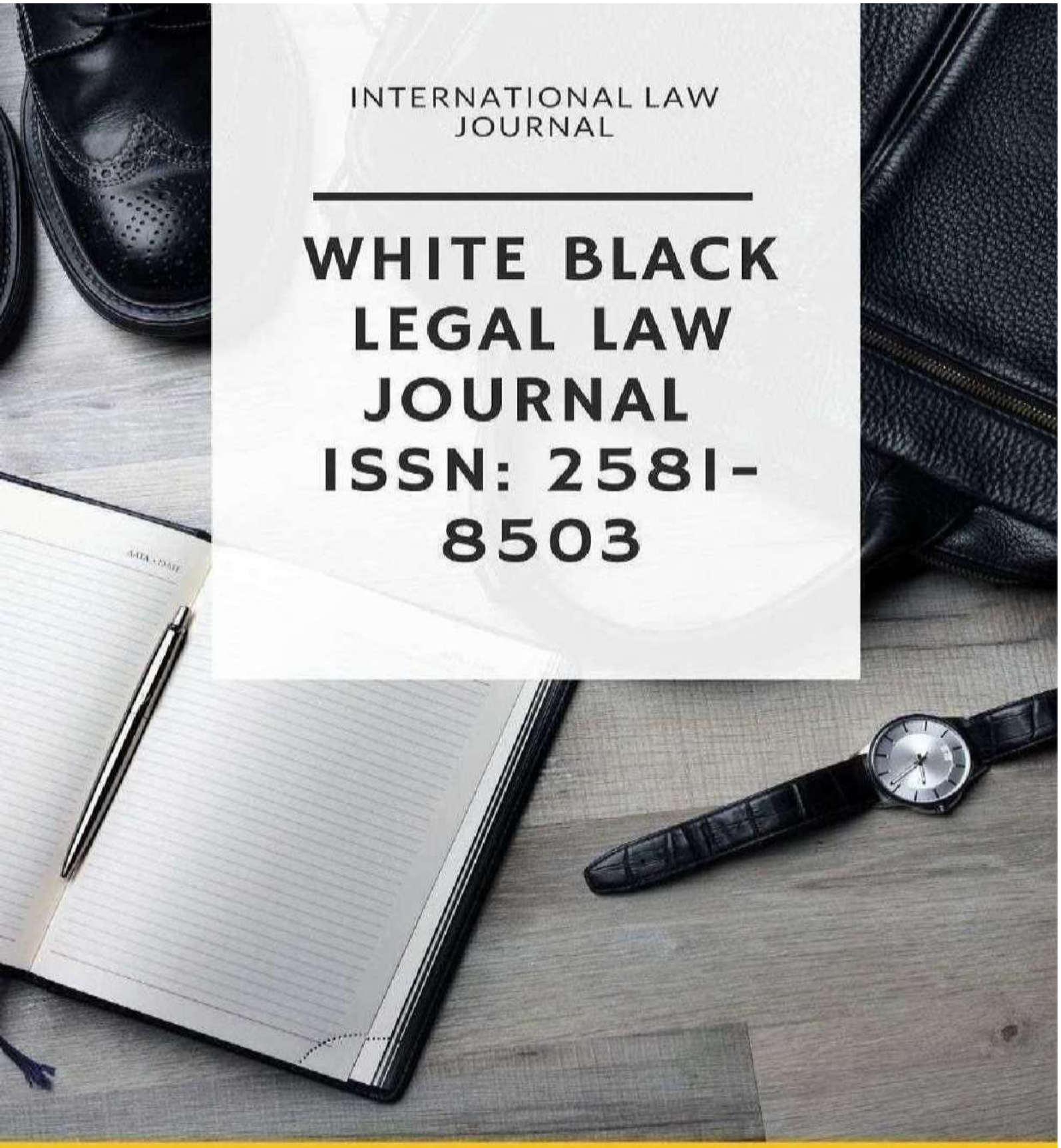

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and

refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

AI-STEERED CYBER DEFENSE: A FORAY INTO LEGAL CHALLENGES WITHIN INDIA'S CYBER LAW FRAMEWORK

AUTHORED BY - RAMIYA SHREE MUTHALRAJ

Abstract

The rapid advancement of Artificial Intelligence (AI) in cyber defense represents a technologicalrevolution, enhancing the capabilities of security systems to preempt, detect, and respond tocyber threats. However, the rise of AI-driven cyber threats, where malicious actors use AI to perpetrate sophisticated attacks, highlights the dark side of this technology. This paper delves into the emerging landscape of "AI in cyber defense", exploring the development of autonomoussystems that offer real-time, intelligent responses to cybersecurity challenges, while also posing new risks. Central to this discourse are the issues of transparency and accountability, particularly when AI operates independently in defending critical infrastructure or sensitive data. The legal landscape in India is evolving to address these challenges, but India's Cyber Law Framework andits National Cyber Security Policy face significant hurdles in accommodating the complexities of AI in cybersecurity. This study examines the legal issues associated with AI in cyber defense , such as liability, data protection, and regulatory oversight. Through an analysis of India's existinglegal structures, the paper identifies key gaps and provides recommendations to further strengthen India's cyber law framework, ensuring it is equipped to handle the growing role of AI in cyber defense while mitigating associated risks.

Introduction

Cyber convergence of Artificial Intelligence and cybersecurity is a kind of turning point in defense as the cyber threat becomes sharper, more complex, and sophisticated by the day. AI hasproven to demonstrate its value in cyber defense by enabling quick and efficient threat detection, response, and mitigation strategies. But this technology innovation also throws in new challenges, especially relating to India's cyber law framework, which is changing alongside rapid digital transformation. The country of India, host to the world's largest democracy and anincreasingly emerging digital economy, is threatened by multiple cyber

