CANONSPHERE LAW REVIEW

ISSN: 3107-460X (Online)

CANONSPHERE LAW REVIEW

Volume 1 Issue 3

July to September, 2025

TABLE OF CONTENTS

Exploring the Impact of Artificial Intelligence in Combating Cybercrime: A Comparative Analysis of India and the Global Context

This long article is written by Divyansh Verma, M.A., Criminology and Criminal Justice Administration, Faculty of Art, Lucknow University of Lucknow, UP, India & Neeraj Kumar, LL.M. (Law), Faculty of Law, BBA University (A Central University) Lucknow, UP, India,

Abstract

The rapid expansion of digital technologies has created both opportunities and challenges, particularly in the realm of cybersecurity. As cybercrime evolves in complexity and scale, traditional methods of defense have proven insufficient to counter emerging threats such as phishing, ransomware, and large-scale network intrusions. This study explores how advanced technological tools are being adopted to strengthen cybercrime prevention and investigation, with a particular focus on comparing India's progress with global practices. While many developed nations have integrated sophisticated solutions into government and private-sector systems, India's adoption has been slower, hindered by infrastructural constraints, regulatory uncertainty, and limited technical expertise. Nevertheless, recent initiatives-ranging from policy reforms to the establishment of dedicated cybercrime units-highlight growing recognition of the need for stronger defenses. The research identifies a key gap: global literature provides extensive insights into large-scale implementation and operational successes, yet little work examines how these strategies can be adapted to the Indian context. This comparative approach aims to highlight differences in adoption, analyze the challenges unique to India, and suggest ways to integrate international best practices into local frameworks. Ultimately, the study contributes to bridging the divide between conceptual discussions and practical enforcement, offering insights that are crucial for policymakers, law enforcement agencies, and technology developers alike. By situating India within a broader global context, the research underscores the importance of building context-specific strategies that combine technological innovation with legal, institutional, and social considerations.

Keywords: Cybercrime, Digital Security, Comparative Study, Law Enforcement, Policy Framework

Introduction

The digital revolution has transformed every sphere of life, from communication and commerce to governance and national security. Alongside these benefits, however, cybercrime has emerged as one of the most pressing challenges of the twenty-first century. Offences ranging from identity theft, phishing, and ransomware attacks to complex threats against critical infrastructure have exposed the vulnerabilities of interconnected systems. As cybercriminals continue to refine their methods, relying solely on conventional defense measures is no longer sufficient. This has created a growing demand for innovative technological responses capable of detecting, preventing, and mitigating such risks with greater efficiency.

Globally, advanced tools have already begun to play a central role in digital defense. In regions such as North America, Europe, and parts of East Asia, governments and private organizations have integrated automated monitoring, predictive analytics, and enhanced digital forensics into their cybersecurity frameworks. These measures not only strengthen protection but also allow quicker responses to attacks, minimizing financial and reputational damage. In contrast, India's progress has been more uneven. While major financial institutions and technology firms have adopted advanced defense mechanisms, the broader ecosystem continues to rely heavily on traditional tools. Factors such as insufficient technical infrastructure, limited skilled manpower, and regulatory uncertainty have slowed adoption across the country. At the same time, cybercrime in India has grown rapidly, affecting individuals, businesses, and government institutions alike.

The central aim of this research is to conduct a comparative analysis of how advanced digital tools are being used to combat cybercrime in India and across the global context. By highlighting differences in adoption, assessing challenges, and identifying opportunities for improvement, the study seeks to provide insights that will guide policymakers, law enforcement agencies, and industry leaders in strengthening cyber resilience.

Historical Background

Cybercrime developed alongside the growth of digital technology. In its initial stages, it involved only minor intrusions, such as breaking into computer systems without permission or releasing primitive forms of malicious software. With the expansion of the internet in the 1990s, new forms of digital misconduct emerged, including online fraud, identity theft, and

the first wave of large-scale hacking incidents. Governments across the world began enacting legislation-such as the United States' CFA Act (1986) and the United Kingdom's CM Act (1990)-to address these growing concerns.

In India, the IT Act of 2000 became the first comprehensive framework to define and regulate offences committed through digital means. Over time, amendments were introduced to address data breaches, cyber terrorism, and financial fraud. Despite these efforts, rapid advances in technology have consistently outpaced the capacity of legal and institutional frameworks to respond effectively.

Globally, nations have increasingly turned toward advanced technological tools for protection, incorporating automated detection, predictive analysis, and digital forensics into cybersecurity. In India, however, the adoption of such measures has been slower, with much of the focus still on policy development and conceptual frameworks rather than widespread implementation.

Statement of Problem

Cyber-crime has expanded in scale and sophistication, outpacing traditional defense mechanisms and posing serious risks to individuals, businesses, and governments. While advanced technological tools have been widely integrated into global cybersecurity frameworks, India's adoption remains limited and uneven. Challenges such as inadequate infrastructure, shortage of skilled professionals, and regulatory uncertainties hinder effective implementation. Existing literature often highlights global progress but provides little comparative insight into India's position. This gap creates the need for a focused study examining how India can adapt international best practices while addressing its own socio-legal and institutional realities.

