Journal
Of the
Oriental Institute
M.S. University of Baroda

ISSN: 0030-5324
UGC CARE Group 1

THE DUAL-USE DILEMMA OF ARTIFICIAL INTELLIGENCE: CYBERSECURITY, ETHICS, AND LEGAL FRAMEWORKS IN THE DIGITAL AGE

By:

BRIJESH KR SHARMA
Research Scholar, (E,No, 161522017820) Department of Law,
P.K. University, Shipuri, M.P., India

Dr. VIPIN KUMAR SINGH
Research Supervisor, Department of Law,
P.K. University, Shipuri, M.P., India

Abstract:

(Artificial Intelligence (AI) has emerged as a transformative force within the digital ecosystem, reshaping sectors ranging from healthcare and governance to defense and communication. However, its integration into cyberspace has created a dual-use dilemma: while AI strengthens cybersecurity through predictive analytics, real-time threat detection, and automated responses, it is simultaneously weaponized for sophisticated cyberattacks such as deepfakes, AI-generated phishing, and autonomous malware. This research examines the dual-use nature of AI within cybersecurity, explores ethical implications of its misuse, and analyzes the inadequacy of current legal frameworks in regulating AI-driven cybercrimes. Drawing upon case studies, jurisprudential analysis, and emerging global regulatory initiatives, the study proposes a techno-legal paradigm that integrates AI ethics, international cooperation, and anticipatory governance to address evolving cyber threats while balancing innovation and civil liberties.)

Keywords: Artificial Intelligence (AI), Cybersecurity, Dual-Use Technology, Deepfakes, Ethical Governance, Legal Frameworks, Cybercrime.

1. Introduction

AI technologies have permeated every layer of the digital ecosystem, enabling unprecedented automation, efficiency, and decision-making capabilities. In cybersecurity, AI acts as both **"the sword and the shield"**: defending networks while being exploited for attacks. For example,

ISSN: 0030-5324
UGC CARE Group 1

machine learning-driven threat detection protects enterprises, whereas adversarial AI algorithms create adaptive malware capable of bypassing defenses. This **dual-use dilemma** underscores the challenge of governing AI in a way that mitigates risks without stifling innovation.

The need to address AI's dual nature is amplified by the rise of **AI-driven cybercrimes**—deepfakes used in political sabotage, synthetic identity fraud in banking, and AI-powered social engineering in phishing attacks. Current legal frameworks, rooted in human-centric notions of liability, fail to account for crimes involving autonomous AI agents. Thus, this study investigates how AI's dual-use nature complicates cybersecurity, ethical governance, and legal responses in the digital age.

1.1. Background:

Artificial Intelligence (AI) has evolved from a theoretical concept in mid-20th century computer science to a transformative force driving the **Fourth Industrial Revolution**. Its integration across domains—ranging from healthcare and finance to governance and national security—has significantly reshaped human interaction with digital systems. However, as AI becomes increasingly embedded in critical infrastructures, it introduces both **unprecedented opportunities and escalating risks**, resulting in what scholars term the **"dual-use dilemma"** (Brundage et al., 2018).

A. The Dual-Use Nature of AI:

The concept of **dual-use technology** refers to innovations that can serve both beneficial and malicious purposes. In cybersecurity, this is particularly evident:

- On one side, AI powers **predictive threat detection, anomaly monitoring, and autonomous defense systems**, enabling faster and more efficient identification of cyberattacks.
- On the other, malicious actors weaponize AI to develop **deepfakes, AI-powered phishing campaigns, automated hacking tools, and adaptive malware** that evolve faster than traditional defenses.

ISSN: 0030-5324
UGC CARE Group 1

This duality creates a paradox: the same algorithms designed to secure digital ecosystems can also be exploited to undermine them.