threats ranging from databreaches to state-sponsored cyber espionage. Generally, the genesis of India's cyber law system is primarily based on the Information Technology Act, 2000 (IT Act), along with amendments and supplementary rules. However, those laws are not properly outfitted to deal with the intricacies that AI-driven technologies introduce, especially in liability, data privacy issues, and the ethical use of AI in offensive and defensive cyber capabilities. These are requirements thatthe legal framework of India must address as AI becomes more integral to cybersecurity. This article explores the revolutionary changes of AI in cyber defense, looks into both the defensive and offensive capabilities of AI, and discovers the legal and ethical challenges India faces in regulating systems based on AI for cybersecurity. It also draws parallels across global trends and recommendations to further enhance the cyber law framework of India to manage AI-induced risks.

AI in Cyber Defense: A Technological Revolution

AI inclusion in cybersecurity has transformed the way organizations can counter their cyber threats. Essentially, AI systems, which are mainly powered by the machine learning algorithm, neural networks, and deep learning models, can scan massive amounts of data in real time; hencethey learn from patterns to identify possible threats when still feasible before damage is done. This capability to process and interpret large datasets at speeds far beyond human capacity allows AI to truly shine in critical areas such as threat detection, predictive analytics, and automated response systems. The real strength of AI in cyber defense is through anomaly detection. Traditional cybersecurity measures, such as firewalls and antivirus software, generallyrely on prescriptive rules and signatures. These work at some level, but failing here is the failure of identifying new or emerging source threats which do not have any particular pattern developed beforehand. AI-based systems can learn from past incidents and identify if there is a failure in usual behavior-even if it doesn't match a known pattern. This enables the discovery andalerting by organizations of APTs and zero-day vulnerabilities that otherwise could not beforeseen.