Objectives of the Research

1. **To examine the evolution and current trends of cybercrime** and assess the limitations of traditional defense mechanisms in addressing emerging threats.
2. **To analyze global practices in combating cybercrime**, focusing on the integration of advanced technological tools within government, corporate, and law enforcement frameworks.
3. **To evaluate India's existing approach** to cybercrime prevention and investigation, with attention to legal frameworks, institutional capacity, and technological adoption.

4. **To conduct a comparative analysis** between India and selected global contexts in order to identify similarities, differences, and areas of improvement in cyber defense strategies.
5. **To propose context-specific recommendations** that connection the break between conceptual research and practical implementation, strengthening India's cybersecurity framework while drawing lessons from global best practices.

Research Methodology

This study assumes a qualitative and comparative research design to study the role of advanced technological tools in combating cybercrime, with a particular focus on India in relation to global practices. The methodology combines doctrinal legal research, policy analysis, and a review of secondary data to provide a comprehensive perspective.

- **Data Collection:** The research relies primarily on secondary sources, with books, peer-reviewed journal, articles, conference proceedings, government reports, and international policy documents. These materials provide insights into both theoretical debates and practical applications of technology in cybersecurity.
- **Comparative Approach:** A cross-jurisdictional analysis is conducted to evaluate how advanced tools have been adopted in different regions, such as North America, Europe, and East Asia, and how these experiences differ from India's evolving framework. This method helps identify best practices, gaps, and opportunities for adaptation.
- **Legal and Policy Analysis:** The study examines Indian laws such as the IT Act, 2000, the BNS, 2023, and international frameworks like the U.S. CFAB Act and the U.K. CM Act. This enables a structured understanding of how law and technology interact in combating cybercrime.
- **Outcome:** The methodology is designed to generate critical insights that bridge global perspectives with India's unique socio-legal context, ultimately offering recommendations for more effective policy and enforcement mechanisms.

Meaning of AI

AI refers to the ability of machinery or computer systems to perform responsibilities that usually need human intelligence. Instead of relying solely on human thought, these systems are designed to learn, and make conclusions on their own.

The term AI was first introduced by John McCarthy, a Stanford professor, who explained it as the study and development of machines capable of behaving intelligently. In simple words, AI is about building systems that can think, adapt, and solve problems much like humans do, but through technology.[1]

The Evolution of AI

From its early days in the mid-Twentieth century, AI has gone through waves of optimism and disappointment. Despite bold claims in the 1950s and 1960s that machines comparable to the human brain were imminent, progress was slower than expected. Periods of stagnation, known as AI winters, followed.

A major breakthrough came around 2012 with the deep learning revolution, which reignited research and practical applications. Today, interest in AI is higher than ever, especially with the rise of generative AI, capable of producing text, images, and audio that closely resemble human creations. However, while impressive, these systems still fall under narrow AI-they do not "understand" their outputs and remain far from the realms of AGI or self-aware AI.

Types of AI[2]

Experts generally divide AI into four major categories depending on how advanced their functions are:

1. **Reactive AI**

   The earliest and simplest form of AI is reactive in nature. These systems can only respond to the information they have in the present moment; they don't "remember" past interactions or learn from them. Their strength lies in processing

[1] John McCarthy, What Is AI? STAN. U. (Nov. 12, 2007), http://www-formal.stanford.edu/jmc/whatisai/ (last visited on Sep. 10, 2015 at 02:02 AM)
[2] Understanding the Different Types of AI," IBM Data and AI Team, IBM (Oct. 12, 2023), https://www.ibm.com/think/topics/artificial-intelligence-types (last visited on Sep. 10, 2015 at 02:02 AM)

large amounts of data quickly and producing accurate outputs, but they lack the ability to adapt beyond what they are designed for.

A famous example is IBM's Deep Blue, which conquered world chess champion Garry Kasparov in 1997. In addition, today's spam filters, recommendation systems, and some basic machine learning models also fall under this category. Although powerful in specific contexts, reactive AI remains limited because most real-life situations demand more than simple reaction — they require anticipation, prediction, and reasoning, areas where humans still outperform machines.

2. Limited Memory AI

To overcome the rigidity of purely reactive systems, researchers created AI that can temporarily use stored data from past experiences. This advancement led to what we now call limited memory AI.

The rise of deep learning in the early 2010s was a turning point. By mimicking the building of the human mind through artificial neural networks, AI began to "learn" and improve as it processed more data. This allowed machines to excel at responsibilities such as image, acknowledgement, language processing, and complex decision-making.

A striking example is Google's AlphaStar, which understood the real-time plan game Star-Craft II by learning from repeated self-play and developing new strategies. Similarly, autonomous vehicles rely on limited memory AI to anticipate the movement of nearby cars and pedestrians. Despite this progress, such systems still depend heavily on massive datasets and struggle when exposed to unfamiliar conditions, unlike humans who can adapt with limited information.

3. Theory of Mind AI

The next level of AI, still under development, is called theory of mind AI. The concept comes from psychology, where it refers to the ability to understand that others have their own emotions, beliefs, and intentions. If machines could achieve this, they would be able to interpret and respond to human states of mind in a much deeper way.