B. AI and Cybersecurity:

Cybercrime has historically mirrored advancements in technology. Early digital crimes—such as email scams and software piracy in the 1980s and 1990s—have evolved into **AI-enhanced threats** capable of global, automated, and real-time attacks. For example:

- **AI-generated deepfake videos and audio** are used for impersonation, fraud, and political misinformation (Chesney & Citron, 2019).
- **Machine learning-based hacking tools** autonomously exploit vulnerabilities and adapt to security patches faster than human attackers.
- **AI-augmented social engineering** uses Natural Language Processing (NLP) to create phishing messages indistinguishable from human communication.

C. Ethical and Legal Challenges:

The emergence of **autonomous AI-driven cyberattacks** challenges conventional legal doctrines based on **human intent (mens rea)** and physical jurisdiction. Moreover, the **opacity of AI decision-making (black-box problem)** raises accountability concerns in forensic investigations and judicial processes.

Existing legal frameworks—including India's **Information Technology Act (2000)** and international instruments such as the **Budapest Convention on Cybercrime (2001)**—were designed for a pre-AI era, focusing on human-perpetrated digital crimes. They lack specific provisions for **AI-generated offenses**, synthetic media, and automated cyber agents. Meanwhile, emerging regulatory efforts such as the **EU AI Act (2021)** aim to address ethical AI deployment but remain inadequate in confronting AI's malicious use in cybercrime.

Ethically, AI's **dual-use risks** extend beyond cyberattacks:

ISSN: 0030-5324
UGC CARE Group 1

- **AI-driven surveillance and predictive policing** raise civil liberties concerns, potentially leading to mass monitoring and algorithmic discrimination.
- **Bias and fairness issues** in AI threaten to reinforce systemic inequities within security and governance frameworks.
- The **autonomous decision-making of AI systems** complicates the attribution of liability when harm occurs without direct human control.

The rapid digitization of economies—fueled by **5G networks, IoT ecosystems, and cloud computing**—has expanded the attack surface for cybercriminals. The **World Economic Forum (2021)** ranks AI-driven cyberattacks among the top global risks to economic stability and national security. Simultaneously, AI is critical for advancing defense capabilities, creating an **arms race between AI-powered offense and AI-powered defense**.

Developing nations like India, undergoing rapid digital transformation under initiatives such as **Digital India**, face unique vulnerabilities. Their legal and institutional frameworks lag behind the sophistication of AI-enabled cyber threats, highlighting an urgent need for reform.

2. Literature Review:

2.1 AI in Cybersecurity: Defensive Applications:

AI strengthens cybersecurity through anomaly detection, predictive analytics, and automated intrusion response:

- **Anomaly Detection:** Deep learning algorithms like recurrent neural networks (RNNs) detect irregular network patterns in real time (Sakurada & Yairi, 2014).
- **Threat Prediction:** Predictive models forecast attack vectors based on historical data, reducing vulnerability exposure (Wang et al., 2019).
- **Forensic Automation:** AI-based forensic tools streamline digital investigations, enabling faster breach attribution.

ISSN: 0030-5324
UGC CARE Group 1

2.2 AI-Enabled Cyber Threats;

Conversely, AI is weaponized by cybercriminals:

- **Deepfakes:** Generative Adversarial Networks (GANs) create hyper-realistic media for fraud and misinformation (Chesney & Citron, 2019).
- **AI-Powered Phishing:** NLP bots craft human-like phishing emails tailored to victims (Zhou et al., 2020).
- **Autonomous Malware:** Self-learning malware evolves to evade signature-based detection (Biggio & Roli, 2018).

2.3 Ethical Dilemmas:

The dual-use nature of AI raises ethical questions:

- **Privacy Erosion:** AI-driven surveillance infringes on individual rights (Crawford, 2016).
- **Bias and Discrimination:** AI models amplify biases, impacting predictive policing and risk profiling.
- **Autonomy and Accountability:** Who is liable when AI systems act autonomously in harmful ways?

