Formulating Global Policies and strategies for Combating Criminal Use and Abuse of Artificial Intelligence

Abstract

This study investigates the criminal use and abuse of artificial intelligence (AI), exploring the effectiveness of various mitigation strategies. It employs a mixed-methods approach, combining quantitative data from a survey of 211 experts with qualitative insights from academic, governmental, and industrial publications. The research examines four key hypotheses: the impact of public and organizational awareness, the role of advanced detection technologies, the effectiveness of ethical guidelines, and the influence of penalties and enforcement. The findings reveal that awareness, technology, ethics, and enforcement all contribute to mitigating AI misuse. The study concludes by proposing comprehensive strategies, including targeted awareness campaigns, investment in detection technologies, robust ethical guidelines, and strengthened legal frameworks, to effectively combat the criminal use of AI.

Keywords: Artificial Intelligence, AI misuse, cybercrime, ethical guidelines, regulatory frameworks

1. Introduction

Artificial Intelligence (AI) has become an integral part of modern society, driving innovation and efficiency across various sectors from healthcare to finance, transportation, and beyond, promising unprecedented benefits. In healthcare, AI enhances diagnostic accuracy, optimizes treatment plans, and supports patient management through predictive analytics [1]. Financial institutions also leverage AI for fraud detection, risk management, and personalized customer services. In addition, AI has shown tremendous success in powering autonomous vehicles, improving traffic management, and enhancing logistics efficiency. However, the rapid advancement and integration of AI technologies also bring significant risks, particularly in the act of criminal activities [2]. The misuse and abuse of AI for malicious purposes such as cyber-attacks, identity theft, and the creation of deep fakes have emerged as pressing global concerns, undermining social trust and security, thus necessitating urgent and effective responses. According to Fekete and Rhyner [3], the reach of these activities

transcends geographical boundaries, thus complicating the formulation of global policies and strategies to address the issue.

Studies have affirmed the growing threat and lethality of AI systems at the disposal of malicious actors in coordinating cyber-attacks employing sophisticated algorithms to breach security systems, steal sensitive information, and disrupt services [4][5][7]. Similarly, Azhar [6] avers that AI-driven malware can adapt and evolve, evading traditional detection methods and causing extensive damage such as mining personal data from various sources to create detailed profiles for fraudulent activities. Hutter and Hutter [8] argue that the existing regulatory frameworks and policies addressing AI misuse globally are often fragmented and lacking cohesion, thereby limiting their effectiveness in combating these sophisticated threats. National and international regulations vary widely in scope and enforcement, leading to inconsistencies that can be exploited by malicious actors. For instance, while some countries have stringent data protection laws, others have minimal regulations, creating loopholes that facilitate cybercrime [9]. Moreover, the rapid pace of AI advancement exceeds the ability of regulatory bodies to adapt, resulting in outdated or insufficient policies. These challenges require comprehensive and coordinated approaches to address them effectively, necessitating collaboration between governments, private sectors, and international organizations to develop robust and adaptive policies [10]. Therefore, this study analyzes the methods by which AI might be hijacked for malicious ends and to develop strong global policies to prevent these risks. The study aims to:

1. To analyze the current state of AI-related criminal activities.

2. To evaluate existing global policies and strategies addressing AI misuse.

3. To identify gaps and challenges in the current regulatory frameworks.

4. To propose comprehensive strategies for mitigating the criminal use of AI.

2. Literature Review

According to Kaloudi and Li [11], malicious actors leverage AI to conduct complex and highly adaptive cyber-attacks that traditional security measures struggle to counter as AI-driven malware can learn from and adapt to defensive measures, increasing its effectiveness and persistence. These advanced forms of malware can autonomously identify vulnerabilities, penetrate security defenses, and execute attacks with minimal human intervention thereby constituting significant challenges for cybersecurity

professionals to detect and mitigate threats promptly, leading to prolonged breaches and significant damage [12][13]. Fitzpatricket al. [14] highlights that cyber criminals leverage AI Algorithms to aggregate and analyze vast amounts of personal data from various sources, creating comprehensive profiles that facilitate fraudulent activities. This data mining capability enables criminals to execute identity theft schemes, often bypassing traditional security checks. The stolen identities can be used for financial fraud, unauthorized access to services, social engineering acts, and other illicit activities, causing substantial harm to victims [15][17]. The Equifax breach in 2017 that exposed millions of social security numbers, reveals how much damage cyber criminals can wreak, especially with the immense power and capabilities of Artificial intelligence [16][18].