Case Study on AI in the Financial Sector, AI-driven cyber defense has highly exploited finance, and today, most banks and financial institutions are embracing AI in fraud and money launderingeradication as well as intrusions in cyber attacks[1]. For example, JPMorgan Chase

[1] Kim, B. J., Yun, S. B., Kim, M. O., & Chun, S. H. (2023). A Case Study on the Introduction and Use of Artificial Intelligence in the Financial Sector. Industry Promotion Research, 8(2), 21-27.

uses AI to analyze clients' behaviors and detect any anomalies that may indicate fraudulent activities. AI systems are able to cross-check real-time transactions against historical data in an efficient manner. In fact, they flag suspicious transactions before fraud can take place, which offers a sense of security that traditional methods often lack, reacting only after the fraud is committed. AI is also critical to predictive analytics, which, based on past trends and attacks, predicts future cyber threats. Predictive analytics uses machine learning models to identify trends in cyberattacks, predict which systems are most vulnerable, and prioritize defenses accordingly. Based on data gathered from previous attacks, AI predicts how attackers may exploit new vulnerabilities and offers proactive measures to mitigate risks. Example: Predictive Defense Against Ransomware, Ransomware attacks have grown in the last decade, and most recently, its high-profile attacks against hospitals, schools, and government sectors have drawn keen attention. AI-based systems that predict ransomware attacks once it senses its onset in encrypted activities or unauthorized access attempts to sensitive data can prevent the ransomware from encrypting critical network data.

Automation of cyber defenses-this is the major contribution that AI makes to cybersecurity. Automated response systems enable AI to respond to threats at the moment they are detected, hence reducing the time needed to neutralize the attack. AI-powered systems may isolate compromised devices, block unauthorized access, and apply patches on their own, all without human intervention. This not only minimizes the damage caused by such an attack but also relieves much burden on human teams of cybersecurity, as they can focus further on more significant tasks. Case Study on AI in Incident Response: Automated response is perhaps best exemplified by Darktrace's Antigena, an AI-powered tool for cybersecurity response that uses machine learning to autonomously respond to cyber events. A threat could be identified, causing Antigena to quarantine infected systems or enforce a network segmentation, all of this withoutthe need for manual intervention. This reduces the time attackers have to exploit vulnerabilities significantly, thereby helping to minimize the impact caused by cyber incidents. AI becomes a new power of threat intelligence platforms, which collect and analyze data from various sources and yield emerging threats. These systems use AI for traffic, security logs, and well-defined external threat databases, thus offering organizations real-time knowledge of the cyber threat.

AI-Driven Cyber Threats: The Dark Side of AI

Phishing has been around for ages, but AI magnified the effectiveness of phishing attacks. Whilewith traditional phishing attacks, generic emails would flood the Internet along with millions of recipients, and some percentage of those would fall for the scam, AI upgraded this approach by creating AI-enhanced phishing in which cybercriminals employ machine learning to create very targeted attacks that are very hard to distinguish. AI-generated phishing relies on the analysis of enormous sets of data for personally tailored phishing emails. AI can produce emails that appear to be from trusted and professional sources while relying on an analysis of a target's online behavior, social media, and communication patterns. The emails can be drafted in a manner suggesting they come from trusted contacts, and it is more difficult to recognize them as coming from impostors. Some organizations have even been attacked with phishing emails written in their chief executive officer's writing style. AI-Driven Phishing Attacks on Executives: For example, in 2021, a variety of high-profile phishing attacks targeted corporate executives through AI-generated emails with the same content, in the names of their colleagues. Thereferences had specific details about ongoing projects and internal discussions that made it all themore convincing[2]. Several high-ranking executives' email accounts were compromised by attackers, leading to massive financial losses and data breaches. This episode makes it evident about the new advancement in AI-enhanced phishing and how this can move undetected through the traditional security controls. Another alarming threat is AI-assisted malware, which utilize AIto evade detection and changes dynamically according to the surroundings. Traditional malware can be recognized by signature-based antivirus software programs, but AI-assisted malware utilizes algorithmic machine learning to dynamically change its code, behavior, or appearance; thus, making it problematic to detect AI. Among the most perilous forms of AI-assisted malware is polymorphic malware, which changes its code every time it infects a new system. This type of malware is always one step ahead of an antivirus program, since each appearance of the malwarewill look different from any previous appearance, thus making detection based on signature impossible. AI can also allow malware to learn from the defenses it encounters and then adapt and find new weaknesses to take advantage of.