Current efforts in emotion AI-which tries to detect and react to human feelings through speech, facial terminologies, or body Expression-are only the beginning. True theory of mind AI would go far beyond detecting moods; it would actually comprehend motives and adjust its behaviour accordingly. This remains one of the

biggest challenges, since AI today can generate art, text, or music without any genuine "understanding" of what it has created.

4. **Self-Aware AI**

The most advanced and speculative form of AI would be self-aware systems-machines with consciousness, emotions, and an understanding of themselves and others. In theory, such AI could think independently, set its own goals, and even express desires or needs similar to humans.

At present, this level of AI is more science fiction than science. We neither possess the algorithms nor the computing power to build machines with true self-awareness. Whether achieving such a state is even possible depends on unlocking mysteries of the human brain that remain unsolved today.

Broader Classifications of AI

Apart from functionality-based categories, AI is also often grouped into three broad levels of capability:

1. **Narrow AI (Weak AI):** The most joint form of AI we see today. It is highly specialized, planned to excel at one exact task-such as language translation, virtual assistants like Siri or Alexa, and recommendation algorithms. While efficient, it lacks general intelligence.

2. **AGI:** Sometimes denoted as strong AI, this remains a goal rather than a reality. AGI would be able to learn, understand, and apply knowledge across multiple domains, much like a human being.

3. **Artificial Superintelligence (ASI):** A hypothetical stage where AI surpasses human intelligence entirely, excelling at problem-solving, creativity, and decision-making. ASI would not only match but exceed human capacity in virtually every field, raising both exciting possibilities and profound ethical concerns.

The Process of Artificial Intelligence

Artificial Intelligence works by imitating human abilities and transferring those traits into machines. Instead of simply running commands, AI follows a cycle that allows it to learn, adapt, and improve. The process generally unfolds in the following stages:[3]

1. **Collecting Inputs**

   AI begins with data. This can be anything from text, images, sound, video, or even signals from sensors. The value and type of input play a major character in how well the system will perform, since better data leads to more accurate results.

2. **Processing the Data**

   Once the data is gathered, the system applies algorithms to interpret and analyze it. These algorithms may include methods like, machine knowledge, deep learning, natural verbal processing, or computer idea. Through techniques such as prediction, classification, clustering, or pattern matching, AI makes sense of the input.

3. **Producing Results**

   After processing, the system delivers an output. The nature of this output depends on the task-ranging from forecasts and recommendations to automated actions or generated content. Since AI adapts to different goals, the results can vary from simple categorizations to complex insights.

4. **Learning and Adjusting**

   A key feature of AI is its capability to progress over time. By learning from mistakes, analysing new data, and incorporating user feedback, the system refines its models and decision-making. This may involve retraining algorithms, fine-tuning processes, or updating rules for better performance.

5. **Evaluating Performance**

[3] How Does AI Work?, GeeksforGeeks (last updated Aug. 6, 2025), https://www.geeksforgeeks.org/artificial-intelligence/how-does-ai-work/. . (last visited on Sep. 10, 2015 at 03:02 AM)

Finally, AI systems are assessed to ensure they work reliably and fairly. This involves measuring accuracy, precision, efficiency, transparency, and even ethical considerations. Regular evaluation helps build trust and ensures that the technology serves its purpose responsibly.

Challenges of Artificial Intelligence

Artificial Intelligence has become deeply integrated into modern life, making its role in technology and governance almost unavoidable. Yet, despite its transformative potential, AI development and adoption face several pressing challenges:

1. **Bias Under Algorithms:** Since AI systems learn from data, they often inherit the same prejudices present in the datasets. This can lead to biased or unfair outcomes, particularly under sensitive ranges such as recruitment, policing, or financial services.[4]

2. **Complexity of Integration:** Implementing AI across industries is not straightforward. Organizations often struggle with the cost of infrastructure, the shortage of skilled professionals, and the difficulty of adapting existing systems to work with AI-driven models.[5]

3. **Security Concerns:** AI technologies themselves can become targets for cyberattacks. Malicious actors may manipulate algorithms, steal sensitive datasets, or exploit system vulnerabilities, raising the risk of large-scale breaches.[6]

4. Unreliable Outputs: AI predictions and decisions are not always consistent. When models encounter incomplete, misleading, or unfamiliar data, the results may be inaccurate-potentially leading to harmful real-world consequences.[7]

[4] S. Barocas, M. Hardt & A. Narayanan, Fairness in Machine Learning (2019), https://fairmlbook.org/. (last visited on Sep. 10, 2015 at 04:02 AM)
[5] Thomas H.D. & R. Ronanki, AI for the Real World, Harv. Bus. Rev., Jan.–Feb. 2018, at 108.
[6] M. Brundage et al., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (2018).
[7] S. Russell & P. Norvig, AI: A Modern Approach 4th ed. (2020).

The Concept of Cybercrimes

Meaning of Cybercrime

Cybercrime refers, to unlawful actions carried out through computers, digital networks, or the internet. In some cases, technology is used, as a instrument to commit the offense; in others, it becomes very target of the attack. Artificial Intelligence systems themselves are increasingly vulnerable to such exploitation.[8]

Categories of Cybercrimes

A. **Crimes Against Individuals:** Ordinary users are often the easiest victims of online offenses, which can take many forms:
   I. **Cyberstalking:** Persistent online harassment or tracking through emails, text messages, or social media platforms.[9]
   II. **Cyber Defamation:** Spreading defamatory or damaging statements about an individual through digital channels.[10]

B. **Crimes Against Property:** Here, the target is not a person but digital assets such as computers, networks, and intellectual property. Examples include:
   I. **Intellectual Property Infringement:** Violations such as software piracy, patent breaches, or trademark misuse.
   II. **Cyber Vandalism:** Intentional destruction or disruption of data, often resulting in service outages or damaged systems.