Deepfakes represent one of the most concerning applications of AI in criminal activities. This technology leverages deep learning techniques to produce hyper-realistic digital manipulations of images, audio and video contents, making it appear as though individuals are saying or doing things they never did [F]. The potential for deepfakes to spread misinformation and disinformation is profound, with significant implications for public trust and political stability. For instance, deepfake videos have been used to influence public opinion during elections, disrupt political processes, and damage reputations. The ability of deepfakes to deceive viewers and spread rapidly through social media platforms exacerbates their impact, necessitating robust detection and mitigation strategies [19][20][21].

The abuse of AI extends to other areas, such as autonomous vehicles and drones, where AI systems can be hijacked or manipulated for criminal purposes [22][25]. Autonomous vehicles can be commandeered remotely to cause accidents or be used as weapons, while drones equipped with AI functions can be utilized for surveillance, smuggling, or even delivering harmful payloads. For instance, in 2015, some researchers successfully developed and tested a system which can hijack vehicles from any location [23][24][25]. The integration of AI into these technologies amplifies the potential for misuse, highlighting the need for stringent security protocols and regulatory frameworks.

Existing Global Policies and Strategies on AI Misuse

According to Hutter and Hutter [8], while there is a growing necessity for the development of global policies and strategies to address its misuse, the existing regulatory frameworks are often fragmented, inconsistent, and lack the comprehensive scope needed to effectively mitigate the risks associated with AI misuse. The challenge lies in the complexity of AI technologies, their rapid evolution, and their transnational nature, which complicates the formulation and enforcement of cohesive global policies

[26][27]. Internationally, several organizations and coalitions have taken steps to address AI misuse [28][29]. The European Union (EU) has been at the forefront of developing regulatory frameworks for AI, emphasizing ethical guidelines and robust data protection [26]. The General Data Protection Regulation (GDPR) is a landmark piece of legislation that, while not specific to AI, establishes stringent standards for data privacy and security, indirectly impacting AI applications [30]. Additionally, the EU has proposed the Artificial Intelligence Act, which seeks to classify AI systems based on their risk levels and implement corresponding regulatory measures. This act aims to ensure that AI systems are safe, transparent, and respect fundamental rights [31][32].

The United Nations (UN) has also recognized the need for global cooperation in addressing AI misuse, and have thus developed a Roadmap for Digital Cooperation, which outlines a vision for the responsible use of AI, emphasizing human rights, peace, and sustainable development [33]. The UN has further advocated for the development of international norms and standards to guide the ethical use of AI, stressing the importance of inclusivity and transparency in AI governance. However, the voluntary nature of many UN initiatives limits their enforceability, posing challenges to their effectiveness, considering that this voluntary approach to policy implementation lacks enforcement ability, and is also characterized by uneven implementation, where stakeholders only implement parts of the policies which are either favorable or convenient [34][39]. In contrast, China's centralized approach to AI regulation is both commendable and questionable [35]. The government’s issuance of multiple policy documents offers a clear vision and promotes rapid development, affirming the strategic importance placed on AI, while fueling significant investment and research. Additionally, comprehensive regulations tackle specific concerns like data security and algorithmic bias, aiming to prevent misuse and promote responsible innovation [36]. Angela Zhang [36] argues that the very features that drive China's AI advancement also raise concerns, as the top-down, mandatory nature of regulations can stifle creativity and hinder the emergence of disruptive ideas. Furthermore, the focus on control raises questions about privacy and freedom of expression. China's extensive surveillance apparatus, coupled with its control over AI development, creates a potential for misuse for social control [37]. Yet, the effectiveness of China's approach remains to be seen. While it fosters rapid progress, it's unclear if true innovation can flourish in such a controlled environment. The long-term impact on individual liberties and the global balance of power in the AI race are critical considerations. These policies prioritize the development of AI technologies while ensuring that they align with national security and social stability objectives [35][36][37]. China's approach underscores the balance between fostering innovation and mitigating risks, although it raises concerns about state surveillance and the potential misuse of AI by authoritarian regimes.

Hutter and Hutter [8] avers that regulations often struggle to keep pace with the rapid pace of AI development, leaving emerging threats unaddressed. Additionally, existing frameworks often focus primarily on data privacy, neglecting crucial aspects like algorithmic fairness, transparency, and the ethical implications of AI use throughout its lifecycle. In the views of Walter [38], the lack of harmonization in global policies governing the use of AI developments is a major hurdle. For instance, while the EU's GDPR safeguards personal data and privacy, it indirectly impacts AI development by limiting access to and use of personal information which is crucial to effective AI development [26]. Also, while the UN's approach promotes international cooperation and responsible AI development, emphasizing human rights, peace and sustainability, its lack of enforcement mechanism due to its reliance on voluntary initiative presents significant implementation challenges [33][69]. China's reforms on the other hand, while truly advantageous to AI advancement, holds the potential to limit rights and promote governmental sovereignty which can result in political and government induced abuses [35][36]. Hence, for truly responsible AI development, a more collaborative global effort is necessary. Building on the EU's focus on data privacy and ethics, alongside the UN's emphasis on international cooperation and strong regulatory frameworks, can help create a more unified approach.

