SUPREMO AMICUS

VOLUME 40 | February, 2026 ISSN 2456-9704

PRE-EMPTIVE CYBERSECURITY MEASURES : A COMPARATIVE LEGAL STUDY OF EU AND INDIA

By *Suryansh Srivastava*
From *School of Law Christ (Deemed to be University) – Pune Lavasa Campus*

By *Amrutha Valavi*
Assistant Professor *at School of Law Christ (Deemed to be University) – Pune Lavasa Campus*

ABSTRACT :
The study demonstrates that machine learning is indeed effective in identifying new vectors of attacks, correct zero-day attacks, and combat sophisticated risks such as adversarial AI attacks, polymorphic malware, deepfakes disinformation. This paper will demonstrate deep into the legal front and how law can determine the extent to which AI powered security is embraced, the people who will be responsible and the level to which it can expand. This emphasizes the necessity of explicable and transparent AI in order to trust it and have a stronger cyber ecosystem. The regulatory framework in the EU is risk-based, and the conformity checks are mandatory along with the security-by-design regulations and the mandatory cybersecurity requirements of high-risks AI systems. This demonstrates an initiative form of law-making that is in tandem with technology. The study also highlights that this type of regulation allows organizations to install some pre-emptive cyber precautions and ensure that they do not have loopholes that are aided by algorithms.
On the contrary, the legal framework of India is fragmented. It mainly depends on the Information Technology Act 2000, the Digital Personal Data Protection Act 2023, and a number of advisories rather than actual requirements. Adversarial AI, accountability of algorithms, and necessary risk tests lack a clear regulation, which causes India to fail to scale proactive cyber defence despite its threat environment increasing at a rapid pace. Comparing these routes, the paper raises the question of how these rule books create cyber preparedness and toughness in no less than an artificial intelligence scenario. This paper aims at proposing policy changes and roadmap through which India can borrow a phase based Implementation of the EU risk-oriented strategies to help it prepare better against emerging cyber threats.

KEYWORDS: Pre-emptive cybersecurity, Artificial intelligence regulation, EU regulation, Indian cyber law regulation.

INTRODUCTION :

The accelerating Hack attacks are becoming far more sophisticated and it is disrupting the traditional methods of protection such as signature inspections or rule engines[1]. The surface of attack is growing exponentially with additional cloud, IoT, autonomous stuff, Web 3.0, and colossal automation. Multi-vector attacks can be removed by hackers in a few seconds, which is faster than manual or conventional tools. This is predominantly why AI has come in as a complete game-changer in cybersecurity introducing intelligent and predictive threat modelling, autonomous response, and intelligent anomaly detection[2]. AI systems scan behaviour, can detect network abnormalities, and monitor real-time data to isolate threats unknown by the static signatures[3].

The Traditional defense preparedness focuses on responding to vulnerabilities only after they had begun to manifest it. Due to the centrality of AI to digital

[1] Leka, B., & Leka, D. (2025). *Advancing Cybersecurity through AI : Insights from EU and Candidate Nations*,13 Balt. J. Mod. Computing 166(2025).
[2] K. Achutan, S.Ramanathan, S. Srinivas & R.Raman, *Advancing Cybersecurity and Privacy with Artifical Intelligence: Current Trends and Future Research Directions, Frontiers in Big Data, Art*. 1497535 (2024).
[3] Selcuk Okdem & Sema Okdem, *Artificial Intelligence in Cybersecurity: A Review and a Case Study*, 14 APPL. SCI. 10487 (2024).

defence, it is essential to enact laws. The rules determine the way AI is constructed, trained, examined, utilized, and inspected in its entire process. This creates security and abuse possibilities which can occur at the time. The EU is at the forefront with AI Act and other additional provisions, such as NIS2, the Cybersecurity Act and GDPR[4]. These are the largest worldwide drive to control AI with threat categories, compulsory security scrutiny, strict transparency responsibility, and continuous oversight. At the same time, the legal environment of India continues to crack down. It has been divided, lacks actual AI-specific cybersecurity regulations. Although we have such policies as the Digital Personal Data Protection Act, draft National Cybersecurity Strategies, and sector guidelines, which do not address adversarial AI, automated cyber weapons, or algorithm bugs in their entirety. Therefore, AI-based cyber threats continue to be a challenge to India.

This paper will delve into the interaction between AI and pre-emptive cybersecurity, relying on the studies on AI threat detection, adversarial machine learning, algorithmic obscurity, and governance hiccups. The parallel drawn between the EU legal system as a prevention paradigm, and will discuss how India might follow comparable step-by-step approaches to increase its level of digital resilience.