C. **Crimes Against Government:** When state systems or sensitive data are attacked, the risks escalate from financial loss to threats against national security:
   I. **Cyber Terrorism:** Disrupting or damaging government websites, portals, or digital infrastructure to cause panic or instability.[11]
   II. **Unauthorized Access to Information:** Obtaining confidential or classified material for political, military, or ideological purposes.[12]

[8] S. W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (2010).
[9] BNS, No. 45 of 2023, § 78(1)(ii).
[10] BNS, No. 45 of 2023, § 356.
[11] IT Act, No. 21 of 2000, § 66F.
[12] *Ibid Sec. 43*
- Section 66 states that if someone gains unauthorized access to a computer system with dishonest or fraudulent intent, it becomes a criminal offense and is punishable under the law.

A notable case ***is RVS Mani*** v. ***Union of India***[13], where the issue of foreign cyberattacks on Indian government databases was examined. The court emphasized the status of strict safeguards U/S 66F of the IT Act, 2000, which criminalizes cyber terrorism and related offenses.6

In Indian Cyber Laws and Policies

1. **IT Act, 2000 (IT Act)**

The IT Act primarily governs electronic transactions, e-commerce, and cybercrimes. Notable provisions include:

- **Section 65**: Anyone who deliberately hides, destroys, or changes computer source code, that is lawfully required to be preserved can face punishment. The penalty may consist of incarceration of up to 3 years, and fine of up to 2 lakh rupees, or both.
- **Section 66**: Anyone who fraudulently commits the acts listed under Section 43 can be punished with up to 3 years in jail, and fine of up to 5 lakh rupees, or both.

Addresses computer-related Crimes, such as hacking, identity theft, and cyber fraud.

- **Section 70**: Prohibits unauthorized entry to protected systems.
- **Section 72**: Deals with the breach of concealment and disclosure by opening electronic records without consent.

The Act also empowers Cyber Appellate Tribunals, to hear appeals against decisions made by Adjudicating Officers in cybercrime cases.

2. **NCS Policy, 2013**

This policy goals to make a safe cyber ecosystem by:

- Defending cyberspace, developing a harmless cyber environment.
- Cooperating with businesses, stakeholders to spread cybersecurity awareness.

[13] 1956 A.I.R. 108 (S.C. India); 1955 S.C.R. (2) 983 (India).

- Implementing cybersecurity solutions, conducting regular drills to assess security posture.[14]

3. **DPDP Act, 2023**

Passed to protect individuals' digital individual data, this Act:

- Recognizes the right of persons to protect their special data.
- Allows processing of such data for lawful purposes.
- Establishes guidelines for data processing, consent, and breach notifications.[15]

4. BNS, 2023

Replacing the Indian Penal Code, this legislation includes provisions addressing cybercrimes:

- **Section 366**: Anyone who creates a fake document or electronic record with the intent to cheat, harm someone, claim property, or commit fraud is guilty of forgery.
- **Section 75**: Addresses sexual harassment, including showing pornography against the will of a woman.
- **Section 78**: Deals with stalking, including monitoring of the use of the internet and online movements by a woman.

***State of TN* vs. *Suhas Katti*[16]:** This landmark case marked the first conviction under the IT Act for cyber harassment. The defendant created a fake email version in the victim's name and posted indecent and defamatory content. The court convicted the accused U/S 67 of the IT Act and U/S's 469 and 509 of the IPC. The case also validated the use of electronic evidence U/S 65B of the IE Act.[17]

[14] Ministry of Electronics & Info. Tech., NCS Policy (2013), https://www.meity.gov.in/sites/default/files/2024-02/NCS_policy-2013_0.pdf. (last visited on Sep. 10, 2015 at 05:02 AM)
[15] The DPDP Act, 2023 (No. 22 of 2023), Ministry of Electronics and IT (June 2024), www.meity.gov.in/static/uploads./2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf. (last visited on Sep. 10, 2015 at 05:02 AM)
[16] Additional Chief Metropolitan Magistrate's Court, Egmore, Chennai (India 2004).
[17] Suhas Katti v. Tamil Nadu, Wikipedia (Dec. 3, 2024), https://en.wikipedia.org/wiki/, Suhas_Katti_v._TN. (last visited Sept. 10, 2025 at 05:20 AM).

International Cyber Laws

A. United States

- **CFA Act. (1986)**: Addresses unauthorized access to computer systems, fraud, and related offenses.[18]

B. Philippines

- **Cybercrime Prevention Act (2012)**: Criminalizes offenses such as hacking, identity theft, cybersex, and libel committed through computer systems.[19]

C. United Kingdom

- **Computer Misuse Act (1990)**: It restricts any intrusion into computer systems, including access gained without permission, entry made to enable other criminal activities, and deliberate actions intended to disrupt or damage computer operations.