AI systems themselves are not impervious to attack. Adversarial attacks: attackers taking

[2] Prince, N. U., Faheem, M. A., Khan, O. U., Hossain, K., Alkhayyat, A., Hamdache, A., & Elmouki, I. (2024). AI-Powered Data-Driven Cybersecurity Techniques: Boosting Threat Identification and Reaction. Nanotechnology Perceptions, 332-353.

advantage of vulnerabilities in AI models through carefully crafted inputs that are likely to induce incorrect predictions or decisions. Such attacks could be used to compromise AI-based security systems by making them misclassify threats or fail to detect malicious activity of any kind. Attacks in the case of image recognition can be pretty nasty, in the sense that even minor perturbations of an image can make a classification model mistake the object it is describing. A very good example of this is how adding noise to an image of a stop sign may cause an AI system to identify it as a yield sign, thus giving way to potential accidents involving autonomousvehicles. It is seen that even AI-based cyber security can be attacked by disguising malware or any other malicious activity as non-malicious in nature. For Example: Adversarial Attacks in Autonomous Vehicles, Adversarial attacks have been recently hijacked due to its applicability ona very recent subject in autonomous vehicles where AI models are used to interpret sensor data and make driving decisions. One such experiment demonstrated that researchers could readily deceive an AI system into rendering a stop sign as a yield sign by introducing small perturbationsto the stop signs. Although this is beyond the purview of cybersecurity, it indicates the vulnerability of AI systems to manipulations by hostile systems and suggests an urgency for robust defense against such attacks in cybersecurity applications.

Autonomous Cyber Defense Systems

Autonomous cyber defense systems, such as AI-powered intrusion detection and response systems, offer significant benefits in terms of speed and accuracy. However, they also raise ethical and legal questions about accountability and oversight. For instance, if an autonomous system incorrectly identifies a legitimate user as a threat and takes action to block their access, it could result in significant disruptions and potential legal liabilities. Ensuring that autonomous systems are subject to appropriate human oversight and can be overridden when necessary is essential to address these concerns. AI-driven cyber attacks represent a significant emerging threat[3]. These attacks can leverage AI to conduct sophisticated social engineering, identifyvulnerabilities, and evade detection. The use of AI in offensive cyber operations raises ethical questions about the responsible use of technology and the potential for escalation. From a legal perspective, there are also challenges related to attribution, as AI-driven attacks may be more difficult to trace back to their source. Developing international norms and agreements to govern the use of AI in cyber operations is crucial to mitigate these

[3] Jambol, D. D., Sofoluwe, O. O., Ukato, A., & Ochulor, O. J. (2024). Transforming equipment management in oil and gas with AI-Driven predictive maintenance. Computer Science & IT Research Journal, 5(5), 1090-1112.

risks. The deployment of AI in cyberdefense often involves the collection and analysis of large volumes of data, including personal information. This raises significant privacy concerns and necessitates robust data protection measures. For example, AI systems used for threat detection may need access to email communications, network traffic, and user behavior data[4]. Ensuring that such data is collected and processed in compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, is essential to protect individual privacy and prevent misuse. Addressing the ethical and legal implications of AI in cyber defense requiresa multi-faceted approach that involves collaboration between policymakers, industry leaders, andcivil society. The development of comprehensive ethical guidelines for the use of AI in cyber defense is crucial. These guidelines should address issues such as dual-use technology, autonomy, bias, privacy, and transparency. They should provide clear principles and best practices for the responsible development and deployment of AI systems, ensuring that ethical considerations are integrated into every stage of the process. Existing regulatory frameworks need to be updated and expanded to address the unique challenges posed by AI in cyber defense. This includes developing new regulations and standards for AI transparency, accountability, and fairness, as well as strengthening data protection laws. Regulatory bodies should also be equipped with the necessary resources and expertise to enforce these regulations effectively.

