

Ministry of Electronics and Information Technology (MeitY)
Government of India

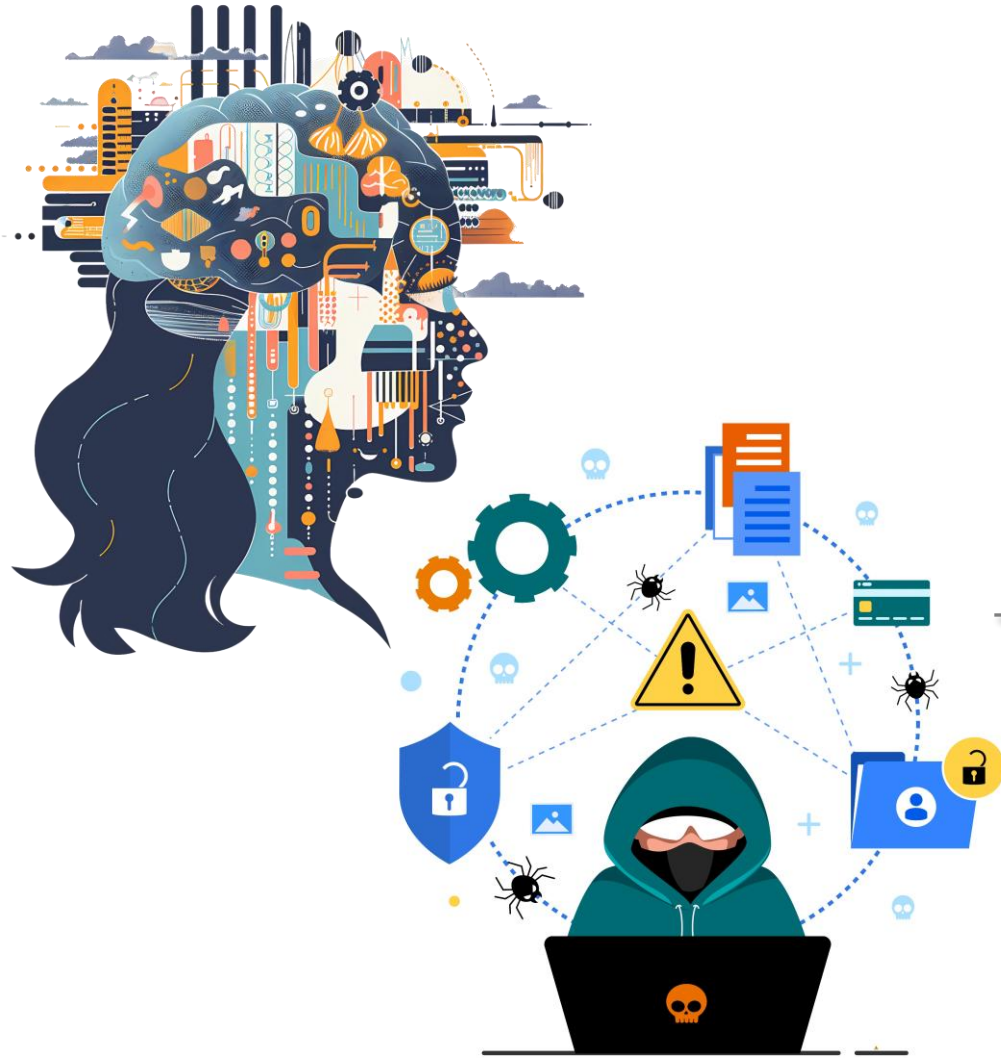


www.isea.gov.in

staysafeonline.in

Information Security Education and Awareness (ISEA) Project

Cyber Hygiene Practices



Artificial Intelligence and Cyber Risk Landscape

Navigating the Opportunities, Threats & Responsibilities

Dr. Sanjay Madan

Scientist 'E',

Applied Artificial Intelligence & Analytics Division



Centre for Development of Advanced Computing (C-DAC),
Mohali

AI & Cyber Risk Landscape

Let me start with a real situation many of us can relate to...