RESEARCH PURPOSE & OBJECTIVE :

The research question examines the fundamental study on How can the risk-based AI regulatory framework used by the EU support enforceable pre-emptive cybersecurity against the voluntary compliance approach used by India and what does it mean to the security of AI systems?

The study investigates a critical dimension to address this question. Firstly, it will disaggregate how EU AI Act actually realizes pre-emptive cybersecurity, such as their risk classification, obligatory conformity checks, the technical documents that must be submitted, and security-by-design provisions that are actually integrated into the law. Secondly, it will explore the existing AI situation in India, including the recommendations of the Ministry of Electronics and Information Technology (MeitY), the activity of the Computer Emergency Response Team (CERT-In), and industry-specific regulations to understand how self-regulation in reality provides the desired outcomes. Thirdly, it will contrast the enforcement component the tough sanctions by the EU hefty fines and market prohibition against the one of India, which relies on self-regulation by the industry and advisory structures.

Furthermore, the study explores the practicality of the contrasting approaches security for AI system security and investigating whether there is a mandatory pre-emptive measure that will reduce cybersecurity vulnerabilities compared to voluntary standards[5]. This will examine expenses, its impact on innovation, market behaviour and the actual security outcomes observed in the framework of each model. Also, it will reflect on what it entails of multinational AI developers operating both where and whether we can speak of harmonisation or not. Ultimately, it would select the best practices, determine whether the EU model can be adapted to the Indian context, and make evidence-supported recommendations to enhance pre-emptive cybersecurity in artificial intelligence systems at the same time keeping regulations relative and promoting technology development of both locations simultaneously.

RESEARCH METHADOGOLY :

This study employs a primarily methodology which is based on a combination of doctrinal analysis of primary legislation (the EU AI Act, NIS2, GDPR and the EU Cybersecurity Act) and a systematized review of secondary sources, including scholarly articles, policy papers, and regulator guidance. It takes the

[4] Council of the European Union, Regulation (EU) 2024/1689 – *Artificial Intelligence Act* (2024).

[5] Zarif Bin Akhtar & Ahmed Taibuil Rawol, *Enhancing Cybersecurity through Artificial Intelligence (AI)-Powered Security Mechanism*, 9 ITJRD 50 (2024).

provisions of substantive risk based, conformity assessment mechanisms and security by design requirements of the EU framework and compares them to the Information Technology Act 2000 of India, the Digital Personal Data Protection Act 2023 of India and MeitY/CERT In advisories. The qualitative data will be collected using semi structured interviews with regulators, industry practitioners and legal scholars across both jurisdictions in order to capture the realities of implementation, and a gap analysis matrix is used to identify differences in enforcement, accountability and technical standards. It is an iterative process, where the legal mapping is used to guide the design of a more gradual process of policy implementation in India.

LITERATURE REVIEW :

The studies have made it clear that AI is redefining defensive cybersecurity by being able to offer real-time anomaly detection, automated responses to incidents, detecting insider threats, and constantly checking vulnerabilities in complex digital environments[6]. The emphasis of modern research is on the fact that machine and deep learning models accelerate and narrow the behavioural red flags detection, isolate bad nodes, and patch zero-day issues[7]. Some literature enables AI not to be an attractive and helpful add-on, but a fundamental change in favor of pre-emptive and autonomous protection against cybercrime. Systematic reviews indicate that AI-based studies on security are generally interested in intrusion detection, malware classification, federated learning to facilitate privacy-preserving analytics, and resilience against attacks. It also shows the increasing attention to safe data-sharing structures and AI models that can operate in uncertainty in line with the changing threats landscape in the world. Nevertheless, concept drift, algorithm bias and deployment issues still have a gap in their management.

The tech reviews demonstrate advancements in both the IoT and wireless sensor network lockdown and lightweight AI models and adaptive encryption[8]. These trends are used to display how more power efficient, scalable, and context aware security solutions are needed, which can operate on decentralized energy constrained systems. However, in a study, however, the majority of breakthroughs occur in the top-resource labs and this raises unanswered questions regarding whether it can be applied in the context of lower budget or rural locations[9].

