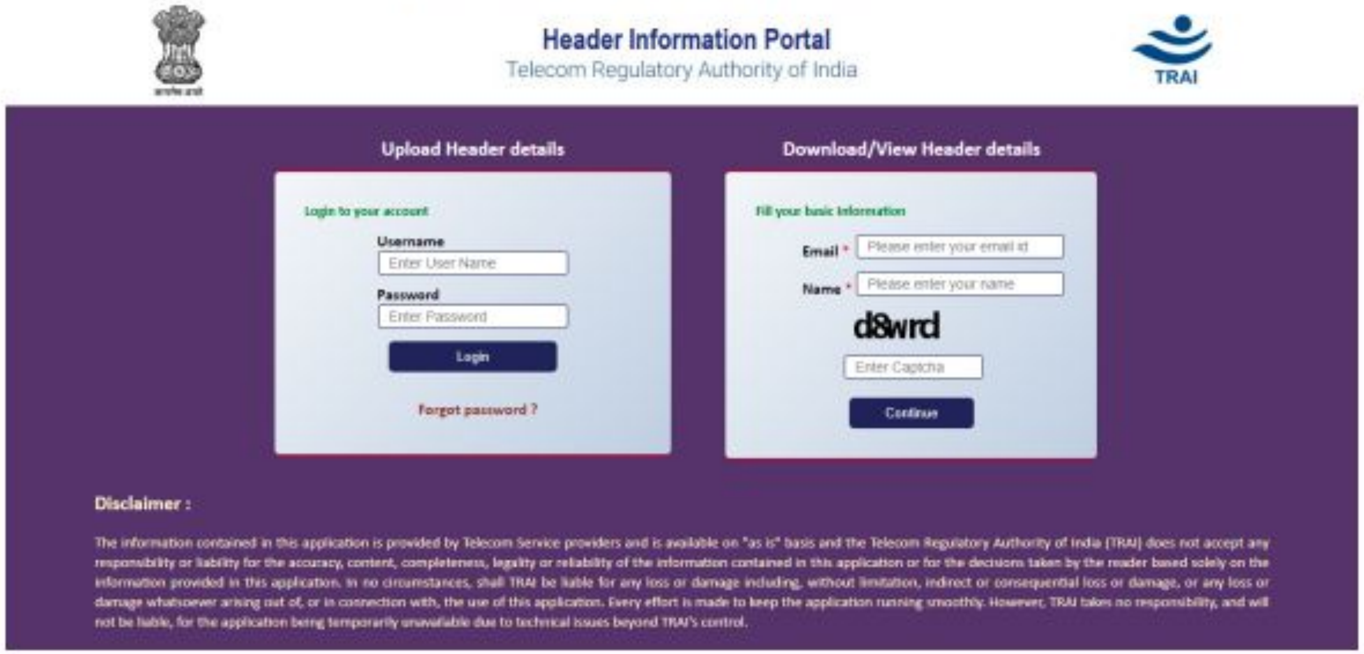
Filing a Complaint on National Cyber Crime Reporting Portal

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 100. National women helpline number is 181.

TRAI initiatives

www.smsheader.trai.gov.in



Header Information Portal

Telecom Regulatory Authority of India

TRAI

Upload Header details

Login to your account

Username: Enter User Name

Password: Enter Password

Login

Forgot password ?

Download/View Header details

Fill your basic information

Email *: Please enter your email id

Name *: Please enter your name

d8wrd

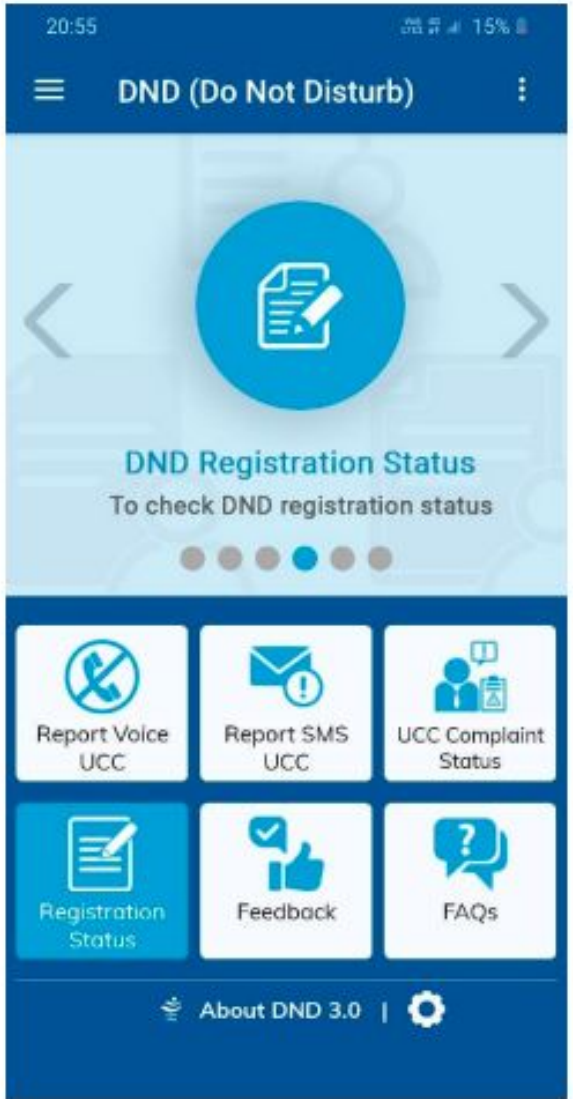
Enter Captcha

Continue

Disclaimer :