“One morning, an employee in an Indian company receives a phone call. The caller sounds exactly like the company’s senior manager — same voice, same tone, same authority.

The caller says: *‘This is urgent. A confidential payment needs to be released immediately. I’m in a meeting. Do it now.’*

Trusting the voice, the employee transfers the money.

Later, it turns out — the manager never called. The voice was generated using Artificial Intelligence.

This is not science fiction. This is today’s cyber risk landscape.”

Artificial Intelligence is transforming our lives — but it is also transforming cyber threats.

Today, we need to understand how AI changes cyber risk, in a simple and practical way.

Why it matters?

It matters now more than ever due to several critical factors:

- India is rapidly digitizing with various services:
 - Digital Payments (UPI) – In India, processes millions of UPI transactions daily
 - Aadhaar-based services
 - Online education, healthcare, banking
- Massive data generation
- Increased dependency on digital platforms

The more digital we become, the larger the cyber risk surface becomes.

Top Threats and Trends in 2025

- **AI-Enabled Attacks:** Over 47% of organizations cite generative AI as a primary concern, allowing attackers to create more sophisticated, scalable, and personalized phishing campaigns.
- **Ransomware and Extortion:** Ransomware remains a top threat, with attackers focusing on data exfiltration and extortion.
- **Supply Chain Exploitation:** Attackers are increasingly targeting the software supply chain and third-party vendors to breach broader, more secure, networks.
- **Identity-Based Attacks:** A significant surge in infostealer malware and stolen credentials (42% increase) is fuelling unauthorized access.
- **Geopolitical Conflict:** State-aligned actors are blending cyber espionage with financial motives.

What is Artificial Intelligence?

Artificial

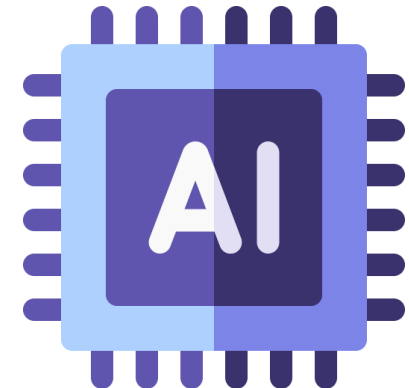
Refers to something which is made or produced by human being rather than occurring naturally, especially as a copy of something natural.

Intelligence

Refers to the ability to acquire and apply knowledge and skills.

Artificial Intelligence (AI) refers to the computer systems that:

- AI system learns from data & analyzes large amount of data
- Recognize patterns by learning historical data
- Make predictions or decisions without explicit programming



Result Quality of AI depends upon – Quality of data & Quality of design

Types of AI

Artificial Intelligence (AI):

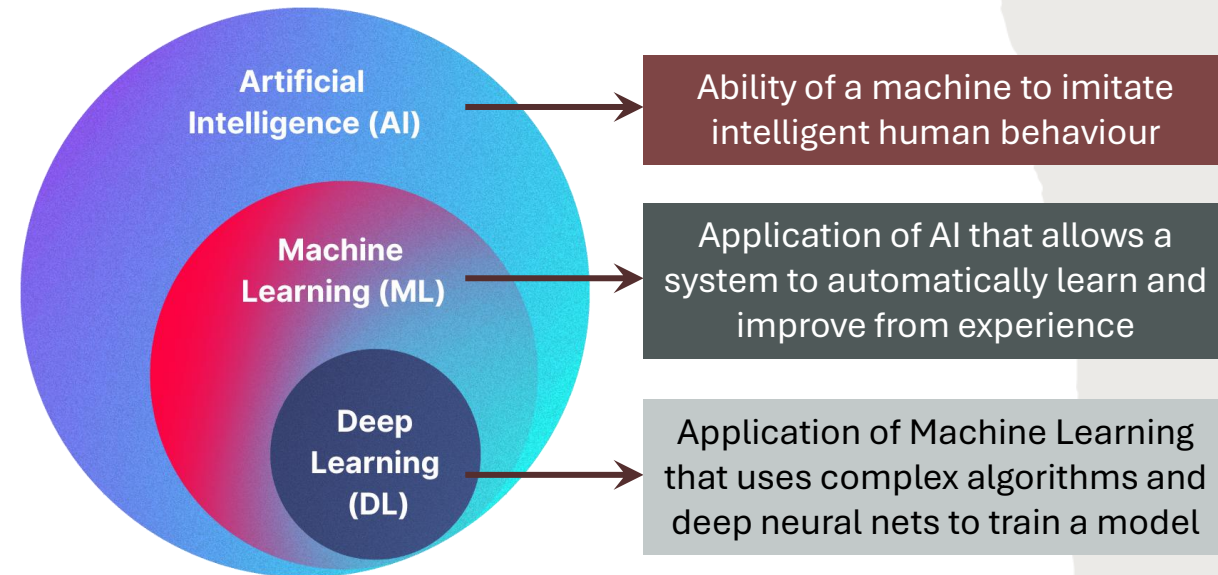
- AI involves creating intelligent machines that perform human-like tasks
- AI can be considered as the umbrella term encompassing ML and DL