Several articles indicate how that use of AI may even create new security vulnerabilities. And continue being extremely consistent regarding the large-scale threats such as data poisoning, model evasion, input manipulation etc. Such attacks are able to disrupt the functioning of an AI, disrupt its forecasts, and lead people to doubt the use of automated security systems. The other big issue that continues to emerge is the level of opaqueness of these systems. The problem with black-box AI is that it is nearly impossible to audit, difficult to comply with regulatory bodies, and unimaginable to hold anyone accountable once a failure happens, particularly when the consequences of such failures can be extremely serious, like in the finance and surveillance sectors or national security[10]. Looking at the cyberspace scenario in India, it is easy to see that there exists a set of structural gaps. The nation remains entangled in outdated legislation which fails to address AI, the supervision of institutions is uncontrollable, actions are lax, and it completely lacks security responsibility of the AI. The existing laws are not even abreast with newer threats such as deepfakes, autonomous malware, AI-based fraud, and algorithmic-accountability concerns. Consequently, the effect is that India is more playing

[6] A.L. Buczak & E. Guven, *A Survey of Machine Learning for Cyber Intrusion Detection*, IEEE Comm. Surveys & Tutorials (2016).
[7] D.Dey & R. Singh, AI in Zero-Day Vulnerability Management, Int'l J. of AI Security (2023).
[8] AI-Driven Security: *How Machine Learning Will Shape the Future of Cybersecurity* (2023).
[9] *Supra Note 1 at Pg. 2*
[10] R. Raji & J. Buolamwini, Actionable Auditing: Investigating Bias in AI, FACCT Proc. (2019).

on the defensive, than on the offensive[11]. Their regulatory background seems to be constructed on the notion that security and AI should be hand-in-hand at any given time. This creates a harmonised, deterrent framework that directly draws the cybersecurity into the heart of AI governance. The strategy of the EU is based on obligatory risk evaluation, the tasks of Security-by-design, ongoing monitoring, and micro organization across the borders. The combination of those rules forms a complete stack strategy that in fact attempts to lock in pre-emptive cyber resilience and provides the digital ecosystem with a safe and stable aesthetic.

LEGAL AND INSTITUTIONAL FRAMEWORK :

1. EUROPEAN UNION -

- The EU AI Act and Risk Based Governance and Cybersecurity Integration –
  The world of regulations set by EU is on a level of the most progressive in the world to incorporate cybersecurity into the book of AI[12]. The most significant is the EU AI Act, which relies on an automated risk system to define and govern AI systems according to their potential societal and security risks to society. High-risk AI, such as the biometrics, critical infrastructure, medicine, policing, etc., must endure the most stringent examination. The Act transforms cybersecurity into a legal requirement that must be met to be compliant, and instead of fixing the bugs when they emerge, it is now looking at the possible attacks even before the product was even developed. This is transforming the response measures to a counter on the offense. The EU is necessitating pre-emptive cybersecurity by compelling developers to think today on the future of attack vectors and drop in defense, as well as making pre-emptive state why nice-to-have than mandatory habeas corpus.

- Implementing Security-by-Design and Security by Default Concepts –
  The security-by-design and security -by- default are the two foundations of the AI Act. A high-risk AI should demonstrate good lifecycle management to maintain constant updates, periodic risk assessment, human supervision, tracking of traceability, as security can no longer rest at the beginning and be diluted over time. This acknowledges that AI evolves with time, particularly when new data or environments are introduced and fast security plans are not so good. The tech innovation and a high degree of systemic risk reduction can be achieved through implementation efforts of digital ecosystem systemic compliance[13]. The promotion of a culture of pre-emptive governance in the AI architecture will increase trust and resilience because security becomes an essential layer of the system rather than an enhanced feature of the operation.

- Conformity Testing as Forms of Enforcement –
  The high-risk AI has to survive a rigorous test to enter the European market or implement it in a sensitive environment, so it must ensure it is robust, accurate, has proper documentation, is transparent, and has cybersecurity measures in place. According to study, such pre-deployment testing is necessary to prevent disastrous events that may arise due to an algorithm malfunction, malicious use, or secret strengths[14]. The

[11] Anuradha Chakraborty et al., *An Analytical Study on Challenges and Gaps in India's Cyber Security framework*, 5 INT'L J. CRIM., COMMON & STATUTORY L. 04 (2025).

[12] Regulation (EU) 2024/1689 of the European Parliament and of the council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J.(L 1689).

[13] Celine Gauthier- Maxence, *European Cybersecurity and AI Framework : Towards Proactive Regulation for a Secure Digital Future*, EU L. LIVE 212 (2024).

[14] Vaios Bolgouras et al., EU Regulatory Ecosystem for Ethical AI & ETHICS 5063 (2025).

requirement of such assessments by the EU means that the issue of security risk is addressed way before it can be miscreant in actual reality.

- Ensuring that the infrastructure is more resistant to cybercrime using the NIS2 Directive- The NIS2 Directive is an addition to the AI Act which fortifies the security responsibilities of critical businesses and significant organisations in the EU- energy, telecoms, finance, healthcare, digital services, you name it. This establishes tough criteria of identifying and reporting incidents, access controls, safety of a supply chain and systemic risk management. A company should have a complete security system that is able to identify the incidences and respond swiftly. The NIS2 strengthens the overall security of the EU as it coordinates its cyber standards and ensures that AI-based systems remain secure[15].

