Scopus

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 19, Issue 2, 2024
https://cgscopus.com/index.php/journals

Artificial Intelligence: Cyber-threat and Legal Requirements

- **Abdul Sakib Majid**
- **Ph.D. Scholar**
- **Gurugram University, Haryana**

- **Dr. Renu Chaudhary**
- **Assistant Professor**
- **Gurugram University, Haryana**

Abstract

Artificial Intelligence (AI) has ominously altered cyberspace. No doubt it has been a colossal aid to mankind and its dependence is only bound to increase with time. AI is at the forefront of many fields including finance, marketing, education, security and health care, to name a few. In an event of cyber security failure AI can help businesses to mitigate the attack. AI algorithms are a helpful measure in detecting questionable patters. Notwithstanding, its benefits it also has a darker side which is also looming upon us simultaneously. One study shows that 75% cyber security professionals believe that there has been an uptick in cyber-attacks, 85% of them, attribute these attacks directly with GenAI. Even a novice hacker can create a sophisticated phishing attack with the help of GenAI. The objective of this research to understand the growth of AI and its abuse with respect to Indian society and how Indian Government is trying to deal with this issue. To analyze the present regulatory frameworks available at hand and how the risk involved around AI can be mitigated. Recommendations given in the paper are an attempt on how to have a holistic approach towards AI.

Keyword: Artificial Intelligence, Cyber Security, Cyber Terrorism, GenAI

Research Methodology

Considering the changing trends in technology and inclination of the world towards Information Technology, application of computers and networking is increasing day by day. Technological advancements and new achievements in internet has globalized the market. Even though there is no significant doctrines laid out to deal with AI. Hence, following issues are statement of problems under this study:

- Whether current regulatory frameworks are sufficient to provide enough safeguards against misuse of AI.
- Whether Indian courts are equipped with sufficient artillery to adjudicate dispute arising out of AI and its related cyber threats.

Methodology adopted by the researcher is purely doctrinal, the research study takes note of new issues and innovations in the field of study area through different literature review.

Introduction

In the year 1988 a maliciously created self-replicating clever program named ‘Morris worm’ was unleashed on the internet which exploited weak passwords. It is known to be the first computer virus on the internet. Robert Tappan Morris the inventor of Morris worm became the first person to be ever convicted the then created Computer Fraud and Abuse Act in USA, and the rest is history, fast forwarding to the present times where internet boom has been all over the world there has been a constant development in cyber threats Crypto-jacking, Man in the middle attacks, SQL injection and data breaches are some cyber concerns to name a few. According to a study conducted by ‘Business Standards’ “India was the highest attacked country by hackers in Asia and the second-most attacked country globally (after the US)”. Annual Report, 2023 by CERT-In categories number of reported cases of cyber security in India during the year 2023 which are approximately 14 lakh incidents.

Security Incidents	Year-2023
Phishing	869
Unauthorized Networking Scanning/Probing	447720
Vulnerable Services	941592
Virus/Malicious Code	184131
Website Defacements	10665
Website Intrusion & Malware Propagation	1045
Others	6895
Total	1592917

A country like India where digitization has a significant impact, combined study conducted by IAMAI and KANTAR reported that in the year 2023 around 55% (821 million) of Indian population has accessed internet. Around 90% are daily users of internet with an average time of 90 minutes/day, most of whom are from rural India. Such numbers are suggestive of the fact of the potential victims for the cyber attackers.

The constant innovation in the field of Information Technology (IT) has led to the development of Artificial Intelligence (AI). The ever-growing extensions of AI is often termed as 5th Industrial Revolution which might have a drastic impact from our daily lives to unparalleled political, social, and economic developments.

