एनआईसी National Informatics Centre

CYBERSECURITY IN THE AGE OF ARTIFICIAL INTELLIGENCE:

SAFEGUARDING INDIA'S DIGITAL FRONTLINE

Deepfake Voice Scam
Attackers copy someone's voice (like your boss) using AI and call to ask for money or data.

Fake Videos (Deepfakes)
AI makes fake videos of leaders or staff saying false things.

Smart Phishing Emails
AI writes realistic, personalized scam emails that look genuine.

AI-made Malware
Hackers use AI to create new virus versions that avoid antivirus tools.

AI Finds Software Bugs
Attackers use AI to find weaknesses in apps faster than humans.

Fake Social Media Posts
Hackers use AI to create new virus versions that avoid antivirus tools.

AI Password Guessing
AI guesses passwords based on your online info (name, birthday, etc.).

AI-driven Ransomware
AI helps ransomware pick the most valuable files to lock and demand more money.

OPERATION SINDOOR

Operation Sindoor showed that while our brave defense personnel protected physical borders, cyberspace relied on the right tools and technology to counter AI-generated images and videos spreading misinformation.

Defending the truth required continuous innovation, smart solutions, and close collaboration to keep public perception grounded.

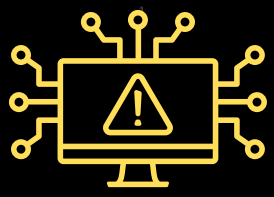
In today's world, wars are not only fought on land, air, and sea — but also in the cloud.

The New Threat Landscape

AI, DEEPFAKES, AND CYBER WARFARE – THE EMERGING FRONT

WORMGPT

The dark twin of ChatGPT, built to weaponize words into cyberattacks.



Over **1.3 million cyber incidents** were reported to CERT-In in the last year

A **25% rise in attacks** on critical infrastructure and defence-linked systems

AI-assisted **phishing and impersonation attempts** have grown fivefold in 2024–25

Hackers evolve with AI — so must our defenses.

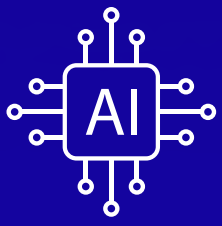
WHEN AI HELPS IN DEFENDING TOO

Threat Detection

How AI works: Uses machine learning models to analyze network traffic and system logs, learning what “normal” behavior looks like.

Phishing & Malware Identification

How AI works: Uses natural language processing (NLP) and pattern recognition to scan emails, URLs, and attachments for suspicious content.



Automated Incident Response

How AI works: Uses real-time event correlation and decision models to automatically respond to attacks.

User Behavior Analytics (UBA)

How AI works: Uses behavioral profiling and anomaly detection to track normal user actions and alert on deviations.

Predictive Defense

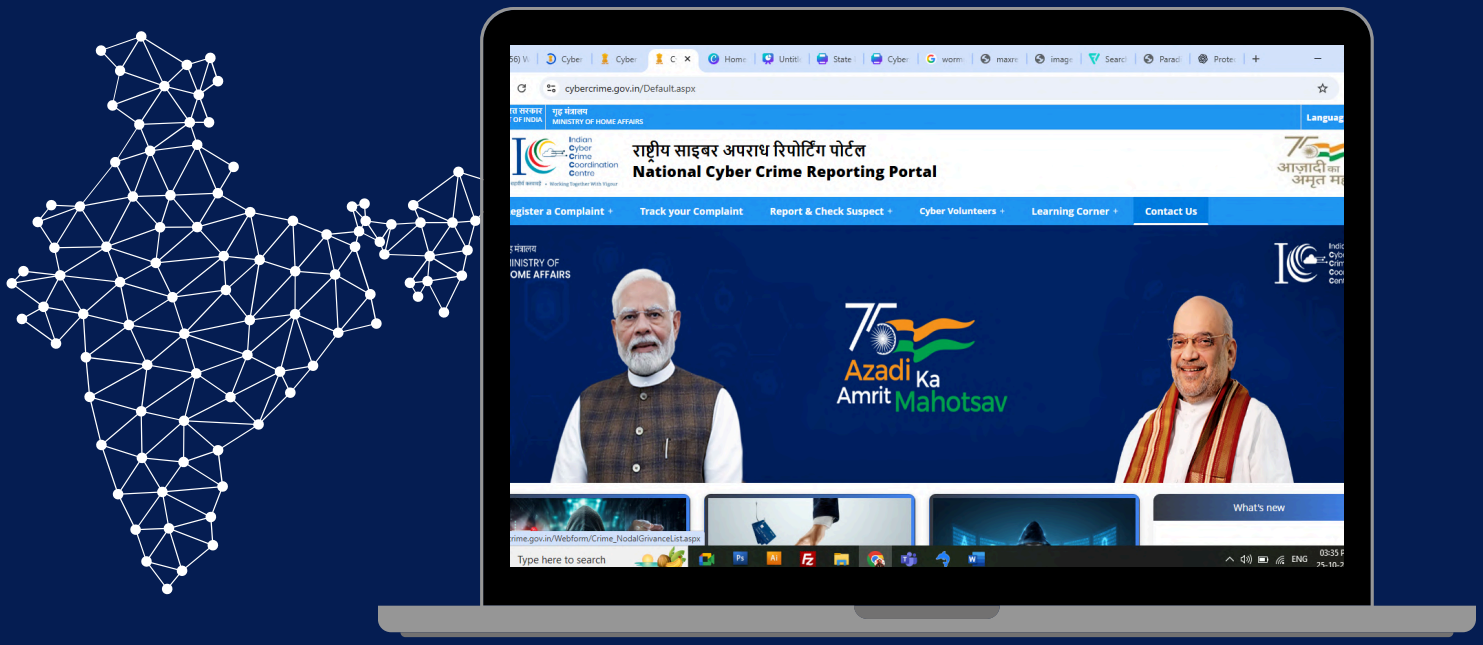
How AI works: Uses predictive modeling and threat intelligence analysis to anticipate attacks based on past incidents and global trends.

NIC एनआईसी National Informatics Centre

India's Response and the Way Forward

SECURING INDIA'S DIGITAL SOVEREIGNTY

https://cybercrime.gov.in



1930
Cyber Crime Helpline

112
National police helpline number

181
National women helpline number

certin
Enhancing Cyber Security in India

सत्यमेव जयते
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Stay Vigilant, Stay Secure