- Cybersecurity Basic in GDPR and Data Protection –
  The GDPR operates as a security backbone. It mandates strict data governance, minimisation, and protection of user's rights. Also, that the such data is processed in accordance with the principle of privacy-by-design and privacy-by-default. The accountability and transparency components of GDPR create an illusion of a safe, reliable environment in which the AI implementation will take place without personal data in appropriation or any other breach of information integrity[16]. This renders data protection to be an unavoidable component of cybersecurity and a method to keep AI systems effective and ethically sound.

- EU Certification Schemes and Cybersecurity Act –
  The EU Cybersecurity Act is the taking of the puzzle together because it implements a pan-European system of certifications of ICT products, cloud services, AI-powered cybersecurity applications. The different certifications standardise benchmarks of security and audit practices in such a way that all the member states are enjoying the same amount of protection. This also promotes digital trust, streamline cross-border operations, enhance stability in supply-chain operations, and cement it[17]. Ultimately, there are opportunities to bring together certification, risk-based governance, data protection, and incident response into a single, consistent, pre-emptive regime with the EU having a strong, legally enforceable cyber safety net based on technical competence.

2. INDIA -

- Weaknesses of the IT Act in a Cyber Threat Landscape Scale Driven by AI –
  In essence, the increasingly slow, yet not quick, evolution of the laws on cybersecurity in India is a consequence of the fact that they are still not adequately suitable to the rapidly expanding AI threat with which we are currently confronted. Its fundamental cyber law is the Information Technology Act, 2000 (IT Act) that addresses hacking, identity theft, data disclosure and cyberterrorism[18]. The Act was drafted prior to the actual relevance of AI, and therefore lacks some of the current risks such as algorithmic manipulation, deepfakes, autonomous malware, machine-learning evasion tricks and giant automated decision-making. Where AI technology can now establish fake identities,

[15] Raluca Csernatoni & Katerina Mavrona, *The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach* (2022).

[16] Blessing Winifed Odume, Regulating AI in Cybersecurity: Challenges and Opportunities (SSRN 2024).

[17] *Supra Note 12 at pg. 5.*

[18] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

evade detection tools as well as interfere with digital infrastructure, the previous law-oriented approach of the IT Act cannot control these novel dangers or hold AI creators and consumers accountable. The latter uncertainty restricts the manner in which India can enhance national cyber preparedness or bring companies to bear on careless AI applications.

- Weaknesses of CERT-In Directions AI-Centric Cybersecurity –
  The incident reporting was conducted to be made successful in the CERT-In Directions (2022) to synchronise the system clocks, standardise retention of logs, and provide timely notifications on attacks[19]. Although that is helpful, it does not address the technological shortcomings of AI systems. The Directions lacks the requirements of adversarial robustness tests, machine-learning models stress tests, data-poisoning attacks, or transparency obligations of AI-facilitated applications[20]. In the absence of such precautions, business owners will be able to deploy AI that responds harshly to minor adversarial modifications or can be intentionally trained to be manipulated in a malicious manner. The absence of AI-specific cybersecurity standards permitting high-risk systems, facial recognition, fraud detection algorithms, predictive policing software, etc, to work with a poor resilience opens the country to smarter attacks.

- Criminal Loopholes in the Digital Personal Data Protection Act (2023) of AI Governance[21] -
  The Digital Personal Data Protection Act (DPDP Act) of 2023 solidifies the privacy regulations in India with establishing the standards of consent, subsection obligation, and individuals on the use of their personal information[22]. Nevertheless, researchers claim that it is insufficient regarding AI-specific problems. This research also examines that it does not have the specifications of transparency, explainability, automated decision review, or reduction of bias in AI models[23]. The Surveillance networks that have been improved with AI, behavioral analytics tools, and predictive algorithms rely on this massive data which can be used to profile or discriminate individuals. And the Lack of AI-specialized security removes privacy and cybersecurity security, and, therefore, there is no detailed law handling the AI-related gathering, processing, and protection of sensitive personal data in India.