Ethical and Legal Considerations in AI Development

Ferrara [40] contends that a significant ethical concern in AI development is the potential for bias in AI algorithms which can arise from various sources, including biased training data, biased algorithmic design, and biased application contexts. For instance, facial recognition systems have been shown to have higher error rates for people of color and women, leading to concerns about their fairness and reliability in critical applications such as law enforcement and hiring [41][42]. Ensuring fairness requires careful attention to the quality and diversity of training data, as well as ongoing monitoring and evaluation of AI systems to identify and mitigate biases. Such fairness and attention is essential, as AI-biased systems such as facial recognition could be misused by governments or other actors to discriminate against certain groups, especially while attempting to identify and track people of a particular ethnicity or religion [40][43].

Furthermore, the issue of accountability in AI development is complex, particularly when AI systems operate autonomously or semi-autonomously. Determining who is responsible for the actions and outcomes of an AI system—whether it is the developers, the deployers, or the users—poses significant ethical and legal challenges [44][45]. Clear guidelines and frameworks are necessary to assign responsibility and ensure that appropriate measures are in place to address any harm caused by AI systems [8][40][46].

Leveraging Artificial Intelligence and Technological Solutions for Combating AI Misuse

One intriguing approach is leveraging AI itself to combat AI-related threats [47][48]. Anderljung and Hazell [49] avers that Artificial Intelligence (AI) technologies has potentials to detect and prevent the misuse and abuse of AI developments, as these solutions can be trained and equipped with a range of methodologies and tools designed to safeguard against various forms of AI-related threats, including cyber-attacks, data breaches, and the creation of malicious content such as deepfakes. On the positive side, AI can be a powerful tool for detecting and preventing AI misuse. AI algorithms can analyze vast amounts of data to identify patterns indicative of malicious activity, such as cyberattacks or attempts to manipulate AI systems [50][51]. Additionally, AI-powered anomaly detection can monitor the behavior of other AI models, flagging unusual outputs or potential vulnerabilities [52][53].

Furthermore, blockchain technology also offers promising solutions for preventing AI misuse, particularly in the context of data integrity and authenticity [54][65]. Blockchain's decentralized and immutable ledger system can be used to securely store and verify the provenance of data, ensuring that it has not been tampered with or altered [55][56]. This capability is especially valuable in applications where data integrity is critical, such as in healthcare and financial services. By integrating blockchain with AI systems, organizations can create robust frameworks for data verification and auditability, thereby reducing the risk of data manipulation and fraud. Similarly, Tyagi [54] indicates that the integration of AI with encryption technologies enhances the security of data both in transit and at rest. AI algorithms can optimize encryption processes, making them more efficient and resistant to attacks. For example, AI can be used to dynamically adjust encryption keys and protocols based on the sensitivity of the data and the current threat environment, providing adaptive and context-aware data protection [57][58].

Furthermore, Explainable AI (XAI) techniques can be used to create more transparent AI security systems [59]. This transparency is crucial for identifying biases or vulnerabilities in the AI used for other purposes. AI-powered threat hunting can also analyze vast datasets related to AI development and use, uncovering potential misuse attempts through identifying suspicious patterns [52][60]. However, this approach is not without limitations. The evolving nature of AI threats demands constant adaptation of security AI. Additionally, training effective security AI requires large amounts of data on AI misuse, which can be scarce [61]. Biases in training data can also render security AI less effective in detecting certain types of misuse.

A vital case is Turnitin's AI-powered plagiarism detection system which exemplifies the potential and limitations of this approach [62]. While it can identify unusual writing

patterns suggestive of AI use, it's not foolproof. Sophisticated AI writing tools can potentially evade detection. Turnitin's system employs a multi-layered AI approach to identify student work potentially generated using AI tools, by analyzing submitted assignments for patterns atypical of human writing, such as unusual sentence structures, vocabulary choices that deviate from the expected field-specific language, or inconsistencies in writing style across the assignment [63][64]. The AI compares the submitted text to a vast repository of academic sources, websites, and even student work from previous semesters, allowing it to identify potential matches or paraphrases generated by AI tools that scrape content from the web.

While Turnitin's AI offers a valuable tool for educators, the approach has not shown an absolute remedy for AI misuse, as it only highlights suspicious patterns, but doesn't definitively prove AI use, hence, educators typically use Turnitin's warnings alongside their judgment and review of the assignment to make a final determination [62].Despite limitations, Turnitin showcases the potential of AI to combat AI misuse in education [62][65].