Promoting Transparency and Accountability

Ensuring transparency and accountability in AI systems is essential to build trust and mitigate ethical and legal risks. This includes developing explainable AI technologies that provide insights into their decision-making processes and enable stakeholders to assess their reliability and fairness. It also involves establishing clear lines of accountability for the actions and decisions of AI systems, ensuring that responsible parties can be held liable for any negative outcomes. Given the global nature of cyber threats and the widespread use of AI, international collaboration is crucial to address the ethical and legal implications of AI in cyber defense. This includes developing international norms and agreements to govern the use of AI in cyber operations, as well as fostering information sharing and cooperation between countries to enhance cybersecurity efforts. Collaborative initiatives can help to ensure a coordinated and effective response to emerging threats and promote the responsible use of AI technologies.

[4] Chen, Z., Xu, G., Mahalingam, V., Ge, L., Nguyen, J., Yu, W., & Lu, C. (2016). A cloud computing based network monitoring and threat detection system for critical infrastructures. Big Data Research, 3, 10-23.

Investing in research and education is essential to advance our understanding of the ethical and legal implications of AI in cyber defense[5]. This includes supporting interdisciplinary research that explores the intersection of AI, cybersecurity, ethics, and law, as well as developing educational programs to train the next generation of cybersecurity professionals and policymakers. By fostering a deep understanding of these issues, we can better prepare for the challenges and opportunities presented by AI in cyber defense.

India's Cyber Law Framework:

India's cyber law regime is primarily envisaged under the Information Technology Act, 2000 (IT Act). Introduced to respond to the increasing need for online transactions, the IT Act established a foundation for electronic commerce regulation, cybersecurity, and digital signatures. The IT Act has since been amended several times to add provisions relating to cybercrime, including hacking, identity theft, and data breach offenses. While the IT Act has so far gone well to counterthe traditional cyber threats, however, it was not developed with consideration of AI technologies. In so doing, the existing legal framework fails to sort out the complexity that is likely to be caused by AI-driven technologies. Key highlights include liability from AI-driven cyberattacks, protection of privacy in AI-driven systems, and ethics regarding AI use in cybersecurity. India has amended the IT Act in the face of an evolving cyber threat landscape. For instance, the IT Amendment Act, 2008 increased the penalties for cybercrimes and introduced new data protection provisions. However, such amendments are largely focused on traditional cybersecurity threats and not on the specific threats posed by AI-enabled systems.

There is a growing demand for AI-specific provisions under the IT Act to regulate the deployment and use of AI in cybersecurity. Such specific provisions can be focused upon issues related to liability, accountability, and transparency in AI-driven systems; as well as the ethics of AI-based surveillance, monitoring, and decision-making in any form of cybersecurity. The Roleof AI in Automated Decision-Making, Automated decision-making is one area where AI-specificregulations are needed. The newer AI systems are very advanced and rely on systems to control and manipulate autonomous decisions without human oversight. Several implications result, including increasing the efficacy of the response to cyber threats;

[5] Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66.

however, it also raises consequential questions of who is accountable when the AI system makes a wrong decision. For instance, if it decides to block the wrong traffic or fails to detect a threat, who is liable for the consequences? Today, India's legal provisions still fail to bring clear answers to them; regulatoryupdates are thus highly required in these clauses.