- Fragmented Framework of India -
  One of the recurrent issues that is being highlighted is the fragmentation of the ecosystem of cybersecurity in India. Each of the different agencies, CERT-In[24], NCIIPC, MeitY and Ministries of Home Affairs and sector-specific regulators perform portions of the responsibilities, creating overlapping responsibilities and uneven enforcement[25]. During a large cyber-attack, this patchwork hinders the process of national responsiveness. It was also pointed that the number of trained cybersecurity professionals and the relevant skills in governance of AI, the deficiency of

[19] CERT-IN, Guidelines for Chief Information Security officers (Jan. 2022)
[20] S. Nakkeeran & Dharamveer Singh , *Challenges in Cybercrime Prevention and Legal Frameworks in India: An Analytical Study, 21 J. ADVANCES & SCHOLARLY RSCH . ALLIED EDUC. 232 92024).*
[21] The Digital Personal Data Protection Act, No. 22 f 2023, INDIA CODE (2023).
[22] *Ibid.*
[23] Amit Jaiswal & Prakash Chandra Mishra, Artificial Intelligence and Cybersecurity Law: Legal Issues in AI-Driven Cyber Defense and Offense, 5 SHODHKOSH : J. VISUAL & PERFORMING ARTS 555 (2024).
[24] *Supra note 18 at pg. 7.*
[25] NITI AAYOG , National Strategy for Artificial Intelligence (June 2018).

digital forensics systems, and the insufficient training of relevant parts of the anti-hacking AI attack vectors. Such loopholes prevent India to research on sophisticated AI-based cybercrimes or implement the existing regulations properly.

- Increasing Cybercrime and Frail Enforcement Machinery –
  The cybercrime in India is on a boom: ransomware, phishing, online financial fraud, identity spoofing, cyberbullying, etc. However, conviction remains excruciatingly low due to processing bottlenecks and archaic investigation processes. According to the study , the lack of AI-specific laws, combined with the out-of-date IT Act processes, will reduce the capacity of India to counter high-tech threats[26]. AI tools allow criminals to attack more quickly and covertly, and as such, the legal and institutional loopholes of the Indian cyber architecture endanger the security of the nation, its economic stability, and its population.

COMPARATIVE ANALYSIS : EUROPEAN UNION - INDIA

An empirical examination reveals drastic variations in the philosophies and frameworks of AI governance and cyber regulations between that of EU and India. It is found that the EU is risk-centric, preventive and focuses on safety, transparency and accountability. India, on its part, has an active approach of reacting to events based on post-facto inquiries and ad hoc warnings. EU regulations involve risk assessment, conformity test, and security-by-design during the AI live stage, active security habits, whereas India has no such legal obligations[27].

The Systemic strength has been also evident in the layered nature of the machinery of the EU: laws governing AI, data protection laws, sector cyber laws, and certification regimes are all interoperative. Such a layered arrangement maintains cyber norms on digital industries. India on the other hand has used the old IT Act that offers divided structure. It is being noted that India does not have a specific AI organization, and there is a lack of inter-agency cooperation, which develops fundamental vulnerabilities and brings national cyber resilience down[28].

Besides, the implementation instruments provided by EU such as conformity assessments, market surveillance, and incident reporting can be viewed as the warning signals and keep AI developers and operators responsible. India does not have required pre-deployment testing or AI audits, as they allow high-risk tools to be left unmonitored to operate either in prejudice, adversarial breakdown, or explainability. This difference indicates the significant divide at the preparations: the EU is equipped to address the new threats, whereas India is susceptible to systemic exploitation.

It is mentioned that despite the EU establishing a digital trust by enacting stringent privacy laws and cyber legislation, India continues to experience a lack of trust due to the occurrence of data breaches, a lack of accountability, and a weak legal framework to curb AI-driven surveillance or profiling. That destroys the trust in society and curbs the harmless use of AI technologies[29]

The comparative results indicate that the preventive, transparent, and technologically adaptive regulatory frameworks are the key to effective cybersecurity in the age of AI. EU provides us with an example of how legal requirements can lean the technological development towards safety, responsibility, and

[26] *Supra note 19 at pg. 7*
[27] Henrik Nolte et al., Robustness and Cybersecurity in the EU Artificial Intelligence Act, in PROCEEDINGS OF THE 2025 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILTY AND TRANSPARENCY (FAccT'25) (2025).
[28] *Supra note 21 at pg. 6*
[29] Hemanth Kumar B.R., *The Impact of Artificial Intelligence on Cyber Laws in India*, 16 INT'L J. SCI. & TECH. 1(2025).

sustainability[30]. The EU ensures that AI systems do not harm but benefit cybersecurity by imposing rigorous testing, documentation, management, and transparency. This proves that tech innovation and tough regulation are not antagonistic towards one another but rather are symbiotic towards digital trust.
The regulatory issues faced by India are not related to the unrealistic potential of technology, it is related to structural change. It is further noted that India is a fast-growing digital economy, massive artificial intelligence talent, and an expanding technologic infrastructure. However, the absence of preventative regulatory institutions implies that the country is unable to put a restraint on risks before they evolve into harm. According to scholars, unless there are AI-specific considerations of explainability, adversarial robustness, algorithmic bias, and automated decision-making, India will be only responsive and operationalized in cybersecurity.