The information contained in this application is provided by Telecom Service providers and is available on "as is" basis and the Telecom Regulatory Authority of India (TRAI) does not accept any responsibility or liability for the accuracy, content, completeness, legality or reliability of the information contained in this application or for the decisions taken by the reader based solely on the information provided in this application. In no circumstances, shall TRAI be liable for any loss or damage including, without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising out of, or in connection with, the use of this application. Every effort is made to keep the application running smoothly. However, TRAI takes no responsibility, and will not be liable, for the application being temporarily unavailable due to technical issues beyond TRAI's control.

DLT portals for compulsory SMS template registration with TSPs

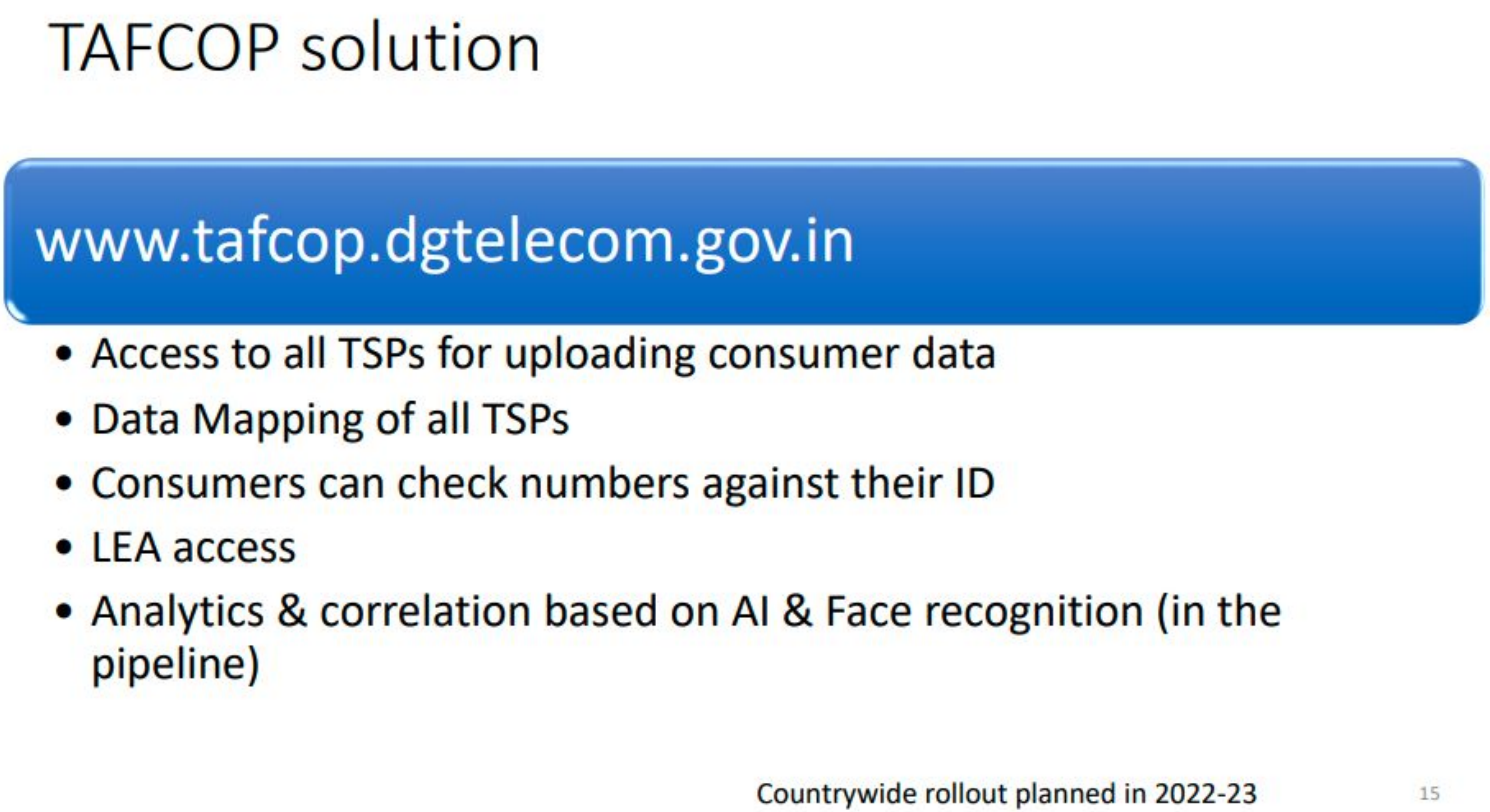


20:55 15%

DND (Do Not Disturb)