AI development can primarily be divided into two categories: (i) machine learning and; (ii) deep learning. Machine learning can be understood as an algorithm that learns from a give data-set which is being constantly fed to it. These algorithms extract patterns and learn implicit rules from samples in a data-set. A common example of this can be Natural Language Processing models like ‘Alexa’ by ‘Amazon’ or ‘Siri’ by ‘Apple’. Deep learning on the contrary works with neural networks where it learns from constantly performing a single task repeatedly with minor changes so as to improve the outcome every single time, one such use of deep learning can be seen in Digiyatra facial recognition system where its software compare a live capture with digital image stored in its database. It is the combination of machine learning and deep learning that makes AI potent enough to sense, reason, act and adapt to a given situation.

The gradual adaptation of AI by government organizations, companies and likely criminal groups leading to automatization in various fields of daily work, potentially offering ways to escape the law. The easy accessibility of AI to non-state actors make it dangerous as it can be used by terrorist organizations causing detriment to national and global security.

AI in itself is not a threat to society, it is a neutral tool and its pros and cons are determined by the person or organization using it. AI can serve the humanity or can be a cause for its instability and destruction.

An attack on India’s most prominent medical institute servers i.e. AIIMS, Delhi has bring in a widespread media attention and raise global security concerns. Such a direct attack on health care institutions poses serious threat as it not only affect the public profile of the organization but also the human life. Sensitive information such as patient name, health risks and other patient related records are exposed. Such attacks highlight the overwhelming sway a cyber-attack can have in the present times. With continuous rise of fin-tech platforms there is a higher need for cyber safety measure to prevent such experts. As confirmed by National Payments Corporation of India (NPCI), UPI transactions have surpassed 10 billion mark with transactional value nearing about 204.77 billion Dollars.

The objective of this paper is to scrutinize how AI can be exploited by dissatisfied class of people or terrorist organization for their personal, political or economic gains vis-à-vis how government can tackle these issues with the help of requisite legal framework.

AI has the ability to cause havoc either by a physical attack or through cyber terrorism.

Physical Attacks

It is not a hidden secret that time and again terrorist organizations or mafias have used vehicles as in integral part of their operations; the reason is simple, any uncontrolled vehicle in a densely populated area is a much cheaper, easier and easy to hide option from security forces. Be it the attack of 9/11 or explosive truck driven by suicide bombers (e.g. Pulwama attack-14/02/2019), all these assaults have one thing in common, terrorists using vehicles to drive them into pedestrians, causing mass casualties. Now with AI in the front seat of this technology driven era it has become much easier to hack into drones or cars running on a computer program thereby negating the need of any human element making it a more effective method of causing destruction. With the use of AI the scope of human error caused by fatigue or fear is also reduced during terror operations as all what is needed is a well-trained algorithm. Hence, it is safe to say that advancement in technology is not only impacting enterprises but also terror stratagems. With more autonomous level of driving in vehicles make them very effective in being weaponized. In Russia-Ukraine war, it is the Ukrainian army which has even the battlefield against Russian tanks and its large army. Use of First Person View (FPV) drones is one such example. Its low cost and easy handling makes it a very potent weapon in the hands of terror groups. Further mixing it with machine learning, as used by self-driven automaker ‘Tesla’ which can integrations like facial recognition and many more to differentiate between objects and people, can cause mayhem. On the one hand such inventions make the environment a safer place to live in but simultaneously a more dangerous also.

Hon'ble Chief Justice of India D.Y. Chandrachud in an event at Madurai expressly flagged the issue of our daily dependence on technology while highlighting the Microsoft outrage of July 19, 2024 he said "*I am an ardent believer of the benefits of technology and just yesterday we saw the adverse effects of technological dependance. After the Microsoft outage flights all across the country were cancelled. Numerous flights from Delhi were cancelled…*"[1]

In the era where everything is impacted by technology up to certain extent it has become more important to not only regulate communications by land, sea, air and space but also to look after cyberspace. It has become the most decisive aspect of contemporary life. It has no physical borders and connect everyone to everything. Now every kind of communication is performed over one or many tech-driven platforms. Cyber security and its lawful regulation helps in creating a safe virtual environment, as digitization being a global phenomenon. AI might also advantage anti-government organizations in developing much more chic and precarious attacks. With the use of AI in such attacks their speed to replicate and multiply will be a huge problem for cyber experts to come up with timely solutions.