Machine Learning (ML):

- ML is a type of AI that uses rules and mathematical models to enable machines to learn from data and improve performance
- For example, a spam filter that learns to identify spam emails based on user feedback is an example of ML

Deep Learning (DL):

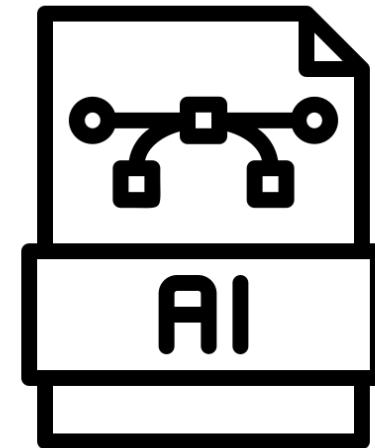
- DL is a type of ML that uses deep neural networks to find patterns and make predictions from large amounts of data
- For example, Self-driving cars use computer vision and deep learning to identify objects and make decisions



Types of AI

Generative AI

- Generative AI is a type of Artificial Intelligence that creates new, original content, including text, images, code, audio, and video by learning patterns from large existing datasets.
- For example, Generative AI has numerous applications in cybersecurity like automative threat detection, analyzing large datasets for identification of anomalies, generating real-time responses to security incidents.



What is Cyber Security?

“Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”



Leveraging AI Capabilities in Cyber Security

- In Pattern Recognition, Anomaly Detection, and Predictive Analysis to combat evolving threats