AI-Driven Cybersecurity Tools

1. Phishing Detection

Phishing attacks, where cyber criminals impersonate legitimate entities to steal sensitive information, are increasingly sophisticated. AI-powered solutions analyze email content, URLs, and sender behavior to classify potential phishing attempts. For instance, companies like Varonis have integrated AI-native email security technologies to detect phishing across various platforms, including email, SMS, and messaging apps like WhatsApp and Slack.[20]

[18] CFA Act, Wikipedia https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act. (last visited Sept. 10, 2025 at 06:20 AM).
[19] Republic Act No. 10175, CP Act of 2012, § [section number], (2012), available at https://www.icj.org/wp-content/uploads/2014/02/Philippines_Cybercrime-Prevention-Act-2012.pdf. (last visited Sept. 10, 2025 at 06:30 AM).
[20] Daniel Todd, Varonis Snaps Up AI Email Security Specialist SlashNext, ITPro (Sept. 4, 2025), https://www.itpro.com/business/acquisition/varonis-snaps-up-ai-email-security-specialist-slashnext. (last visited Sept. 10, 2025 at 06:30 AM).

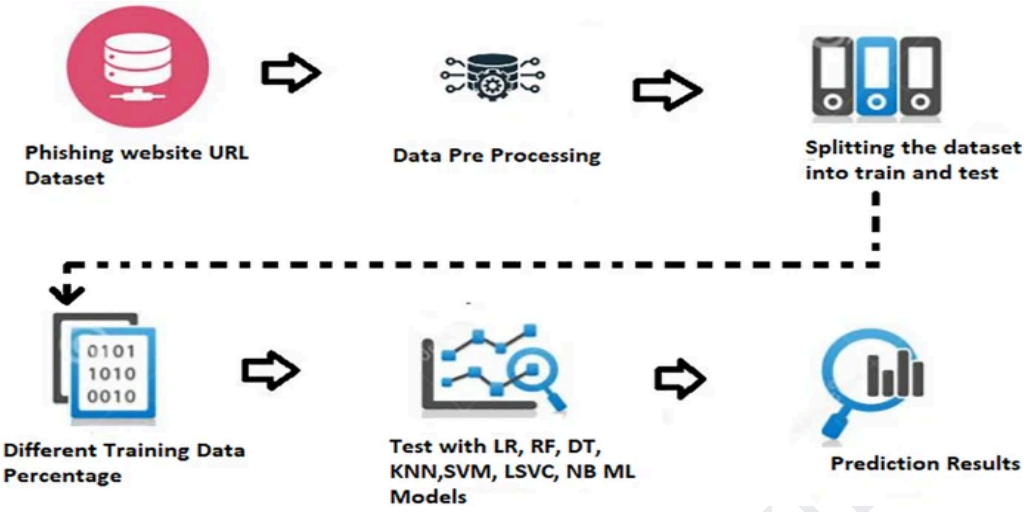

Figure 1: Phishing Detection Workflow- steps include dataset collection, preprocessing, splitting into training and testing, applying ML models, and obtaining prediction results.[21]

2. Threat Intelligence

AI enhances threat intelligence by systematizing the collection and scrutiny of data from multiple sources to detect emerging cyber threats. This practical approach allows organisations to anticipate and mitigate potential attacks before they occur.

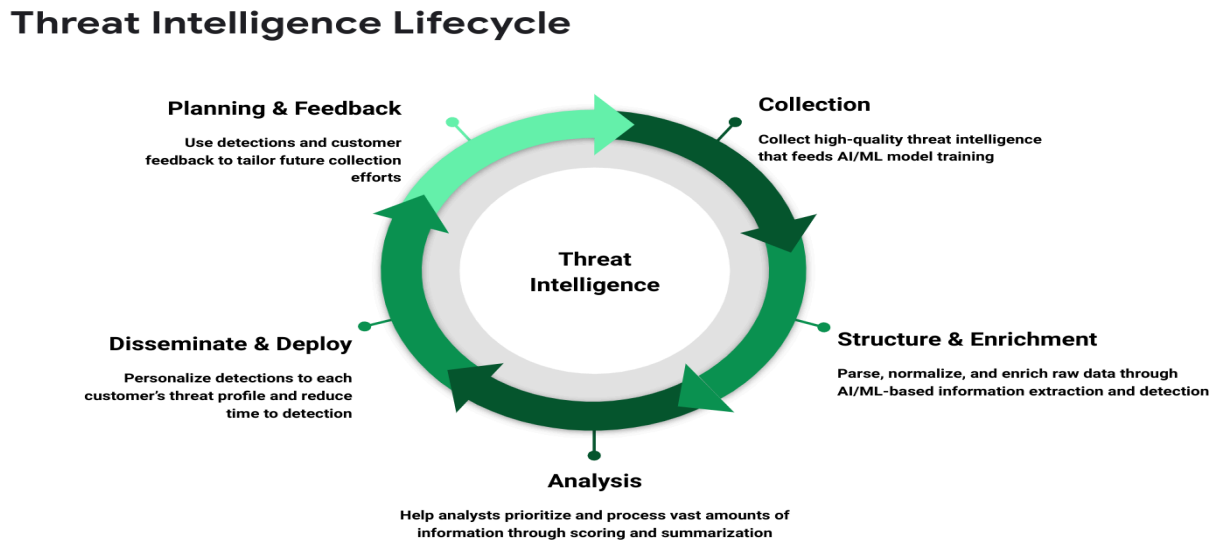

Figure 2: Threat Intelligence Lifecycle – stages include Collection, Structure & Enrichment, Analysis, Dissemination & Deployment, and Planning & Feedback.[22]

[21] Adapted from phishing detection and machine learning model frameworks.
[22] Adapted from cybersecurity threat intelligence frameworks.