Also, India faces many challenges in regulatory enforcement such as low technical capacity, institutional ineffectiveness, and a low level of cross-border cooperation pulls down its cyber preparedness. On the other side, the harmonised regulatory system by EU increases the level of coordination amongst member countries, enhances common digital markets and enables holistic threat-response strategies. Thus, this comparative analysis explains why implementing law in cyberspace and matchmaking on a global scale is important when addressing cyber threats embedded in AI.

PRIMARY FINDINGS :

1. The Regulatory Orientation and Governance Ideology –
   The European Union has a risk-based and preventive regulatory philosophy, the safety, transparency, and accountability of an AI system are integrated at all adopted phases of its life cycle. This is demonstrated by the EU AI Act, which stipulates that risk assessments, conformity checks, and security-by-design should be conducted prior to implementation to ensure vulnerabilities are identified early enough and flaws or malicious programs are prevented before the system decides to malfunction or attack others[31]. By comparison, India employs a reactive system of governance, which is based on post-incidents investigation, industry specific advisory and obsolete provisions of the law under the IT Act, 2000[32]. According to scholars, India does not have any laws that compel organisations to assess AI models to adversarial robustness, bias or explainability prior to deployment, which increases the exposure to AI-related threats.

2. Differences in the structure and institutional Framework –
   The regulatory ecosystem of the EU is of a multi-layered and harmonized nature, combining AI-related laws with laws on cybersecurity (NIS2) and data-protection regulations (GDPR) and Eurozone-wide certification systems. The result of this coherence is consistent cybersecurity standards in sectors. The organization of India is however torn and old fashioned, with regulatory duties being fragmented between CERT-In, MeitY and other sector organisations[33]. A lack of a specialized artificial intelligence controller or coordinated mechanism of enforcement creates inherent vulnerabilities on a systemic level and uneven national cyber preparedness.

3. Enforcement Capacity and Trust in the State –
   The Amplified compliance between the EU is enforced with the conciseness of the conformity tests and market mapping and accountability,

[30] Vaios Bolgouras et al., EU Regulatory Ecosystem for Ethical AI, 5 AI & ETHICS 5063(2025).
[31] Regulation (EU) 2024/1689 of the European parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).
[32] *Supra Note 17 at pg. 7*
[33] CERT-IN, Guidelines for Chief Information Security Officers (Jan.2022).

which require secure and transparent AI systems. In India, there are no checks exist to perform before deployment and potentially high-risk AI tools are left to work without formal auditing. Consequently, the EU develops increased digital trust, and India is confronted by social distrust towards the frequent cases of data breach and the absence of legislation to protect against AI-based threats. These variations explain why India needs to implement preventive decisive regulations.

RECOMMENDATIONS AND POLICY FRAMEWORK :

1. EUROPEAN UNION -

- Improving SME Support of AI Act Implementation –
  Even though the European Union has one of the most complex AI and cybersecurity regulation systems, the population-level support of small and medium-sized enterprises (SMEs) remains a priority. The EU technology landscape consists of SMEs that constitute a significant portion of the tech system yet are commonly unable to meet the financial, technical, and administrative needs of the high-risk AI compliance. As a solution, the EU can expand the technical assistance programmes, implement specific funding initiatives and invoke so-called regulatory sandboxes allowing SMEs to test AI systems under a closely monitored, low-risk environment[34]. Such actions would assist the SMEs in the safety and cybersecurity needs without suffocating innovation, competition and operational capacity.

- Improving Conformity Evaluations Standards in High Risk Sectors –
  The other major area of improvement is to strengthen the conformity assessment in the AI Act. Replacement of old methods by newer assessment tools might fail to integrate sector risks as the adversarial AI threats develop in multiple sectors such as medical care, banking, transit, and critical infrastructure. It would be possible to build finer, context-specific testing conditions that would help the auditors compare vulnerabilities more objectively and guarantee that AI systems going to the EU market will be resistant to upcoming cyber threats[35]. Landmarking of such tests would enhance conformity and a sense of reliability in users, developers and regulators.

- Enhancing the EU Cybersecurity Research and Innovation Ecosystems –
  The long-term resiliency expresses the need to invest in the long-term cybersecurity research and innovation landscape in Europe[36]. EU must fund specialised research centres, encourage the formation of partnerships between the public and the industry and the extension of more advanced ranges of cyber Attacks that would occur on a scale with the intention to simulate a large scale attack and test the defensive mechanisms. These measures would help streamline the development of advanced AI-based malware detection, prediction, and neutralisation solutions to identify, predict, and mitigate advanced patterns of threats. With the development and support of a culture of innovation solution, the EU will be able to maintain its technological dominance and at the same time provide sufficient safeguards against increasingly sophisticated cyber offenders.