Types of AI relevant to Cyber Security

Rule-based Systems

- Uses pre-defined rules
- Example: Firewall rules

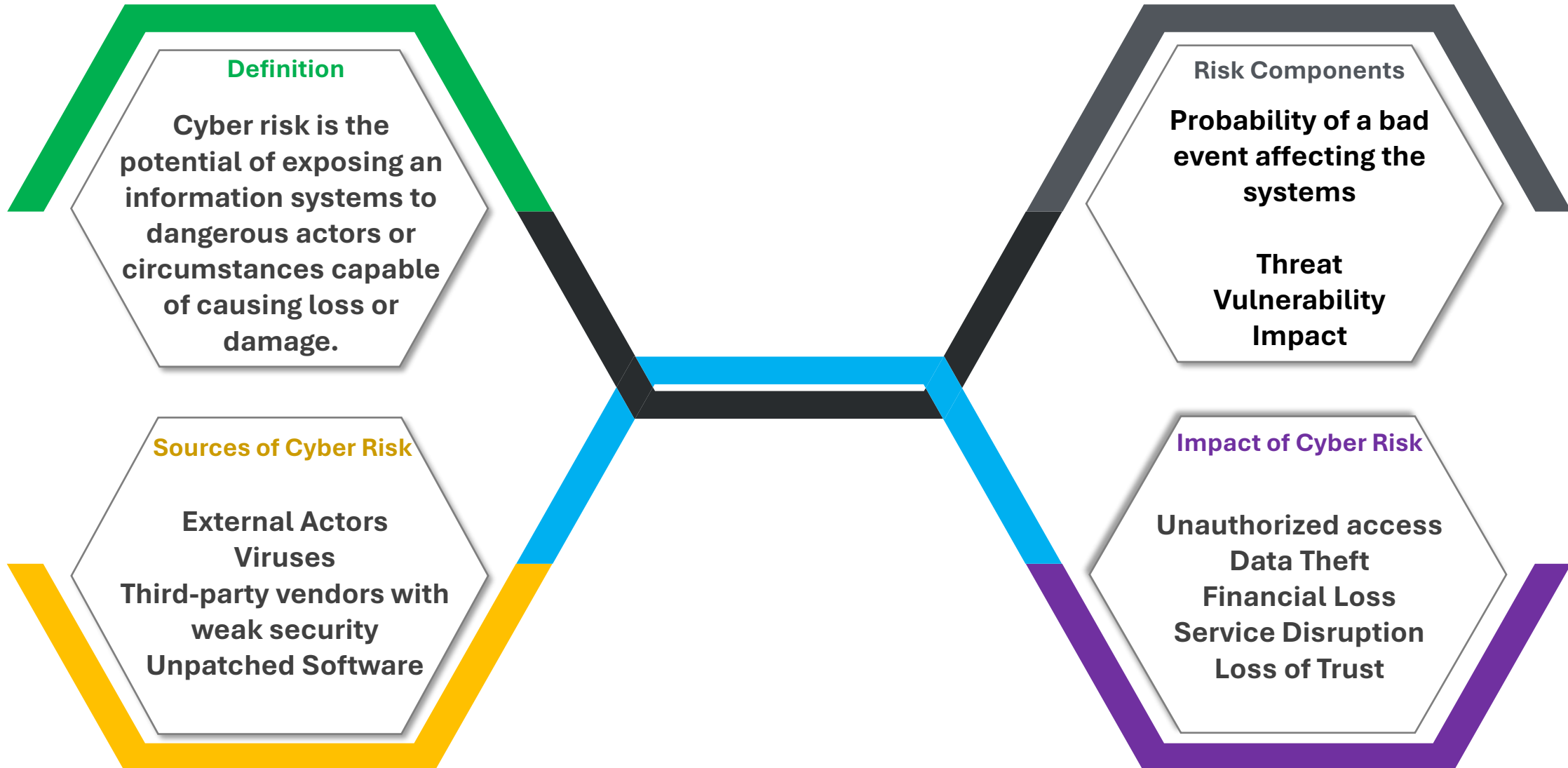
Machine Learning

- Learns normal vs. abnormal behaviour
- Used for fraud detection, Intrusion detection, etc.

Deep Learning

- Used to learn complex patterns
- Like in image recognition, speech, deepfakes etc.

What is Cyber Risk?



Common Cyber Threats

Threat Categories

- **Phishing** – Tricking the users
- **Malware** – Malicious Software
- **Ransomware** – Data hostage
- **Credential Theft** – unauthorized acquisition of login information by malicious actors
- **Website defacement** – unauthorized actors breaches web server to alter website content

Risks in Indian Context:

- Fake bank SMS
- Fake government portals
- WhatsApp scam messages

WHAT IS MALWARE?

Malware is an executable binaries which is malicious in nature and to perform variety of malicious activities and harm cyber infrastructure.

- It is one of the most common cyber threats.
- It is a single term for any type of malicious software developed by cyber attackers, designed to steal data or destroy on a computer or network.
- It commonly spread through network vulnerabilities, downloads, or email attachments.

Are the Anti-virus software sufficient to protect us?

Records and monitor keystrokes typed on a computer keyboard.