Section 66F of 'The Information Technology Act, 2000' provides for punishment and defines cyber terrorism[2]. With the help of AI it's easier to exploit cyber security weaknesses. If a hacker tries to enter an encrypted system and upon him failing he will have to start again but with the

[1] (Microsoft outage showed us adverse effects of technological dependence: CJI DY Chandrachud, 2024)

[2] 66F. Punishment for cyber terrorism.–(1) Whoever,– (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by– (i) denying or cause the denial of access to any person authorised to access computer resource; or (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or (iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or (B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism. (2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

adaptation of machine learning such hacks become more accurate and fast and every next hack attack will be more lethal. Hence, empowering cyber terrorists to cause a potential amount of disruption and damage in any working model, whether governmental or non-governmental.

WannaCry ransomware attack of 2017 which affected different organizations in over 150 countries around the globe is a prime example of unsafe cyberspace we are already living in. The cyber-attack exploited the vulnerability in Windows computer. It moved laterally through an organization in seconds, paralyzing hard drives and inspiring copycat attacks. It affected National Health Service (NHS) system in UK on a larger scale so much so, that ambulance services and patients across the nation had to be diverted due to non-availability of services because of ransomware. The ability of the cyber-attack to spread automatically reflects the power of AI making it independent and speedy.

Now it is a well understood concept that anything disrupting cyberspace can have global ramifications making domain of cyber security the utmost priority for national and international organizations. It is widely believed that National Security Agency (NSA) of United States of America, knew about this flaw in Windows system which they never reported to Microsoft and developed a ransomware ‘EternalBlue’ to exploit it and which was later stolen from NSA. The then Vice President of Microsoft, Brad Smith criticized US government for non-cooperation and timely intimation of the bug, which could have prevented the attack. It is important to have an interconnected approach and cooperation among nations and organizations in the domain of cyber space as it has trans-boundary effects.

GenAI vis-à-vis Cybersecurity

GenAI is a specie under the genus of AI, its main ability is to generate outputs based on data it has been fed or trained on. Where AI understand patterns and then predict the outcome, GenAI has the capacity to construct a new content either in the form of text, audio or images etc. it is based on deep learning method called ‘generative adversarial networks’ (GANs) to formulate new content.

It is important to realise that GenAI and its legal intersection with cyber security has to be understood in the framework of its usability. AI tools like ‘WormGPT’ and ‘FraudGPT’ are being continuously leveraged by cyber criminals. Using of AI for attacking is one of its use while on the contrary it can also be used as to counter such attacks by providing an apt defance mechanism, as it allows interminable detection of attacks. AI models can be trained to predict daily user behavioural patterns and therefore, categorizing any malicious activity. Acronis, a global leader in cyber security and data protection reported a surge of 293% in 2024 in phishing and email attacks as compared to 2023. It is imperative to have a holistic approach so as to secure digital data, comprehensive security awareness programs and in case of a breach incident response planning is required, so as to combat cyber threats.

Misuse of GenAI

World Economic Forum in its 19th edition of 'The Global Risks Report 2024' capitalized the fact countries will face in coming decade, according to report misinformation is at the top of the list in terms of risk posing and India being ranked at no. 1 country to be facing this risk. With the substantial increase of daily dependence on use of AI is also supplemented by the challenges, some of which can be:

- **Deepfakes**

Deepfakes are highly manipulated audio-video or pictures created by AI which portrays a person doing or saying something. AI models are trained by feeding photographs, audios and videos of a targeted individual so as to create a convincing imitation. With more and more evolvement of technology such deepfakes are getting harder to detect due to being more realistic in nature.