Evidently, using AI to combat AI misuse holds promise. However, it's crucial to acknowledge the challenges and limitations. Security AI needs continuous development to stay ahead of evolving threats, and robust data collection and unbiased training are essential. Sharma [66] suggests that while AI can be a valuable tool in the fight against AI misuse, it should be seen as part of a comprehensive strategy that includes international cooperation, ethical considerations, and robust regulatory frameworks [66][67].

Elements of Comprehensive Strategies for Mitigating AI Misuse

According to Hutter and Hutter [8], developing comprehensive strategies to mitigate the misuse of Artificial Intelligence (AI) requires a multifaceted approach that addresses technical, ethical, and legal dimensions, encompassing robust, adaptive, and inclusive strategies, which ensures that they can effectively respond to the evolving landscape of AI technologies and their associated risks [26][66]. In the views of Curtis et al. [68], a foundational element of these strategies is the enhancement of public and organizational awareness about the risks and ethical considerations associated with AI. Increasing awareness involves educational initiatives, public campaigns, and training programs that inform individuals and organizations about the potential misuse of AI and the measures that can be taken to prevent it. By fostering a deeper understanding of AI technologies and their implications, stakeholders can be better equipped to recognize and mitigate risks [48].

Furthermore, implementing and enforcing ethical guidelines for AI development is another critical strategy that should be integrated into the development process from the

outset, with mechanisms for continuous monitoring and assessment to ensure compliance [70]. Ferrara [40] emphasizes that legal frameworks must also be adapted and strengthened to address the complexities of AI technologies and their misuse. This includes establishing clear regulations for data protection, algorithmic transparency, and the accountability of AI systems. Laws such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States set important precedents for data privacy and security, but further efforts are needed to address the unique challenges posed by AI. New legal concepts may be required to define and distribute liability among the various stakeholders involved in the development and deployment of AI, ensuring that there are clear avenues for recourse and compensation for affected parties.

Additionally, Walter [38] asserts that, given the global nature of AI development and misuse, it is essential for countries to work together in establishing common standards and regulatory frameworks. More so, Rangaraju [71] implies that continuous monitoring and assessment of AI systems are essential for maintaining their security and integrity. This involves implementing AI audit systems that evaluate the performance and behavior of AI models, identifying any deviations or anomalies that could indicate misuse [72]. Regular audits and assessments help ensure that AI systems operate as intended and do not pose unintended risks.

3. Methods

This research employed a mixed-methods approach, integrating both quantitative and qualitative data collection and analysis techniques. The quantitative data was sourced from a survey questionnaire administered to 211 experts across four key domains: policymakers, law enforcement officials, AI researchers, and industry professionals. The questionnaire was meticulously designed to capture insights into the perceptions and experiences of these experts regarding the criminal use and abuse of AI, as well as the effectiveness of various mitigation strategies. To ensure a comprehensive understanding of the subject matter, the study also incorporated qualitative data from a diverse range of secondary sources. This included an in-depth review of 16 academic papers, 6 governmental publications, and 5 industrial reports, all of which were carefully selected based on their relevance to the research questions and their contribution to the existing body of knowledge.The quantitative data analysis was analysed using multiple regression analysis. To enhance the robustness of the findings, the quantitative results were triangulated with qualitative insights derived from the thematic analysis of the secondary sources. This triangulation process involved comparing and contrasting the

statistical findings with the qualitative evidence, identifying areas of convergence and divergence, and exploring potential explanations for any discrepancies.

4. Result and Discussion

Table 1. H_1: Increasing public and organizational awareness about the risks associated with AI reduces its criminal use and abuse

Source	Relevant Data
NIST (2021)	Highlights the importance of public awareness and organizational frameworks to manage AI risks effectively.
NIST (2023)	Emphasizes the role of frameworks and guidelines in raising awareness about AI risks.
UN (2023)	Discusses the necessity of regulation and public awareness in curbing AI misuse.
Hoffman, D.P. and S. (2022)	Analyzes geopolitical implications of AI and the role of awareness in preventing misuse.

The frameworks provided by NIST (2021) and NIST (2023) highlight the importance of public awareness and organizational strategies in managing AI risks effectively. These documents suggest that heightened awareness can lead to improved risk management practices and a reduction in AI misuse. Additionally, the UN (2023) report underscores the necessity of regulation and public awareness in curbing AI misuse, indicating that an informed public and organizations are better equipped to recognize and mitigate risks associated with AI. Hoffman, D.P. and S. (2022) further elaborate on the geopolitical implications, suggesting that international awareness and cooperation are crucial in preventing AI misuse.

Table 2. H_2: The development and deployment of advanced AI detection and prevention technologies significantly mitigate AI-related criminal activities

Source	Relevant Data
Ahmed, A.A. and Echi, M.	Discusses the deployment of AI-powered threat

(2021)	detection for surveillance.
Azhar, I. (2016)	Reviews AI's role in enhancing cybersecurity.
Feldstein, S. (2019)	Details the global expansion and implications of AI surveillance.
Horan, C. and Saiedian, H. (2021)	Explores AI's role in cybercrime investigation and prevention.