Collects information about user without their knowledge

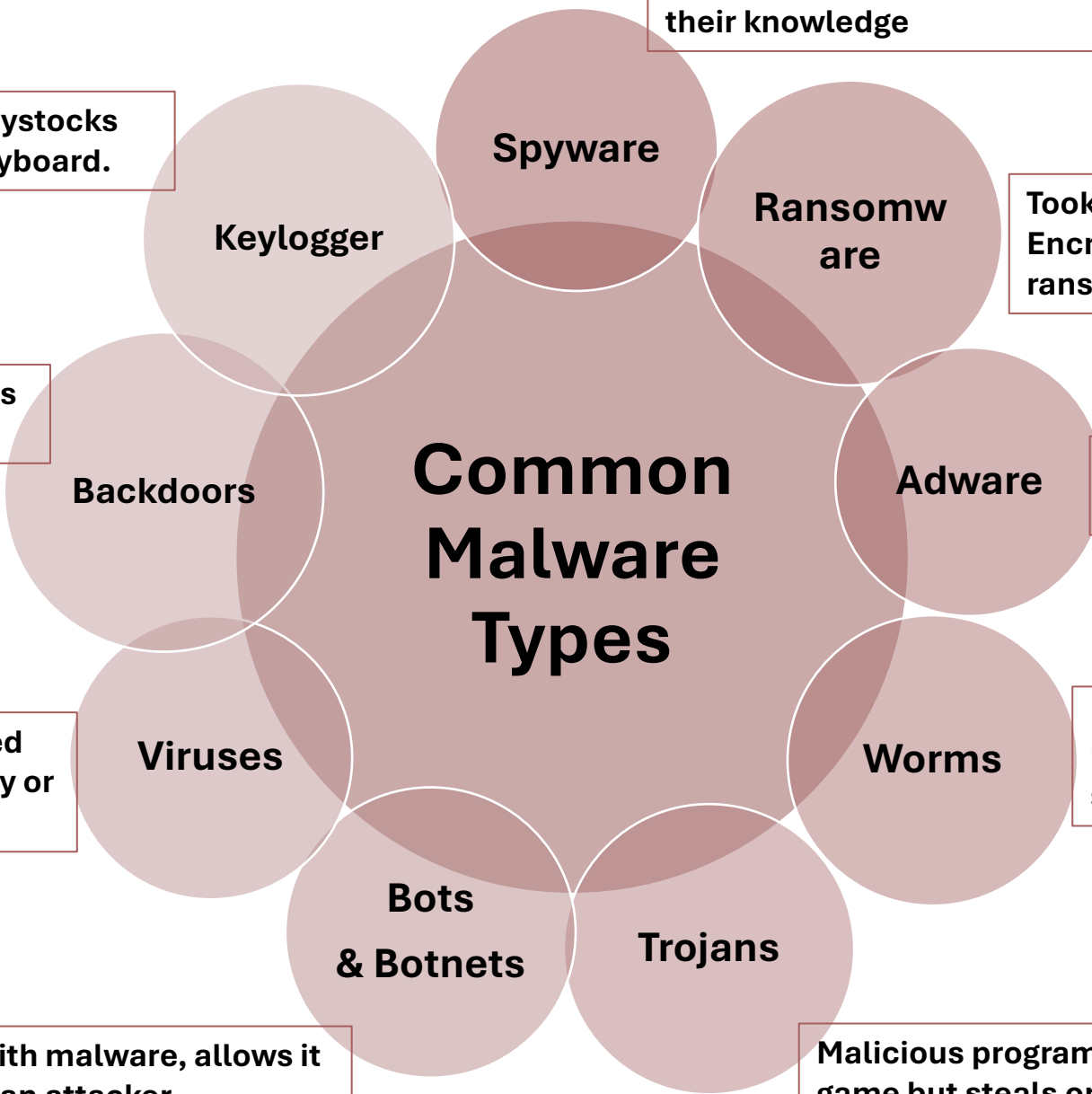
Took control of Computer & Encrypts data, user need to pay ransom to use data

Unwanted ads and pop-ups with malicious link to infect system.

Replicate themselves on system. Usually slow down network and spread very quickly over network

Malicious program that seems to be a game but steals or erase information.

Bot is a computer infected with malware, allows it to be remotely controlled by an attacker



Allows remote & unauthorized access of the computer to perform attack.