One very exemplary use of Deepfake, which was first of its kind in India in music industry was used by a music production company 'Inside Motion Picture' in creating an audio-video song 'Mera Na' for famous Punjabi Singer/Rapper Sidhu Moosewala after his death in an unfortunate shooting incident. On the contrary Deepfakes can be used to spread propaganda so as to manipulate public opinion, such rifts are likely to arise during election campaigning so as to polarize the voters in favour of a certain political party or candidate. They may even be a concern for national security. In a time where their exist so much global political instability due Russia-Ukraine Conflict, Israel-Gaza attacks or Indo-China boarder encroachment, it is more important than ever to have a verified news. The mere knowledge of the fact that such potent AI techniques are in existence can delegitimise the trust of people authentic information.

- **Data Poisoning**

In present times where social media influence has a huge impact on our society and everything we do or happening around us is posted on various social media handles. Hence, it become easy to control data for its adverse use and opinion. AI models are generally trained by using data sets available to an organization which are collected from its users. Therefore, quality, diversity and quantity matters very much while training an AI model. So if a data is corrupted by way of data explosion then it is vitally important that the AI model trained from that data set might not be accurate in its findings. Recently tech-giant Google apologised for the remarks given by its AI model 'Gemini' on Hon'ble Prime Minister of India. The sole purpose of data poisoning is to interfere in the learning process of the AI tool which can in turn be used by attackers to exploit and succeed in their goals. An early example of such data poisoning is case study of AI chatbot 'Tay' unveiled by Microsoft in 2016. Where the purpose was to have casual and playful conversations with it but soon after its unveiling people started exploding it with all sorts of racist and misogynistic remarks and Tay being a computer program/robot started repeating the same sentiments back to its users. As the old saying in programming world goes 'flaming garbage pile in, flaming garbage pile out.'

- **Automated Attacks**

Another adverse use of GenAI is in creating automatic attacks as it can learn to bypass security protocols from its previous failed attempts and then use all that information to write a new malicious code so as to create phishing pages or write scam letters, all that without any human intervention. FraudGPT is one such example of it.

Indian Regulations to Govern AI Framework

With all the development and constant upgradation of infrastructure in India the aim to the government is to make it a next technological hub for global trade and commerce, for this the shift of attitude of the government policies towards the use of technology in every sector is evident. The regulation today in place might not be at par to substantially govern GenAI or AI as none of the statues define those terms expressly. Though, 'cyber security' has been defined as "protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction."[3]

[3] Section 2(1)(nb), Information Technology Act, 2000.

- **Information Technology Act, 2000 (IT, Act)**

India does not have any special law which deals with the cyber security exclusively. Information Technology Act, 2000 has outlasted its purpose of enacting. As preamble of the Act states that "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."[4] But with time and to tackle with developments in the field of computer technology, the Act has been amended several times. It now covers the fields like electronic voyeurism, identity theft and cyber security.

- **CERT-In**

Government of India in 2009 has notified about the appointment of 'Indian Computer Emergency Response Team (CERT-In)', so as to detect, respond and protect against cyber security incidents. Due to sudden and steady spike in cyber frauds and concerns for them CERT-In Rules[5] were notified so as to deal with the problem at hand.

Apart from Information Technology Act, 2000 there are Rules[6] laid down by CERT-In. On 28th April 2022 CERT-In issued directions[7] with regards to mandatory reporting of cyber security incidents by service providers, data centres, intermediaries, body corporate and Government organizations, within six hours of the incident. These practice directions were issued so that a trusted and safe internet space can be created. These directions makes it mandatory about to report "attacks or malicious activities affecting systems/software/applications related to artificial intelligence and machine learning." [8]

[4] Information Technology Act, 2000
[5] The Information (The Indian Computer Emergency Response Team and Manner of Performing Functions and The Information (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.
[6] ibid
[7] Notification No. 20(3)/2022-CERT-In, Government of India.
[8] ibid

Notwithstanding that these directions still miss out on defining expressly as to what constitute Artificial Intelligence or Machine Learning.

- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)**

These rules regulate how to process and handle, personal and sensitive data of uses. It applies to both individual and corporate body. The rules provide IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" as one such standard for cyber safety of personal information and data.