- Growing Digital Forensics and Incident Response Cross-border Operations –

[34] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Artificial Intelligence in Society* (2019).
[35] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), *Cybersecurity Certification: European Scheme for ICT Products* (2020).
[36] Fei Su et al., advancing the Role of the European Union in Promoting Global Cyber Stability (SIPRI. Plo'y Paper Dec. 2023).

Lastly, to safeguard the Digital Single Market in the EU, cross-border cooperation in digital forensics and incident response is needed to strengthen. In these cases, cyber threats tend to move across national borders, which makes the partnership of investigative skills inevitable. Paying closer attention to the development of a better-knit network of digital forensics units, which are able to cooperate on intelligence exchange, to joint investigations and to quick exchange of technical expertise on large-scale cyber-attacks would significantly enhance the overall capacity of the EU to respond to major cyber-attacks. This co-operation would ease enforcement and enhance the and strength and cohesion of the larger EU cybersecurity structure.

2. INDIA -

- Building Institutional and technical Capacity -
  The broad institutional and technical capacity building must commence, and India should implement a differentiated, context sensitive regulatory framework. Being a fast-evolving yet a little poor economy, the informational trend of regulation in India today should not rush in introducing the strict EU-style commitments and bombard native institutions and businesses, causing inefficient adherence and retarded innovations. Rather, the urgent need should be the enhancement of the institutional capacity concerning the critical levels of regulatory and enforcement functions, including CERT-In, NCIIPC, MeitY, state-level cyber-cells, and data protection institutes. It is possible to eliminate the risks through fitting professional certification channels in AI safety, adversarial machine learning, digital forensics, and cybersecurity risk analysis, promoting academic partnerships, and targeted training programs to empower regulators with the means to assess the algorithmic systems, identify their vulnerabilities, and react to the arising issues. The establishment of such human capital comprises the basic layer upon which the regulatory framework can be put in place in future with a lot of success.

- Improving Inter- Agency coordination and Cyber Governance Architecture -
  The cybersecurity situation in India is characterized by cracks in responsibilities and mandate overlay among organizations. The consequence of this fragmentation is the lack of consistency in enforcement, slow response to threats, and gaps in regulations. This makes it important to strengthen mechanisms of coordination in order to have coherent governance of a country[37]. With implementation of combined command schemes, centralised threat intelligence organs, and expedited and direct communication at CERT-In/NCIIPC and to the sectoral regulators and state cyber cells, the government can significantly enhance the preparedness to cyber-attacks. A centralized national incident reporting system, cross-agency auditing and sharing data would eliminate overlaps and produce a more resilient, synchronized cybersecurity structure that can deal with AI-driven threats.

- Adopt phased and Adaptive Regulatory Exercise -
  The Strengthening of Indian industries is a key aspect, considering that it has varied abilities. India must initially include a set of ethical, transparent, and responsible AI adoption guidelines to the government and the applications in the public sector so that they can be used as a national standard without overloading the private sector. Also, AI-based regulatory sandboxes would facilitate staged testing, risk-taking, and part-experimental learning when arbitrating binding commitments. Such sandboxes are able to test such critical issues as explainability of

[37] *Supra Note 27 at pg. 9.*

algorithms, bias reduction, robustness against adversarial examples, and automated decision-making[38]. India could allow a slow, evidence-based regulatory implementation approach to enable the ecosystem to be ready to embrace more all-inclusive AI laws in the future.

POLICY RECOMMENDATION : PHASED IMPLEMENTATION MODEL

PHASE 1	PHASE 2	PHASE 3
Foundational Stage Companies in the 1st Stage are encouraged not being forced to follow basic AI safety guidelines. Training and awareness programmes which will help people to understand the risk of artificial Intelligence. The government and industry should start working together and set up small expert groups to further prevent Risk.	Sector Specific Mandatory Rules Rules in this phase had become slightly strict, but not only for important sectors like finance, healthcare and critical infrastructure. AI system can be tested safely inside a regulatory sandbox before it is set to be released out. For the startups and low-risk users they get lighter rules so it does not affect new innovation.	National Framework Rules become clearer and more organised and now India has enough skilled experts, labs and testing systems and is being moved to strong national law. All-important AI systems go through audits, testing, and certification to ensure that there are a safety and cyber-check before it is being released.