Malicious executable code attached with another executable file. Modify or delete data.

Backdoors

Adware

Worms

Trojans

Bots & Botnets

Viruses

Who is at Risk?

Individuals	Organizations	Government & Infrastructure
<ul style="list-style-type: none">• Bank Fraud• Identity Theft• Social media hijacking	<ul style="list-style-type: none">• Data breaches• Financial loss• Reputation damage	<ul style="list-style-type: none">• Power grids• Railways• Healthcare Systems

Cyber risk affects national stability

Key Vulnerabilities

- **Critical Infrastructure:** Energy, healthcare, and government sectors are primary targets.
- **Cloud and IoT:** Expanding digital footprints, including cloud misconfigurations and unsecured IoT devices, are providing larger attack surfaces.
- **Skill Gaps:** A shortage of cybersecurity professionals weakens the ability of organizations to defend against complex, automated attacks.

Traditional Cybersecurity – It's Limitations

Traditional Security Relies on:

- Known attack signatures
- Manual Analysis
- Static rules

Limitations:

- Not able to detect new attacks
- Response is slow
- High false alerts

Key Vulnerabilities & Targets

Threat Categories

- **Phishing** – Tricking the users
- **Malware** – Malicious Software
- **Ransomware** – Data hostage
- **Credential Theft** – unauthorized acquisition of login information by malicious actors
- **Website defacement** – unauthorized actors breaches web server to alter website content

Risks in Indian Context:

- Fake bank SMS
- Fake government portals
- WhatsApp scam messages

Why AI is needed in Cybersecurity

- Real-time Threat Detection & Response
- Managing High Volume of Data
- Proactive Defense (Predictive Analytics)
- Automated Routine Tasks
- Behavioral Analysis for Insider Threats
- Combating Sophisticated Malware

Learns Unknown Attack Patterns

Handles Massive Data Volumes

Operates Continuously

Reduce Human Workload

AI in Fraud Detection

AI in Fraud Detection uses machine learning and predictive analytics to analyse large datasets in real-time, identifying anomalies and behavioural patterns, which indicate fraudulent activity.

- AI learns normal transaction behaviour, and flags deviations, such as:
 - Unusual location
 - Abnormal time
 - Unusual amount
- Banks use AI to monitor:
 - UPI Transactions
 - Credit cards
 - Net banking

Applications

AI in Email & Message Security

Analyses:

- Language patterns
- URLs
- Sender behaviour

Helps to find:

- Fake GST emails
- Fake income tax notices
- Fake courier messages

AI in Network & System Monitoring

Monitors:

- Login behaviour
- File access patterns
- Network traffic

Detects:

- Insider threats
- Compromised accounts
- Malware movement

AI is also Used by Attackers

Artificial Intelligence itself is neither good nor bad. It is a tool, and like any other tool, it can be misused.

AI learns patterns, Attackers use the same learning ability to:

- Study victim behaviour
- Identify weaknesses
- Adapt attacks automatically

Why Attackers are attracted to AI:

- Low skill requirement
- Automated execution
- Thousands or millions of targets

AI-Powered Attacks

Phishing Attack:

- Uses perfect grammar
- Personalized content
- Context-aware messages

Example:

Phishing Email mentioning:

- Aadhaar
- PAN
- Bank KYC
- Scholarship or subsidy

Deepfakes & Voice Cloning:

- AI-generated:
- Fake Video
- Fake audio
- Fake images

Risks:

- Fake political speeches
- Fake celebrity endorsements
- Fake official instructions

Emerging Cyber Risk Landscape

- Attacks are faster
- Attacks are smarter
- Attacks are harder to attribute

High Risk Sectors:

- Banking & Finance
- Healthcare
- Power & Energy
- Smart cities
- Defence & Space