- **Financial Sectorial Regulations**

Today cyber security is a major concern in every sector of economy. Financial institutions like SEBI, RBI, and IRDAI etc. are hugely dependent on third-party cloud service providers (CSPs) for data processing and storing. It is important to have a stricter compliance mechanism for regulated entities (REs) as they do not have direct control over data managed independently by CSPs. Hence, REs should maintain high security standards and conduct regular audits to have an oversight over CSPs. Also placing CSPs under contractual obligations to maintain certain security canons.

- **Digital Personal Data Protection Act, 2023 (DPDPA, 2023)**

Digital Personal Data Protection Act, 2023 is one of its kind legislation and India’s first enactment to deal specifically with personal data, is introduced by the government. Its main objective is to safeguard individual privacy in this digital age. DPDPA is India’s own version of General Data Protection Regulation (GDPR) enacted by European Union (EU). While both the regulations in their own jurisdictions provide for number of rights to users over their personal data and putting stricter obligations on organizations that process personal data to implement proper security procedures in case of data breaches. Both provide for appropriate remedies for non-compliance. Despite their similarities they have some key differences like GDPR has a stricter compliances for transfer of personal information outside the jurisdictional domain of EU as compared to its India counterpart. Moreover, GDPR has categorized data as personal data or critical data in terms of its usage, which is missing in DPDPDA, as it applies uniformly to all and every type of personal data.

While there is no express definition of AI under the DPDPA but definitions of ‘automated’[9] and ‘processing’[10] are wide enough in their interpretation as to govern personal data handling using AI tools. DPDPA also penalizes ‘personal data breach’. Any kind of personal data breach by ‘data fiduciary’[11] has to be reported to data protection board and affected ‘data principal’[12]. It places stricter financial penalties for non-compliance extending up to Rs. 200 crore.

The jurisprudence regarding the interplay between personal data and AI or GenAI, has yet to be developed by data protection board with time. As DPDPA primarily focuses on protection of personal data it leaves a grey area where use of aggregated or anonymised data in conjunction with GenAI where identity on an individual might be protected but such data might affect the learning process of AI model.

- **Digital India Act, 2023**

As the Current IT Act, 2000 is not at par with advancement of technology and it lacks at many folds such as; lack of coordinated response mechanism for cyber security incidents, limited recognition of new categories of cybercrimes or lack of ample requisites so as to protect data privacy etc. The Digital India Act is an attempt to protect and balance the tenets of Digital India. The Act will enable to have a safeguard against embryonic knowledge in the area of AI, machine learning, Blockchain, Augmented Reality and natural language processing etc. DIA might be on the similar lines as that of EU AI Act, a first legislation to expressly regulate `Artificial Intelligence.

It is a way forward to achieve Digital India Goals of 2026. Since the Act is expected to replace the two decade old IT legislation hence, its future is still in shadows whether it will come to light or not. It might not be as easy as it looks like, considering the vastness of the field in the

[9] Section 2(b), Digital Personal Data Protection Act, 2023.
[10] Section 2(x), Digital Personal Data Protection Act, 2023.
[11] Section 2(i), Digital Personal Data Protection Act, 2023.
[12] Section 2(j), Digital Personal Data Protection Act, 2023.

domain of technology, as one legislation is all it takes to regulate it or we need multiple sector-specific regulations, only the time will decide the fate of the Act.

Despite all the legislations already in place or expected to be enacted it is evident that our laws still lack behind to catch up with the technological movement. AI, ML, Blockchain, AR/VR, IoT etc. are things of today and are yet to be addressed by a proper legislation. Nevertheless, it’s time to have a regulation so to curb the menace of AI or ML etc.