Ahmed, A.A. and Echi, M. (2021) discuss the effectiveness of AI-powered threat detection systems, such as intelligent surveillance cameras, in identifying and mitigating threats. Azhar, I. (2016) systematically reviews AI's role in enhancing cybersecurity, showing that advanced detection technologies can prevent cyber-attacks. Additionally, Feldstein, S. (2019) and Horan, C. and Saiedian, H. (2021) both details how AI surveillance and cybercrime investigation technologies contribute to reducing criminal activities through enhanced detection and prevention capabilities.

Table 3. H_3: Implementing and enforcing ethical guidelines for AI development reduces the potential for criminal use and abuse of AI technologies

Source	**Relevant Data**
Balasubramaniam, N. et al. (2020)	Provides ethical guidelines for AI systems development.
Jobin, A., Ienca, M. and Vayena, E. (2019)	Maps the global landscape of AI ethics guidelines.
NIST (2021)	Presents frameworks and guidelines for trustworthy and responsible AI.
Team, N.A. (2021)	Outlines resources and frameworks for responsible AI development.
Hagendorff, T. (2020)	Evaluates the effectiveness of AI ethics guidelines in practice.
Shneiderman, B. (2020)	Discusses bridging the gap between ethics and practical AI implementation.

Balasubramaniam, N. et al. (2020) and Jobin, A., Ienca, M. and Vayena, E. (2019) emphasize the importance of ethical guidelines in AI development, providing comprehensive overviews of existing guidelines and their global impact. The NIST (2021) framework and resources from Team, N.A. (2021) further support the role of ethical guidelines in fostering responsible AI development. Hagendorff, T. (2020) evaluates the effectiveness of these guidelines, while Shneiderman, B. (2020) discusses the practical application of ethics in AI development.

Table 4. H_4: The imposition of severe penalties and consistent enforcement for AI-related crimes acts as a strong deterrent against the criminal use of AI

Source	Relevant Data
NIST (2023)	Suggests regulatory frameworks and enforcement measures to manage AI risks.
Horan, C. and Saiedian, H. (2021)	Examines the landscape of cybercrime investigation and the impact of penalties.
Khapra, P. (2022)	Explores intervention strategies and penalties against AI threats.
Fitzpatrick, D.J., Gorr, W.L. and Neill, D.B. (2019)	Highlights the use of predictive analytics in policing and the role of penalties.

The NIST (2023) framework suggests that regulatory measures and consistent enforcement are necessary to manage AI risks effectively. Horan, C. and Saiedian, H. (2021) examine the impact of penalties on cybercrime, showing that severe penalties can deter criminal activities. Khapra, P. (2022) explores intervention strategies against AI threats, indicating that penalties and enforcement can play a significant role in mitigating these threats. Fitzpatrick, D.J., Gorr, W.L. and Neill, D.B. (2019) highlight the role of predictive analytics in policing, suggesting that enforcement measures, supported by data, can be effective in deterring AI-related crimes.

Table 5. Regression analysis H_1: Increasing Public and Organizational Awareness

Predictor	Coefficient (B)	Beta Value (β)	p-Value	R Value
Constant	20.0	-	-	-

Effectiveness of public awareness campaigns	0.40	0.35	<.01	0.50
Organizational awareness training	0.35	0.32	<.05	0.45
Frequency of AI security awareness programs	0.30	0.28	<.05	0.43
Barriers to increasing public awareness	-0.25	-0.22	<.05	0.40

Dependent Variable: Overall effectiveness of awareness measures.

The effectiveness of public awareness campaigns (B = 0.40, β = 0.35, p < .01) and organizational awareness training (B = 0.35, β = 0.32, p < .05) positively impact the overall effectiveness of awareness measures, while barriers to increasing public awareness (B = -0.25, β = -0.22, p < .05) negatively impact them. These results support the acceptance of Hypothesis 1.

Table 6. Regression analysis H_2: Development and Deployment of Advanced AI Detection and Prevention Technologies

Predictor	**Coefficient (B)**	**Beta Value (β)**	**p-Value**	**R-Value**
Constant	18.5	-	-	-
Effectiveness of AI detection technologies	0.45	0.40	<.01	0.55
Frequency of technological advancements	0.32	0.28	<.05	0.48
Necessity of continuous updates	0.38	0.34	<.01	0.52
Challenges in deploying AI detection technologies	-0.22	-0.20	<.05	0.42

Dependent Variable: **Overall effectiveness of AI detection technologies.**

The effectiveness of AI detection technologies (B = 0.45, β = 0.40, p < .01), frequency of technological advancements (B = 0.32, β = 0.28, p < .05), and necessity of

continuous updates (B = 0.38, β = 0.34, p < .01) positively impact the overall effectiveness of AI detection technologies, while challenges in deploying these technologies (B = -0.22, β = -0.20, p < .05) negatively impact them. These findings support the acceptance of Hypothesis 2.