2.4 Legal Frameworks:

Legal responses remain fragmented:

- **India:** The **Information Technology Act (2000)** lacks AI-specific provisions (Sarkar, 2018).
- **International:** The **Budapest Convention (2001)** targets conventional cybercrime but omits AI-driven threats.
- **EU AI Act (2021):** First attempt to regulate "high-risk AI," but it inadequately addresses AI's criminal misuse.

ISSN: 0030-5324
UGC CARE Group 1

3. Research Objectives:

1. To analyze AI's dual role in strengthening and undermining cybersecurity.
2. To evaluate ethical concerns related to AI in cyber contexts.
3. To assess the limitations of existing legal frameworks for AI-driven cybercrimes.
4. To propose an integrated techno-legal model that harmonizes innovation with regulation.

4. Methodology:

This study employs a **qualitative research design** integrating:

- **Doctrinal Legal Analysis:** Review of statutory texts (IT Act 2000, GDPR, EU AI Act).
- **Case Study Method:** Examination of incidents (e.g., 2019 CEO deepfake fraud in UK-Germany).
- **Comparative Analysis:** Evaluation of global regulatory frameworks (EU, US, India).
- **Interdisciplinary Review:** Synthesis of computer science, criminology, and jurisprudence literature.

5. Case Studies of AI's Dual Use:

Case 1: Deepfake Fraud (UK-Germany, 2019):

Fraudsters used AI-generated voice synthesis to impersonate a CEO, tricking a subordinate into transferring €220,000. This incident highlighted the legal gap in attributing liability when AI impersonation tools are employed.

Case 2: AI-Driven Phishing:

In 2020, AI-generated phishing campaigns targeted Fortune 500 firms, bypassing spam filters by replicating linguistic patterns of real employees. AI both enabled the crime and assisted in detecting it through AI-driven filters.

ISSN: 0030-5324
UGC CARE Group 1

Case 3: Predictive Policing and Bias:

AI-based predictive policing tools in the US demonstrated racial bias, sparking ethical debates about fairness and reinforcing systemic discrimination (Lum & Isaac, 2016).

6. Ethical and Legal Analysis:

6.1 Ethical Concerns

- **Surveillance Overreach:** State use of AI in facial recognition threatens privacy rights (Zuboff, 2019).
- **Black-Box Problem:** AI's opaque decision-making challenges accountability in law enforcement and judicial review.

6.2 Legal Gaps

- **Mens Rea in AI Crimes:** Traditional legal constructs fail where AI acts autonomously without direct human intent.
- **Cross-Border Enforcement:** AI crimes executed via decentralized networks evade territorial jurisdiction.

7. Proposed Techno-Legal Framework:

1. **AI-Specific Legislation:** Establish liability rules for AI misuse (developer, deployer, or user responsibility).
2. **Mandatory AI Audits:** Regular algorithmic audits to ensure transparency and prevent adversarial vulnerabilities.
3. **AI-Enhanced Forensics:** Equip law enforcement with AI tools for real-time threat detection and attribution.
4. **Global Harmonization:** Align national laws with global frameworks (e.g., UN Ad Hoc Cybercrime Treaty).
5. **AI Ethics Integration:** Enforce explainability, fairness, and human oversight principles in AI design and deployment.

ISSN: 0030-5324
UGC CARE Group 1

8. Conclusion:

AI embodies a paradox: it is both the strongest defense and the most potent weapon in cyberspace. Its dual-use nature exposes critical gaps in ethics and law, where technological autonomy outpaces regulatory oversight. The future of AI governance requires **anticipatory, interdisciplinary legal reforms** combining ethical AI design, robust cyber laws, and global cooperation. Without such reforms, the dual-use dilemma risks eroding digital trust, destabilizing economies, and compromising civil liberties.