3. Security Information and Event Management (SIEM)

AI-driven SIEM systems integrate (SIEM) to provide actual analysis of security alerts. These systems utilize machine learning to notice anomalies and potential threats, enabling swift responses to cyber incidents.

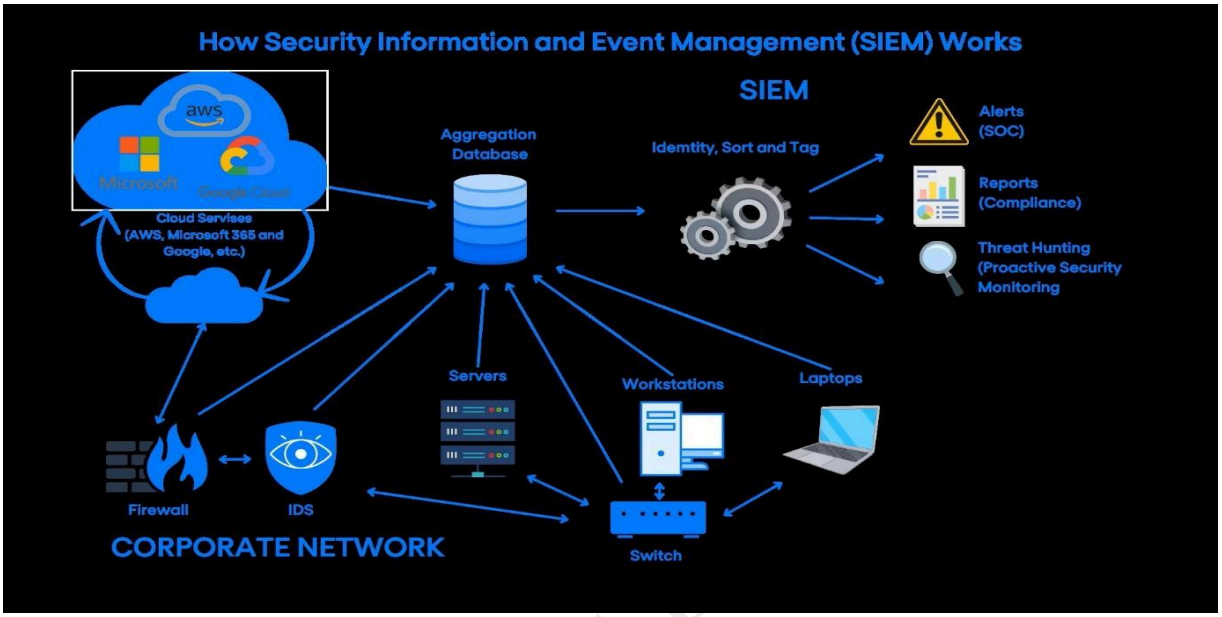

Figure 3: How Security Information and Event Management (SIEM) Works.[23]

In AI in Indian Cybersecurity

India is increasingly adopting AI to bolster its cybersecurity measures:

1. **Government Initiatives:** The Indian government is investing in AI technologies to enhance the capabilities of cybersecurity agencies.

2. **Private Sector Collaboration:** Indian tech companies are partnering with global AI firms to develop advanced cybersecurity solutions tailored to local needs.

3. **Educational Programs:** Institutions are offering specialized courses in AI and cybersecurity to build a skilled workforce capable of addressing emerging cyber threats.

[23] Adapted from cloud service providers (AWS, Microsoft 365, Google Cloud) and corporate network security models.

Global AI Cybersecurity Landscape

Internationally, AI is being utilized to combat cybercrimes:

1. **United States:** AI is employed in various sectors, including finance and healthcare, to detect and prevent cyber threats.

2. **European Union:** The EU is implementing AI regulations to ensure ethical use while enhancing cybersecurity measures.

3. **Asia-Pacific:** Countries in this region are investing in AI research and development to strengthen their cybersecurity frameworks.

Challenges

While AI offers significant advantages in cyber-security, it also presents challenges:

1. **Adversarial AI:** Cyber-criminals are utilizing AI to develop cultured attack strategies, such as AI-generated phishing emails that are increasingly difficult to detect.