The EU has been experiencing the Pre-emptive AI cybersecurity principles, which India can be willing to adopt, through a gradual risk-based, and capacity-building approach as opposed to an outright copying of the EU model in all its strictness. India can first in the initial stage provide voluntary principles on AI Security-by-design, initiate prelim risk-classification systems, introduce countrywide awareness programmes and introduce A regulatory sandboxes to test risky AI systems in a safe manner. The second phase explores where India is able to progressively make high-risk sectors, including finance, healthcare, transport, and important infrastructure, subject to mandatory rules, but startups and low-risk sectors should take flexible paths with the low-burden compliance requirements. The last phase would bring with it a comprehensive national AI cybersecurity legislation that has structured audits, adversarial testing, certification schemes and harmonisation with adapted EU standards. This gradual strategy would be enough to enhance the regulatory intensity in accordance with the increase of the technical capacity, the maturity of the institution and the economic preparedness of India and thus Pre-emptive AI cybersecurity can be both possible and sustainable in a developing country like India.

CONCLUSION :

It has emerged that artificial intelligence has turned out to be a disruptive technology in the area of cybersecurity in particular in the manner organisations, identifying, analysing and responding to cyberattacks. The features of AI-powered systems are far superior to the features of traditional cybersecurity tools and enable real-time anomaly detection, predictive threat modelling, automatic response to incidents, and advanced behavioural analytics. This means that such inventions can help security infrastructure to transcend stagnant, signature-based design of infrastructures to dynamic and adaptive defence designs capable of sensing new attack patterns and responding in machine time. The

[38] Trajkovska Elena et al., Prevention of Cybercrime in the Age of Artificial Intelligence (AI) Within the European Union, in 11TH INT'L SCI. CONF. PROC. (Pearl Blue Rsch. Grp. Ed., 2025).

qualities that make AI powerful, however, introduce novel types of risks that have never been encountered. Accountability is threatened by algorithmic opacity which refers to the state of affairs in which the decision-making process becomes difficult to comprehend[39]. This type of adversarial manipulation, such as data poisoning, model evasion, and synthetic identity attacks, puts vulnerabilities in such a way that they can no longer be adequately addressed using traditional security structures. Besides this, AI-dependent systems will also be more likely to spread systemic risks in the sense that they will enable automated cyberattacks to propagate promptly by using digital ecosystems. Only under the condition that technological advancement will be accompanied by the system of governance which is preventative, transparent and capable of changing together with any new threats the full potential of AI to offer cybersecurity as the modern literature suggests can be reached.

To this extent, the European Union is a pioneer in applying the logic of cybersecurity requirements into the AI governance in the world. EU has adopted a risk-based governance approach to preventative security using a highly complex and multidimensional regulatory framework incorporating the AI Act, the General Data Protection regulation or GDPR, and the EU Cybersecurity Act. The AI Act demands high countries to possess a more rigorous pre-deployment risk judging, conformity check, and data regarding lifecycle management of the high-risk AI systems. This will ensure that the vulnerabilities in the area of cybersecurity are identified at an early age and addressed when such systems are not yet within the societal or critical infrastructure domain. The ecosystem will be enhanced by GDPR through its requirement of accountability, data protection and data breach notification protocols that would restore the integrity of data utilized to train and run AI systems. At the same time, the NIS2 Directive and the Cybersecurity Act increase the overall resilience in the cyber domain standardizing the security requirements, introducing certification frameworks, and enabling the co-ordinated gamification of the cyber incident response of the member states[40] . All of these devices institutionalise Cybersecurity-by-design and puts the EU in a normative position of the responsible use of the AI.

India's at a big turning point. It also possesses one of the most active and fast-growing digital economies and a substantial amount of innovation based on AI, and the regulation has not been coordinated yet. It lacks specific AI legislation, the IT Act is old and the regulation is spotty. This disrupted banking, healthcare, e-governance and telecoms putting them at risk of AI-based cyber-attack. The current system does not require hard adversarial tests, provide transparency of algorithms, and requires inadmissible standards of the use of the high-risk AI. They argue that we should adopt the preventative approach of the EU, including require explainability, assure robustness, certifications and a domestic policy on AI, to keep up with India.

India should begin to reform the post facto enforcement strategy in the future through the use of a risk-based strategy. The various ways in which India can have a stable and reliable AI ecosystem include improving the institutional capacity, which will improve interagency coordination and introduce the rules gradually that are aligned with the local investment in tech preparedness. The future of cyber security will be pegged upon the harmonization of the policies with the technological progress the two are a dynamic balancing forward and backward that the EU and India need to keep perfecting in order to keep their digitalized societies safe.

*****

[39] *Supra Note 11 at pg. 5.*

[40] *Supra note 23 at pg. 11.*