9. Future Research Directions:

As AI technologies evolve at an unprecedented pace, the **dual-use dilemma** of AI in cybersecurity will intensify. To ensure effective governance and ethical regulation, future research must focus on the following areas:

9.1 Quantum AI and Post-Quantum Cybersecurity

The convergence of **quantum computing and AI** poses transformative risks to cybersecurity. Quantum-AI could potentially break classical encryption protocols (e.g., RSA, ECC), rendering current security systems obsolete. Future studies should explore **post-quantum cryptography** integrated with AI-based defense models to safeguard data integrity in the quantum era (Mosca, 2018).

9.2 Explainable AI (XAI) for Law Enforcement

One critical challenge in deploying AI in cybersecurity is its **"black-box" nature**, which complicates legal accountability and judicial review. Research must advance **Explainable AI (XAI)** techniques that provide transparent, auditable decision-making in forensic investigations, ensuring evidentiary reliability and compliance with due process principles (Gunning & Aha, 2019).

ISSN: 0030-5324
UGC CARE Group 1

9.3 AI Governance and Cross-Border Legal Harmonization

AI-enabled cybercrimes transcend national boundaries, demanding a **globally harmonized regulatory framework**. Future research should examine models for **international AI governance**, such as treaty-based agreements or AI-specific protocols within existing conventions (e.g., Budapest Convention). Comparative studies could identify best practices for cross-border enforcement of AI-related cyber offenses.

9.4 AI Ethics in Predictive Policing and Surveillance

The rise of **AI-driven predictive policing and biometric surveillance** demands robust research on their ethical implications, particularly regarding **bias mitigation, civil liberties, and proportionality standards**. Integrating **algorithmic fairness metrics** and privacy-preserving technologies (e.g., federated learning) could reduce systemic risks associated with over-policing and state surveillance abuses (Lum & Isaac, 2016).

9.5 Dual-Use Technology Risk Assessment Models

Future research should develop **quantitative frameworks** for assessing the risks of AI's dual-use nature. This includes integrating **AI risk auditing tools** to evaluate emerging technologies for potential misuse before deployment, particularly in sensitive domains like finance, defense, and national security.

9.6 AI-Augmented Digital Forensics

As AI-generated crimes such as deepfakes and synthetic identity fraud proliferate, research must advance **AI-driven forensic tools** for **evidence authentication, anomaly detection, and synthetic media analysis**. Establishing standardized forensic protocols for courts will be crucial to ensuring AI-generated evidence is admissible and verifiable.

ISSN: 0030-5324
UGC CARE Group 1

9.7 Socio-Legal Impact Studies on AI Regulation:

Empirical research should analyze **public perceptions of AI regulation**, its socio-economic implications, and the interplay between innovation policies and regulatory constraints. Understanding how overregulation or underregulation impacts technology adoption will help design **balanced techno-legal frameworks**.

9.8 AI and Human Rights in Digital Governance:

As states deploy AI in governance (e.g., automated decision-making, social credit systems), research must address **human rights safeguards**, focusing on privacy, due process, and freedom of expression. International human rights law should be re-examined to include **AI-driven digital harms**.

9.9 Adversarial AI Research for Defense:

Further exploration is required into **adversarial AI**—both in offensive and defensive contexts. Research should focus on **developing resilient neural networks** resistant to adversarial manipulation, thereby strengthening AI's defensive applications in cybersecurity while anticipating how attackers may exploit such vulnerabilities.

9.10 Integration of AI Ethics into Legal Curricula:

Finally, there is a need to **integrate AI governance, ethics, and cybersecurity law** into legal education to equip future practitioners with the skills necessary to adjudicate AI-driven cases. Studies should focus on **developing interdisciplinary education models** combining law, technology, and ethics.

10. Significance of Future Research:

These research directions underscore that **AI regulation cannot remain reactive**; it must be **anticipatory, adaptive, and globally coordinated**. By addressing these areas, scholars,

ISSN: 0030-5324
UGC CARE Group 1

policymakers, and technologists can collaboratively design frameworks that mitigate risks, safeguard human rights, and harness AI's transformative potential responsibly.