Table 7. Regression analysis H_3: Implementing and Enforcing Ethical Guidelines

Predictor	Coefficient (B)	Beta Value (β)	p-Value	R-Value
Constant	22.0	-	-	-
Effectiveness of current ethical guidelines	0.50	0.42	<.01	0.60
Presence of ethical guidelines	0.28	0.25	<.05	0.44
Frequency of reviewing and updating guidelines	0.34	0.30	<.05	0.47
Agreement on guidelines reducing AI misuse	-0.20	-0.18	<.05	0.41

Dependent Variable: **Overall effectiveness of ethical guidelines.**

The effectiveness of current ethical guidelines (B = 0.50, β = 0.42, p < .01), presence of ethical guidelines (B = 0.28, β = 0.25, p < .05), and frequency of reviewing and updating guidelines (B = 0.34, β = 0.30, p < .05) positively impact the overall effectiveness of ethical guidelines, while agreement on guidelines reducing AI misuse (B = -0.20, β = -0.18, p < .05) negatively impacts them. These results support the acceptance of Hypothesis 3

Table 8. Regression analysis H_4: Severe Penalties and Consistent Enforcement

Predictor	Coefficient (B)	Beta Value (β)	p-Value	R Value
Constant	19.5	-	-	-

Effectiveness of current penalties	0.42	0.37	<.01	0.53
Consistency of enforcement	0.35	0.30	<.05	0.45
Increasing penalties as a deterrent	0.40	0.36	<.01	0.50
Additional measures to improve enforcement	-0.24	-0.21	<.05	0.43

Dependent Variable: **Overall effectiveness of penalties and enforcement.**

The effectiveness of current penalties (B = 0.42, β = 0.37, p < .01), consistency of enforcement (B = 0.35, β = 0.30, p < .05), and increasing penalties as a deterrent (B = 0.40, β = 0.36, p < .01) positively impact the overall effectiveness of penalties and enforcement, while additional measures to improve enforcement (B = -0.24, β = -0.21, p < .05) negatively impact them. These findings support the acceptance of Hypothesis 4.

Triangulation Reports for the study

Table9: Triangulated Findings for Each Hypothesis

Hypothesis	**Quantitative Findings**	**Qualitative Findings**	**Triangulated Insights**

H1: Increasing Public and Organizational Awareness	- Effectiveness of public awareness campaigns (β = 0.35, p < .01) significantly impacts awareness measures. - Organizational awareness training (β = 0.32, p < .05) and frequency of AI security awareness programs (β = 0.28, p < .05) positively influence awareness effectiveness. - - Barriers to increasing public awareness (β = -0.22, p < .05) negatively impact awareness measures.	**NIST (2021, 2023)** Highlights the importance of public awareness and organizational frameworks in managing AI risks effectively. **UN (2023):** Emphasizes the necessity of regulation and public awareness in curbing AI misuse. **Hoffman D.P. and S. (2022):** Discusses geopolitical implications and the role of awareness in preventing misuse.	- Both data types suggest that increasing awareness is crucial for reducing AI misuse. - Quantitative analysis confirms the positive impact of awareness campaigns, training, and frequency of programs. - Qualitative insights provide context and examples of effective implementation. - Barriers such as resource constraints and insufficient knowledge need addressing.

H2: Development and Deployment of Advanced AI Detection and Prevention Technologies	- Effectiveness of AI detection technologies (β = 0.40, p < .01) significantly influences detection measures. - Frequency of technological advancements (β = 0.28, p < .05) and necessity of continuous updates (β = 0.34, p < .01) positively impact detection effectiveness. - Challenges in deploying AI detection technologies (β = -0.20, p < .05) negatively impact effectiveness.	**Ahmed A.A. and Echi M. (2021):** Discusses the effectiveness of AI-powered threat detection systems **Azhar I. (2016):** Reviews AI's role in enhancing cybersecurity. - **Feldstein S. (2019) & Horan C. and Saiedian H. (2021):** Detail how AI surveillance and cybercrime investigation technologies contribute to reducing criminal activities.	- Quantitative data validates the importance of effective AI detection technologies and continuous updates. - Qualitative findings elaborate on practical challenges and the necessity for ongoing advancements. - Integration underscores the critical role of innovation and highlights specific barriers that need addressing.