Outlook by Indian Courts

As of now there has been no specific adjudication on the use of AI or other relative technologies. It is an area of law which is yet to be developed. However, there were instances when Indian courts did not hold back on their opinion on the use of AI. Recently Delhi High Court observed that “The above responses from ChatGPT as also the one relied upon by the Plaintiffs shows that the said tool cannot be the basis of adjudication of legal or factual issues in a court of law. The response of a Large Language Model (LLM) based chatbots such as ChatGPT, which is sought to be relied upon by ld. Counsel for the Plaintiff, depends upon a host of factors including the nature and structure of query put by the user, the training data etc. Further, there are possibilities of incorrect responses, fictional case laws, imaginative data etc. generated by AI chatbots. Accuracy and reliability of AI generated data is still in the grey area. There is no doubt in the mind of the Court that at the present stage of technological development, AI cannot substitute either the human intelligence or the humane element in the adjudicatory process. At best the tool could be utilised for a preliminary understanding or for preliminary research and nothing more.”[13]

In another instance Delhi High Court while realising the adverse impact of AI and use of Deepfakes observed that; “The technological tools that are now freely available make it possible for any illegal and unauthorised user to use, produce or imitate any celebrity’s persona, by using any tools including Artificial Intelligence. The celebrity enjoys the right of privacy, and does not wish that his or her image, voice, likeness is portrayed in a dark or grim manner, as portrayed on the porn websites. Moreover, the Plaintiff’s image is being morphed along with other actresses in videos

[13] (CHRISTIAN LOUBOUTIN SAS & ANR. vs M/S THE SHOE BOUTIQUE – SHUTIQ, 2023)

and images generated in a manner, which are not merely offensive or derogatory to the Plaintiff, but also to such other third party celebrities and actresses."[14]

Risk Mitigation Approach

The escalating use of AI and the adverse impacts it may cause necessitate to have AI centric legislations. NITI Aayog Report in 2021 emphasised on having a responsible use of AI in India with highlighting the principles of privacy, transparency and reliability. Another effective approach is to provide incentives for research in the field of AI. As the field of AI is new and its literacy among people is not adequate. There is a requirement for educating judiciary and law enforcement agencies so that legal issues around AI can be resolved in a smooth way in an effective manner. It is important to identity legal and ethical issues surrounding AI. Hence, to incentivise the field of AI research it is important to have a collaboration between government and large corporations, so as to promote innovation and accessibility.

Cyber Insurance is another way of mitigating the risk involved in AI development. As projected by Data Security Council of India (DSCI), there is expected growth of 25% in 2024 in cyber insurance market. Cyber insurance not only help companies in providing first-party coverage and liability coverage, but also provide benefits such as regular third party audits, criminal reward funds and post incident public relations support.

Where on one hand AI poses a risk to cyber security it can also be used as an effective tool in combating cyber threats. Convolutional Neural Networks and Recurrent Neural Networks have been proven effective in filtering out fabricated media files, tools like Deepware Scanner based on machine learning is used to detect deepfake videos. Self-practice of implementing Multi-factor authentication systems can be an additional layer of safety against AI programs trying to gain unauthorized access.

Collaborative approach between different agencies whether state sponsored or private will have sweeping effect in having a holistic risk management program. NITI Aayog and Microsoft in 2018 announced a collaboration so as to clout AI and cloud computing in order to elucidate challenges

[14] (ANIL KAPOOR vs SIMPLY LIFE INDIA & ORS, 2023)

faced by agricultural and healthcare industry, while at the same time building educational capacity in AI and data sciences.

It has been evident that non-coordination among various security agencies whether internationally or nationally due to the sudden competitive security environment has been a major loophole which terrorist organizations are using to their benefit. A timely communication and active participation of Private-Public organizations is must. Software's from companies like Google, Microsoft, Apple, Accenture, Infosys etc. are used globally by various state and non-state actors. Hence, unlike nations who are represented by international institutions globally, such companies lack an apt representational body. Due to the continuous increase and efficiency of each AI attach, there is a significant need to have a separate international body having representation from all Public-Private sectors, as global problem requires global solutions. United Nations (UN) has an International Programme on Cybercrime as part of its Office on 'Drugs and Crime' but given the current scenario a proper outlook and over-haul is necessary to deal with the issue of AI and cyber terrorism.

'The Bletchley Park Declaration' is one of its kind global pact to understand, manage and tackle the risks of AI by joint efforts. India along with United States, China, European Union and several other major counties signed it. The objective of the summit was not to outline a blueprint for international law on regulating AI, but to frame a global consensus and formulate risk based policies considering national circumstances, though non-binding in nature.