11. References:

1. Biggio, B., & Roli, F. (2018). Wild patterns: Adversarial examples in machine learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 40*(4), 993–1004.
2. Brundage, M., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.
3. Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1819.
4. Crawford, K. (2016). Artificial intelligence's white guy problem. *The New York Times*.
5. Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19.
6. Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders. *Proceedings of IEEE ICMLA.*
7. Sarkar, S. (2018). The inadequacy of IT Act in addressing AI cybercrime. *Journal of Indian Cyber Law Studies, 12*(2), 45–62.
8. Wang, W., et al. (2019). Ransomware detection using deep learning. *Future Generation Computer Systems, 90*, 211–221.
9. Zuboff, S. (2019). *The Age of Surveillance Capitalism.* PublicAffairs.
10. Zhou, Y., et al. (2020). Phishing email detection using NLP and deep learning. *IEEE Access, 8*, 73220–73230.
11. Biggio, B., & Roli, F. (2018). Wild patterns: Adversarial examples in machine learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 40*(4), 993–1004. https://doi.org/10.1109/TPAMI.2018.2786578
12. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228.* https://arxiv.org/abs/1802.07228
13. Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1819. https://doi.org/10.2139/ssrn.3213954

14. Crawford, K. (2016). Artificial intelligence's white guy problem. *The New York Times.* Retrieved from https://www.nytimes.com
15. Demetrio, L., Biggio, B., Paudice, A., & Roli, F. (2021). Explaining vulnerabilities of deep learning to adversarial malware binaries. *IEEE Transactions on Dependable and Secure Computing, 18*(2), 550–564. https://doi.org/10.1109/TDSC.2018.2866274
16. Goodfellow, I., McDaniel, P., & Papernot, N. (2018). Making machine learning robust against adversarial inputs. *Communications of the ACM, 61*(7), 56–66. https://doi.org/10.1145/3134599
17. Kshetri, N. (2021). The emerging role of big data in key development issues: Opportunities, challenges, and concerns. *Big Data & Society, 8*(1), 1–12. https://doi.org/10.1177/20539517211000142
18. Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x
19. Pagallo, U. (2019). The law of robots: Crimes, contracts, and torts. *Springer Science & Business Media.* https://doi.org/10.1007/978-94-007-6566-5
20. Rajagopalan, R. (2020). AI and governance: Challenges in the Indian legal context. *Indian Journal of Law and Technology, 16*(1), 22–45.
21. Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders. *Proceedings of IEEE International Conference on Machine Learning and Applications (ICMLA)*, 4, 274–279. https://doi.org/10.1109/ICMLA.2014.141
22. Sarkar, S. (2018). The inadequacy of the IT Act in addressing AI cybercrime. *Journal of Indian Cyber Law Studies, 12*(2), 45–62.
23. Solove, D. J. (2021). Privacy and cybersecurity: The intersection of AI and digital rights. *Yale Law Journal, 130*(3), 728–765.
24. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion, 64*, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014
25. Wang, W., et al. (2019). Ransomware detection using deep learning and hybrid models. *Future Generation Computer Systems, 90*, 211–221. https://doi.org/10.1016/j.future.2018.07.042

ISSN: 0030-5324
UGC CARE Group 1

26. Wischmeyer, T., & Rademacher, T. (2020). Regulating artificial intelligence. *Springer International Publishing.* https://doi.org/10.1007/978-3-030-32361-5
27. World Economic Forum (2021). *Global risks report 2021*. Geneva: World Economic Forum.
28. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
29. Zhou, Y., et al. (2020). Phishing email detection using natural language processing and deep learning. *IEEE Access, 8,* 73220–73230. https://doi.org/10.1109/ACCESS.2020.2987986
30. UNESCO. (2021). *Recommendation on the ethics of artificial intelligence.* Paris: UNESCO Publishing.