India's National Cyber Security Policy:

In this regard, besides the IT Act, India's Personal Data Protection Bill 2019 (PDP Bill) can be identified as one of the major strides towards protecting the privacy of individuals in the digital age. In that respect, the PDP Bill tries to regulate collection, storage, and processing of personal data. In this regard, the bill would enable control by the individual over the data and greater accountability from the organizations towards cases of data breaches. However, similar to the IT Act, the PDP Bill was not particularly drafted keeping AI in view. AI-based cybersecurity systems usually rely on huge volumes of data, thereby causing significant problems with respect to privacy. Such systems handle enormous personal and sensitive information for identifying patterns, anomaly detection, and anticipating possible threats. In the process, they may unknowingly cause an invasion of privacy without proper safeguards in place. In the case Data privacy in AI-based cybersecurity systems,in the year 2020, one of the major banks in India adopted AI-based fraud detection systems with the prime function of scrutinizing customers' transactions for detecting anomalous patterns, which are indicative of fraudulent activities. The system highly succeeded in combating fraudulent activities, but its use also raised data privacy concerns since they consist of collecting and analyzing sensitive financial information. The argument was that the AI system of the bank is opaque and hardly gives its customers a sense of control over their data usage[6]. The case here serves as a manifestation of the clash between imperatives of appropriate cybersecurity measures and individual privacy protection. In addition to the IT Act and the PDP Bill, India has a national cyber security policy, known as NCSP (National Cyber Security Policy), that assumes a very important position in the formation of cybersecurity perception in the country. NCSP was introduced in 2013 with an objective to protect critical information infrastructure and promote cyber resilience and encouragecollaboration between the private and public sector with regards to cyber threats. However, policy should be updated as the role of AI increases in cyber and as the need for specific guidelines.

[6] Yanisky-Ravid, S., & Hallisey, S. (2018). 'Equality and Privacy by Design': Ensuring Artificial Intelligence (AI) Is Properly Trained & Fed: A New Model of AI Data Transparency & Certification As Safe Harbor Procedures. Available at SSRN 3278490.

Legal Issues of AI in Cyber Defense

Just like in the case of AI-driven cybersecurity, some of the burning legal issues relate to determining liability when such AI systems are linked to cyber incidents. Most traditional cybersecurity tools operate under human control, while AI systems make decisions based on programming and the datasets they analyze. Once the AI system fails to detect a threat or even causes a security breach inadvertently, who is liable becomes complex. Liability in Automated Incident Response Suppose there is an incident response system, operating through artificial intelligence, that incorrectly identifies legitimate traffic as a cyber threat and blocks access to thecritical system. This would cause them tremendous financial and operational losses. Whose responsibility will it be? The AI developer, the organization deploying it, or the user configuring it? The present legal framework in India provides no clear-cut answers to these questions[7]. Thatis why specific provisions on liability pertaining to AI need to be included in the IT Act. AI-based cybersecurity systems process huge amounts of personal data that otherwise might not relate to each other, in search of patterns and threats. The direct data privacy concerns arise - especially with India's upcoming Personal Data Protection Bill. Though the PDP Bill mentions regulation of collection, storage, and processing of personal data, the privacy aspects related toAI have not been fully addressed. For example, AI systems inadvertently can collect more information than is reasonably necessary to accomplish the purpose of security, thereby infringing on the right to privacy. Surveillance and monitoring by AI also is capable of violating the same basic rights of privacy unless regulated.

Another legal challenge to AI in cybersecurity is bias. AI models are trained from large datasets and, if these datasets contain biased information, the AI model may replicate the same bias or even magnify it. This means biased models of AI can, in the arena of cybersecurity, actually treatthe same group fairly but less than other groups unfairly, to say in case of discrimination. In 2021, one of the largest Indian tech companies introduced an AI-driven surveillance system to monitor employees to allegedly ensure data breaches did not occur[8]. But since this system triggered many employees from certain backgrounds as probable threats due to the biased data used in developing the AI model, it serves as a specific example of the risk of AI bias on cybersecurity systems while again compelling urgent legal framework concerns regarding fairness and non-discrimination by AI. The ethical issues associated with the adoption of AI