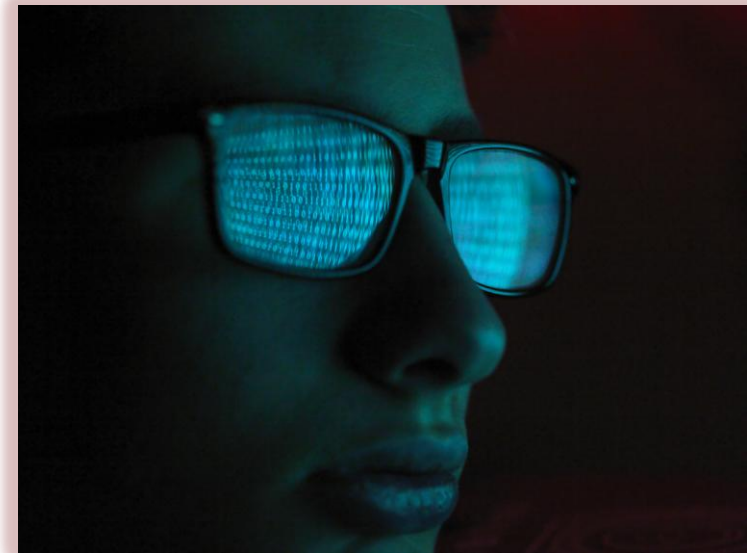


Needs for AI in Cyber Security

- In cybersecurity, AI refers to utilizing computational algorithms and advanced machine learning techniques to analyze, detect, and respond to cyber threats.
- AI in cybersecurity involves the development of intelligent systems that can autonomously or semi-autonomously identify patterns, anomalies, and potential risks within vast amounts of data.

ADVANCED THREAT DETECTION

- AI algorithms can be used to analyze vast amounts of data in real-time to detect patterns, anomalies, and potential threats that might evade traditional signature-based detection systems
- This enables early identification of sophisticated and previously unknown threats.



BEHAVIORAL ANALYSIS

- AI-based systems employ behavioural analytics to understand typical user behaviour, network activities, and system operations
- They can detect deviations from these norms, signalling potential security breaches or malicious activities



AUTOMATED INCIDENT RESPONSE

- AI enables automated incident response by swiftly identifying and mitigating security incidents
- It can take immediate actions to contain threats, isolate compromised systems, or apply remediation measures, reducing the response time and minimizing damage



PREDICTIVE ANALYSIS

- AI can forecast potential security risks based on historical data, trends, and emerging threat intelligence
- This proactive approach allows organizations to preemptively fortify their defenses against future threats



AUGMENTING HUMAN DECISION-MAKING

- AI does not replace human analysts but assists them by providing insights, recommendations, and context
- It helps security professionals make informed decisions faster and more accurately.



Mitigation Strategies

What Individuals can do

- Verify before trusting
- Avoid urgency-based requests
- Use strong passwords
- Enable two-factor authentication
- Stay informed


National-Level Approach

- Cyber awareness at scale
- AI governance frameworks
- Skilled cybersecurity workforce
- Public-private partnerships

What Organizations must do


- Deploy AI-based security solutions
- Employee awareness training
- Incident response planning
- Human AI collaboration

In the age of Artificial Intelligence, cybersecurity is not only about protecting systems — it is about protecting people, trust, and the nation.

Call  **1930** (Helpline number)

to register any complaint about cybercrime.



You can also file your complaint  online through **www.cybercrime.gov.in**

You can also file your complaint at the **nearest police station**





www.isea.gov.in

staysafeonline.in



ISEA Whatsapp Number for Incident Reporting

+91 9490771800



Join our WhatsApp and Telegram Channel at
ISEA - Digital Naagrik



To Share Tips / Latest News, mail us to
isea@cdac.in



[c/InformationSecurityAwareness](https://www.youtube.com/channel/UCInformationSecurityAwareness)



[/company/information-security-awareness/](https://www.linkedin.com/company/information-security-awareness/)



[/infosecawareness/](https://www.facebook.com/infosecawareness/)



[/InfoSecAwa](https://www.x.com/InfoSecAwa)



[/infosec_awareness/](https://www.instagram.com/infosec_awareness/)



[/Informationsecuritytips/](https://www.pinterest.com/Informationsecuritytips/)