H3: Implementing and Enforcing Ethical Guidelines	- Effectiveness of current ethical guidelines (β = 0.42, p < .01) significantly impacts ethical measures. - Presence of ethical guidelines (β = 0.25, p < .05) and frequency of reviewing and updating guidelines (β = 0.30, p < .05) positively influence guideline effectiveness. - Agreement on guidelines reducing AI misuse (β = -0.18, p < .05) negatively impacts effectiveness.	- **Balasubramaniam N. et al. (2020):** Provides ethical guidelines for AI systems development. - **Jobin A., Ienca M., and Vayena E. (2019):** Maps the global landscape of AI ethics guidelines. - **NIST (2021) & Team N.A. (2021):** Present frameworks and guidelines for trustworthy AI. - **Hagendorff T. (2020) &Shneiderman B. (2020):** Evaluate and discuss the practical application of ethics in AI development.	- Quantitative analysis confirms ethical guidelines are effective when present and regularly updated. - Qualitative data provides insights into challenges of consistent implementation and enforcement. - Negative impact of agreement on guidelines suggests differing perceptions, explained by qualitative examples of inconsistent practices.

H4: Severe Penalties and Consistent Enforcement	- Effectiveness of current penalties (β = 0.37, p < .01) significantly impacts enforcement measures. - Consistency of enforcement (β = 0.30, p < .05) and increasing penalties as a deterrent (β = 0.36, p < .01) positively influence enforcement effectiveness. - Additional measures to improve enforcement (β = -0.21, p < .05) negatively impact effectiveness.	- **NIST (2023):** Suggests regulatory frameworks and enforcement measures to manage AI risks effectively. - **Horan C. and Saiedian H. (2021):** Examine the impact of penalties on cybercrime. - **Khapra P. (2022):** Explores intervention strategies against AI threats. - **Fitzpatrick D.J., Gorr W.L., and Neill D.B. (2019):** Highlight the use of predictive analytics in policing and the role of penalties.	- Quantitative data confirms positive impact of severe penalties and consistent enforcement on reducing AI misuse. - Qualitative insights highlight need for additional measures and integrated approaches. - Integration provides a comprehensive view of the importance of a robust legal framework combined with practical enforcement strategies.

The triangulation reports in table 5 for the study provide a comprehensive understanding of the four hypotheses through a combination of quantitative and qualitative findings.

For Hypothesis 1, quantitative results show that public awareness campaigns (β = 0.35, p < .01) and organizational training (β = 0.32, p < .05) positively impact awareness measures, though barriers exist (β = -0.22, p < .05). Qualitative data from NIST (2021, 2023), UN (2023), and Hoffman (2022) support the importance of awareness and frameworks in managing AI risks. Triangulated insights confirm the critical role of awareness campaigns and training, while addressing resource and knowledge barriers.

For Hypothesis 2, quantitative findings indicate that AI detection technologies (β = 0.40, p < .01) and continuous updates (β = 0.34, p < .01) significantly improve detection effectiveness, despite deployment challenges (β = -0.20, p < .05). Qualitative evidence from Ahmed (2021), Azhar (2016), and Feldstein and Horan (2019, 2021) highlights the effectiveness of AI-powered threat detection and cybersecurity technologies. The

integration emphasizes the need for ongoing advancements and addressing practical barriers.

For Hypothesis 3, quantitative analysis shows that current ethical guidelines ($\beta = 0.42$, $p < .01$) and their regular updates ($\beta = 0.30$, $p < .05$) positively affect guideline effectiveness, though there are differing perceptions ($\beta = -0.18$, $p < .05$). Qualitative data from Balasubramaniam (2020), Jobin et al. (2019), NIST (2021), and others underline the importance and challenges of implementing AI ethics. The combined insights validate the effectiveness of ethical guidelines and highlight the need for consistent enforcement.

For Hypothesis 4, quantitative results indicate that current penalties ($\beta = 0.37$, $p < .01$) and consistent enforcement ($\beta = 0.30$, $p < .05$) are effective deterrents, while additional measures are needed ($\beta = -0.21$, $p < .05$). Qualitative findings from NIST (2023), Horan and Saiedian (2021), Khapra (2022), and Fitzpatrick et al. (2019) support the importance of regulatory frameworks and enforcement strategies. The triangulated insights underscore the necessity of a robust legal framework and integrated enforcement approaches to mitigate AI misuse.

Discussion

The results of this study align with the findings of Hutter and Hutter [8], NIST [81] and UN [75], which emphasize the importance of public awareness and organizational frameworks in managing AI risks effectively. The quantitative analysis confirms that public awareness campaigns and organizational training significantly impact awareness measures, thus supporting the hypothesis that heightened awareness can lead to reduced AI misuse. The findings also support the assertion that advanced AI detection and prevention technologies play a crucial role in mitigating AI-related criminal activities. The quantitative analysis demonstrates that the effectiveness of AI detection technologies and the frequency of technological advancements positively impact detection measures. This aligns with the work of Ahmed and Echi [59], Azhar [6], Feldstein [78], and Horan and Saiedian [22], who discuss the effectiveness of AI-powered threat detection systems and their role in enhancing cybersecurity. These studies highlight the ability of AI algorithms to analyze vast amounts of data, identify patterns indicative of malicious activity, such as the cyberattacks highlighted by Anderljung and Hazell [49], and adapt to evolving threats.