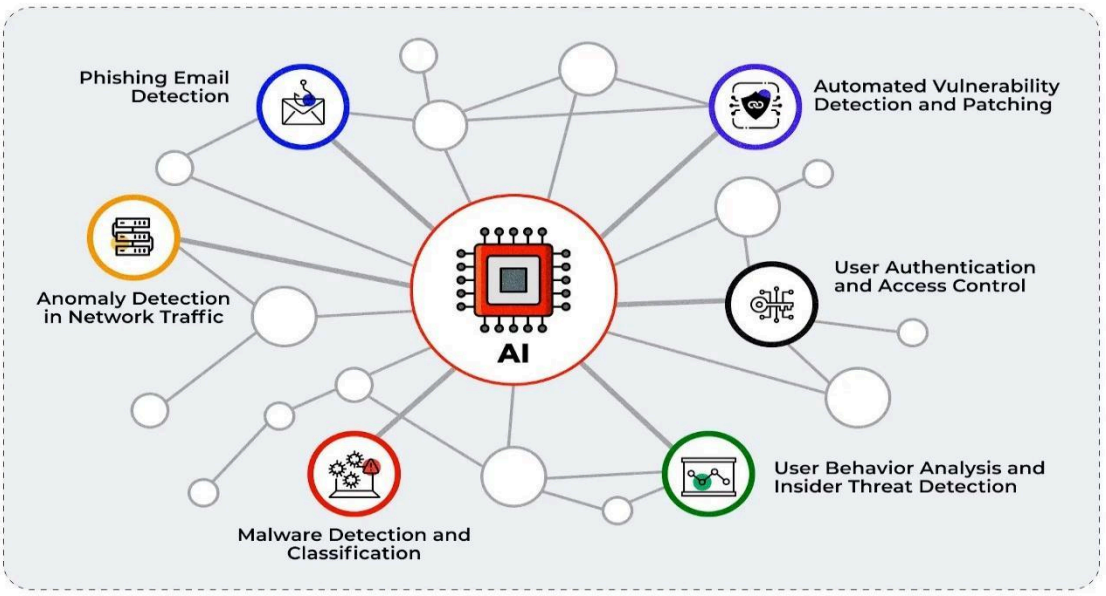

Figure 4: Applications of AI in Cybersecurity- including phishing detection, anomaly detection in network traffic, malware classification, automated vulnerability patching, user authentication, and insider threat detection.[24]

[24] Adapted from cybersecurity applications of intelligent systems.

2. **Data Privacy:** The use of AI in cyber-security increases concerns about data secrecy and the ethical implications of surveillance.

3. **Skill Gap:** There is a shortage of specialists with proficiency in both AI and cyber-security, hindering the effective implementation of AI-driven security solutions.

AI's Role in Preventing Cybercrime: A Comparative Analysis of India and Global Practices

In Indian Perspective

1. **Academic Insights on AI in Cybersecurity**

In 2012, researchers KD. N., Kumar M. A., and Kumar M. R. P. highlighted the importance of advanced cryptographic techniques, such as quantum channels, in enhancing cybersecurity measures. They emphasized that robust security protocols are essential to mitigate cyber threats effectively.[25]

2. **Strengthening Cybercrime Investigation Infrastructure**

Indian states have established dedicated Cyber Crime Cells within police departments. These units are staffed with trained professionals equipped with the latest technology to investigate and combat cybercrimes effectively.

3. **Role of CERT-In in Cybersecurity**

India's Computer Emergency Response Team (CERT-In), operating under the Ministry of Electronics and IT, serves as the country's key agency for safeguarding cyberspace. Created U/S 70B of the IT Act, 2000, its mandate is to handle cyber-security incidents and improve the resilience of national networks. In 2017, the agency introduced the Cyber Swachhta Kendra, also known as the Botnet Cleaning and Malware Analysis Centre. This program was designed as a public-focused

[25] Mahesh Chandra, Reduction of Cyber-Crimes by Effective Use of AI Techniques, 8 Int'l J. Recent Tech. & Eng. 8643, 8643–8648 (Nov. 2019), https://doi.org/10.35940/ijrte.D8566.118419. (last visited Sept. 10, 2025 at 011:30 AM).

initiative to alert users about malware and botnet infections while offering practical guidance for corrective measures.[26]

In April 2022, CERT-In introduced new rules requiring that any cyber incident be reported within 6 hours of being identified. The directive covers a wide range of stakeholders, such as internet and cloud service providers, data centers, technology firms, and government bodies.[27]

4. **Addressing Technical Challenges**

In July, 2024 CERT-In reported a significant issue related to a faulty update of the CrowdStrike Falcon Sensor software, which caused widespread problems with Microsoft Windows systems. This incident highlights the challenges in maintaining cybersecurity infrastructure and the importance of timely updates and patches.[28]

International Perspective

1. **United States: AI in Homeland Security**

The U.S. Department of Homeland Security (DHS) utilizes AI to advance its critical missions, defend against new threats from AI, and support the DHS workforce.[29]

2. **Israel: AI in Military Cyber Defence**

Israel has established a unified military AI command to enhance its cybersecurity capabilities. The (IDF) use AI to detect and prevent cyber-attacks on military networks. Machine learning algorithms analyse network data to classify possible threats in actual.[30]

3. **United Kingdom: AI in Crime Prevention**

The UK's National Crime Agency (NCA) employs AI to detect and prevent child misuse and internet fraud. Machine learning algorithms analyse data from