[7] Pal, S., Kumari, K., Kadam, S., & Saha, A. (2023). The ai revolution. IARA Publication.
[8] ÜNVER, H. A. Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights.

besides those of bias are that the more powerful the system, the greater possibilities there are for the potential misuse of AI systems. Two applications from the list of potential applications for AIare mass surveillance and monitoring, together with offensive cyber operations, that are possible and have ethical implications with their deployment. As an example, AI- powered surveillance systems might be used in tracking a person's online behavior that affects the rights of privacy andcivil liberties. On the other hand, AI-technologized offensive tools might be used in cyberattacks from the other side where defense turns into an aggression state in cyberspace.

The cyberattacks are usually cross-border and, therefore, it is challenging to seek recourse under local laws in AI-driven cyber incidents. It is international cooperation that best deals with cross-border cyberattacks, and India's legal framework has not given proper mechanisms to collaborate with other countries over AI-related cybersecurity issues yet. India would have to engage with international organizations and governments for developing a global framework on AI in cybersecurity to effectively fight AI-driven cyber threats. These would encompass sharing threat intelligence, harmonization of legal standards, and protocol building for the investigation and prosecution of cross-border cybercrimes across the globe.

Recommendations to further strengthen India's Cyber Law Framework

The IT Act needs to add AI-specific provisions that would address the peculiar challenges thrown forth by AI to the concept of cybersecurity. Among these must be liability, accountability,transparency, and fairness in the AI-driven system. Such provisions will also clearly articulate what is ethically permissible in AI usage within surveillance, monitoring, and offensive cyber operations. The new Personal Data Protection Bill should address the privacy implications of AI-driven cybersecurity systems. This includes putting limits on excessive collection and analysis through AI systems and protecting people's rights to control how their data will be used in AI-driven applications for cybersecurity[9]. The legal frameworks should be established to combat AI bias within the cybersecurity systems. These should include testing on the organization's AI model for any biases, which should be observed and viewed during the design of fair and non-discriminatory AI operations. The law should ensure there is a legal platform for the transparency of AI decision-making processes and right the individuals to seek

[9] Alhitmi, H. K., Mardiah, A., Al-Sulaiti, K. I., & Abbas, J. (2024). Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions. Cogent Business & Management, 11(1), 2393743.

redress for thedecisions deemed as biased or unfair.

Cyber threats are global in nature and, therefore India has to interact with international bodies to bring about a global framework for AI in cybersecurity - participate in treaties and agreements related to cyber defense, share threat intelligence with other countries, and collaborate on cross-border AI-driven cyberattacks investigations. Last but not least, ethical guidelines on AI use in cybersecurity should be initiated by India. Such guidelines would warrant that AI systems are used responsibly and that the installation of such systems does not infringe on individuals' rights to privacy or civil liberties. The government must ensure that there is accountability and transparency involved in the use of AI for surveillance or monitoring purposes.

Conclusion

This is why India's legal framework needs to evolve further in matching the burgeoning threats itposes-empowered by AI as increasingly integrated into cyber defense. While it stands to offer great benefits in enhancing cybersecurity, there are cross-cutting legal, ethical, and regulatory issues that may arise from it if we do not use it well. Updating the Information Technology Act includes stronger provisions for data privacy protection regulation and ensuring AI bias and fairness enables India to build a set of conditions that would effectively support its inclusion in the safe application of cybersecurity. International cooperation in the pursuit of ethical AI use is also suggested as a way in which India can further move forward as a world leader in the practiceof AI in cyber defense. Over time, the cyber threats evolve, and thus, policymakers, legal experts, and cybersecurity professionals in India need to work together to ensure that AI is leveraged responsibly, applied fairly, and perfectly transparent. Such an evolution of cybersecurity in the future will be not only dependent on the revolution of technology but also onthe development of a sound legal framework that protects the individual and organizations in the digital age.