DND Registration Status

To check DND registration status



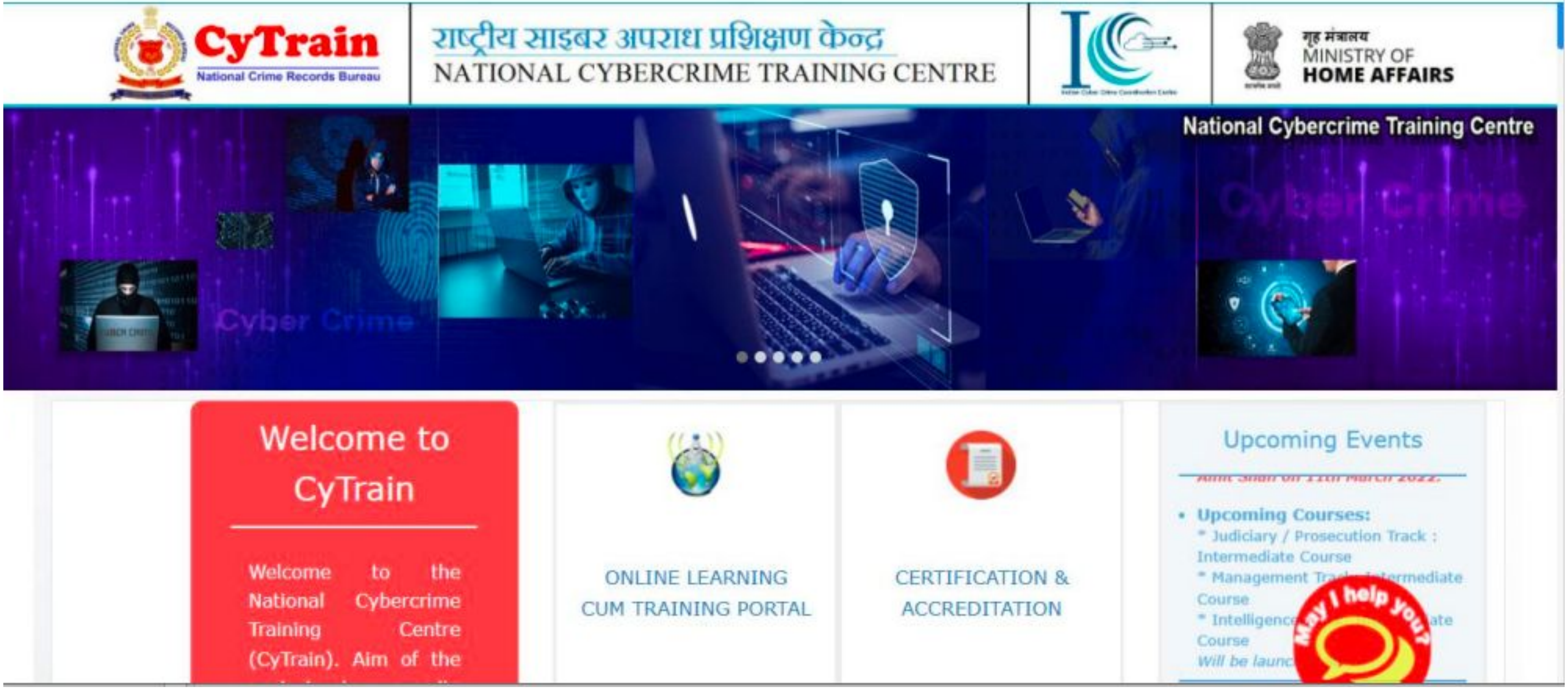
TAFCOP solution

www.tafcop.dgtelecom.gov.in

- Access to all TSPs for uploading consumer data
- Data Mapping of all TSPs
- Consumers can check numbers against their ID
- LEA access
- Analytics & correlation based on AI & Face recognition (in the pipeline)

Countrywide rollout planned in 2022-23

I4C www.cytrain.ncrb.gov.in



CyTrain
National Crime Records Bureau

राष्ट्रीय साइबर अपराध प्रशिक्षण केन्द्र
NATIONAL CYBERCRIME TRAINING CENTRE

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Welcome to CyTrain

Welcome to the National Cybercrime Training Centre (CyTrain). Aim of the

ONLINE LEARNING CUM TRAINING PORTAL

CERTIFICATION & ACCREDITATION

Upcoming Events

Amit Shah on 11th March 2022.

- **Upcoming Courses:**
  * Judiciary / Prosecution Track : Intermediate Course
  * Management Tra Intermediate Course
  * Intelligence ate Course
  Will be launc

“Cybersecurity is a shared responsibility and its boils down to this: In Cybersecurity, the more systems we secure, the more secure we all are “.

Cyber World

THANK YOU

The Invisible criminals are more Dangerous than the visible one"

You can find me at:
dr.pandeysurabhi@gmail.com

INDIAN INSTITUTE OF PUBLIC ADMINISTRATION