One may say that such non-binding agreements merely serve a consensus formation purpose and lack real intent of action. As one of the greatest difficulty in the implementation of such International agreements is in holding the person accountable who breaks it. Paris Accord (2015), is a great example of it, a non-binding agreement for regulation of climate change. Even after 9 years of its signing countries still fail to reach their target emission goals. Same might be the case with Agreements on AI. Considering the current pace of growth on the field of AI, there is a strong need for institutional response at a global stage.

Conclusion

AI advancement is a double edged sword, and its user defines whether it is to make life simple and easy or have an adverse and negative side effects. The current legal standards are not up to the mark to deal with upcoming cybercrimes, there is urgent need to have an effective regulatory mechanism. Merely placing a law on paper is not enough to combat AI controlled attacks, the need of the hour requires to have its proper implementation and sensitization. There must be a thin line of difference as to when AI is camouflaged for combating and committing an offence. A visionary enactment that strikes right at the middle of risk and innovation around AI development is needed to bring a change in status quo.

References

‘The Global Risks Report 2024’, World Economic Forum 19th Edition. (2024). *The Global Risks Report.* Geneva: World Economic Forum.

AIIMS Ransomware Attack. (2023, July 5). Retrieved from Cyber Management Alliance: https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack

ANIL KAPOOR vs SIMPLY LIFE INDIA & ORS, CS(COMM) 652/2023 (High Court of Delhi September 20, 2023).

CERT-In. (2023). *Annual Report.* New Delhi: Ministry of Electronics & Information Technology (MeitY).

CHRISTIAN LOUBOUTIN SAS & ANR. vs M/S THE SHOE BOUTIQUE – SHUTIQ, CS(COMM) 583/2023 (High Court of Delhi August 22, 2023).

Das, S. (2023, August 31). *UPI crosses 10 billion monthly transactions, confirms NPCI*. Retrieved from mint: https://www.livemint.com/economy/upi-crosses-10-billion-monthly-transactions-confirms-npci-11693498082161.html

David Warde-Farley, I. G. (2016). *Perturbations, Optimization, and Statistics*. MIT Press Direct.

Dhillon, A. (2024, February 2024). *India Confronts Google over Gemini AI tool's 'fascist Modi' responses*. Retrieved from The Guardian: https://www.theguardian.com/world/2024/feb/26/india-confronts-google-over-gemini-ai-tools-fascist-modi-responses

India highest attacked country by hackers in Asia, 2nd globally in 2022. (2023, February 2023). Retrieved from Business Standard: https://www.business-standard.com/article/international/india-highest-attacked-country-by-hackers-in-asia-2nd-globally-in-2022-123020800616_1.html

KANTAR. (2023). *Intenet In India* . IMAI.

Microsoft outage showed us adverse effects of technological dependence: CJI DY Chandrachud. (2024, July 20). Retrieved from Bar and Bench: https://www.barandbench.com/news/microsoft-outage-showed-adverse-effects-technological-dependence-cji-dy-chandrachud

SCHAFFHAUSEN. (2024, 30 July). *Acronis H1 2024 Cyberthreats Report Highlights a 293% Surge in Email Attacks*. Retrieved from Acronis: https://www.acronis.com/en-us/pr/2024/acronis-h1-2024-cyberthreats-report-highlights-a-293-surge-in-email-attacks/

Sur, A. (2024, July 1). *Digital India Bill likely to be delayed, government may opt for smaller, urgent regulations*. Retrieved from Money control: https://www.moneycontrol.com/technology/digital-india-bill-likely-to-be-delayed-government-may-opt-for-smaller-urgent-regulations-article-12759435.html

Vincent, J. (2016, March 24). *Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day*. Retrieved from The Verge: https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

Zaki, A. (2023, August 30). *85% of Cybersecurity Leaders Say Recent Attacks Powered by AI: Weekly Stat*. Retrieved from CFO: https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/