[26] Cyber, Swachhta Kendra, https://www.csk.gov.in (last visited Sept. 10, 2025 at 11:50 AM).
[27] Axel Sukianto, India's 6-Hour Data Breach Reporting Rule (Clearly Explained), UpGuard (Jan. 7, 2025), https://www.upguard.com/blog/indias-6-hour-data-breach-reporting-rule. (last visited Sept. 10, 2025 at 11:55 AM).
[28] CERT-In, Advisory CIAD-2024-0035: Outage of Microsoft Windows Due to CrowdStrike Agent Falcon Sensor Update, ORA Centre, AST (July 19, 2024), https://www.cert-in.org.in/advisory/CIAD-2024-0035. (last visited Sept. 11, 2025 at 12:01 AM).
[29] U.S. Dep't of Homeland Sec., Artificial Intelligence at DHS, https://www.dhs.gov/ai (last visited Sept. 11, 2025 at 01:07 PM).
[30] Israel Establishes a Unified Military AI Command, Cyber-Security Intelligence (Jan. 6, 2025), https://www.cyber-security intelligence.com/blog/israeli-establishes-a-unified-ai-military-command-8164.html. (last visited Sept. 11, 2025 at 01:09 PM).

several sources, such as social media and dark web forums, to classify possible threats and suspects.[31]

Artificial Intelligence and Cybersecurity

In the present digital era, where sensitive data is constantly being stored, shared, and processed online, the risk of cyber intrusions has grown significantly. Criminals exploit vulnerabilities in systems and networks to steal valuable information or disrupt services. The central aim of cyber-security is therefore to safeguard devices, networks, and online platforms from such malicious activities.

AI is now being increasingly deployed as a powerful tool in strengthening cybersecurity measures. Its role can be understood through two broad approaches:

AI Approaches in Cybersecurity

1. **Assisted Intelligence**

   This form of AI helps organizations carry out tasks that were once considered too complex or time-consuming. For instance, AI systems can quickly analyse big volumes of data to identify unusual activity patterns that may specify a potential breach.[32]

2. **Augmented Intelligence**

   Unlike fully autonomous systems, augmented intelligence works alongside human experts, enhancing their capability to detect and respond to threats. It refines existing security protocols rather than replacing human decision-making altogether.[33]

[31] NCA Issues Urgent Warning About 'Sextortion', (NCA) (Apr. 29, 2024), https://www.nationalcrimeagency.gov.uk/news/nca-issues-urgent-warning-about-sextortion. (last visited Sept. 12, 2025 at 02:09 PM).

[32] L. Craig, N. Laskowski & L. Tucci, What Is AI (AI)? Definition, Types, Examples & Use Cases, CIO (Oct. 1, 2024), https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence. (last visited Sept. 12, 2025 at 05:09 PM).

[33] Megan Cornish, LICSW, AI vs. Augmented Intelligence: What's the Difference, and Why Does It Matter in Behavioral Health? What Clinicians Think about AI for Behavioral Health, Eleos (Mar. 26, 2025), https://eleos.health/blog-posts/artificial-intelligence-vs-augmented-intelligence-in-behavioral-health/. (last visited Sept. 12, 2025 at 06:09 PM).

Key AI Subsets Used in Cybersecurity

- **Machine Learning (ML):** By using advanced statistical models, ML allows systems to "learn" from past data and adapt to new patterns of attacks without requiring explicit programming instructions.[34]

- **Neural Networks:** These systems function somewhat like the human brain—processing information through interconnected nodes. They are especially effective in recognizing complex patterns in cyber threats, such as malware behaviour or abnormal network activity.[35]

Impact of AI on Cybersecurity Operations

AI-enabled systems bring significant improvements in multiple areas, including:

1. **Strengthening Security Controls:** By automating detection and response mechanisms, AI helps in closing security gaps more efficiently.
2. **Managing IT Asset Inventory:** AI tools ensure that all devices and software connected to a network are continuously monitored, making it easier to identify potential points of vulnerability.

3. **Reducing Threat Exposure:** Through predictive analysis, AI can highlight areas most likely to be targeted by attackers, allowing organizations to prepare defenses in advance.

Conclusion

Cyber-crime has become one of the most pressing tasks of the digital era, threatening persons, businesses, and GVT's alike. While advanced technological tools have emerged globally as effective instruments for detection, prevention, and investigation, their adoption has been uneven across regions. Countries in North America, Europe, and East Asia have successfully integrated such systems into both public and private sectors, ensuring faster responses and stronger resilience. In contrast, India continues to face significant obstacles, including infrastructural limitations, skill shortages, and policy uncertainty, which slow down large-scale implementation.

[34] S. RUSSELL & P. NORVIG, AI: A MODERN APPROACH (4th ed. Pearson 2021).
[35] IAN GOODFELLOW, Y. BENGIO AND A. COURVILLE, DEEP LEARNING (MIT Press 2016).

This research highlights the gap between global practices and India's current framework, emphasizing the need for a balanced approach that combines legal reform, institutional strengthening, and technological adoption. By situating India within a comparative framework, the study demonstrates that while challenges persist, opportunities for improvement are substantial. Lessons drawn from international experiences can be adapted to India's unique socio-legal environment to build a more robust cyber defense system.

Ultimately, combating cybercrime requires not only technological innovation but also coordinated efforts between policymakers, enforcement agencies, and industry stakeholders. Bridging the gap between conceptual research and practical implementation will be key to ensuring that India keeps pace with global advancements in digital security.