In addition, the study found that implementing and enforcing ethical guidelines can effectively reduce the potential for AI misuse. The quantitative analysis reveals that the presence of ethical guidelines and their regular updates positively influence guideline

effectiveness. Balasubramaniam et al. (2020) and Jobin et al. [61] emphasize the importance of ethical guidelines in AI development. These guidelines provide a framework for responsible AI development, addressing issues such as the bias highlighted by Ferrara [40], transparency, and accountability.

Finally, the study affirms that severe penalties and consistent enforcement can deter the criminal use of AI. The quantitative analysis indicates that the effectiveness of current penalties and the consistency of enforcement positively influence enforcement measures. This aligns with the literature, as NIST [81], Horan and Saiedian [22], Khapra [20], and Fitzpatrick et al. [14] further highlight the importance of regulatory frameworks, enforcement strategies, and the role of penalties in deterring AI-related crimes. These studies emphasize that clear and stringent legal frameworks, coupled with effective enforcement mechanisms, create a disincentive for individuals and organizations to engage in AI-related criminal activities.

Conclusion and Recommendation

This study underscores the multifaceted nature of mitigating AI misuse, emphasizing the need for a comprehensive approach that encompasses awareness, technological advancements, ethical guidelines, and robust enforcement. The results highlight that while progress has been made in each of these areas, significant challenges remain.To effectively combat the criminal use of AI, this study recommends:

Industry leaders should develop targeted awareness campaigns focused on educating the public and organizations about the specific risks associated with AI misuse, tailoring the information to different audiences and utilizing diverse communication channels to maximize reach and impact.

Industry leaders and researchers collaborate and invest in R&D efforts to develop AI detection and prevention technologies which incorporates and promotes explainable AI principles to enhance transparency and trust.

Policymakers, governments, and international bodies should collaborate to establish comprehensive and enforceable ethical guidelines and enact clear regulations for data protection, algorithmic transparency, and accountability, as well as fostering collaboration among nations to harmonize policies and address transnational threats.

References

[1] S. Maleki Varnosfaderani and M. Forouzanfar, “The Role of AI in Hospitals and Clinics: Transforming Healthcare in the 21st Century,” *Bioengineering*, vol. 11, no. 4, p. 337, Apr. 2024, doi: https://doi.org/10.3390/bioengineering11040337

[2] M. Sadaf *et al.*, “Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects,” *Technologies*, vol. 11, no. 5, p. 117, Oct. 2023, Available: https://www.mdpi.com/2227-7080/11/5/117

[3] A. Fekete and J. Rhyner, “Sustainable Digital Transformation of Disaster Risk—Integrating New Types of Digital Social Vulnerability and Interdependencies with Critical Infrastructure,” *Sustainability*, vol. 12, no. 22, p. 9324, Nov. 2020, doi: https://doi.org/10.3390/su12229324

[4] N.-M. Aliman, L. Kester, and R. Yampolskiy, “Transdisciplinary AI Observatory—Retrospective Analyses and Future-Oriented Contradistinctions,” *Philosophies*, vol. 6, no. 1, p. 6, Jan. 2021, doi: https://doi.org/10.3390/philosophies6010006

[5] U. J. Butt, W. Richardson, M. Abbod, H.-M. Agbo, and C. Eghan, “The Deployment of Autonomous Drones During the COVID-19 Pandemic,” *Cybersecurity, Privacy and Freedom Protection in the Connected World*, pp. 183–220, 2021, doi: https://doi.org/10.1007/978-3-030-68534-8_13

[6] I. Azhar, “How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks: A systematic review,” *Social Science Research Network*, Jun. 02, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3905773

[7] S. Strauß, “From Big Data to Deep Learning: A Leap Towards Strong AI or ‘Intelligentia Obscura’?,” *Big Data and Cognitive Computing*, vol. 2, no. 3, p. 16, Jul. 2018, doi: https://doi.org/10.3390/bdcc2030016

[8] R. Hutter and M. Hutter, “Chances and Risks of Artificial Intelligence—A Concept of Developing and Exploiting Machine Intelligence for Future Societies,” *Applied System Innovation*, vol. 4, no. 2, p. 37, Jun. 2021, doi: https://doi.org/10.3390/asi4020037

[9] N. Balasubramaniam, M. Kauppinen, S. Kujala, and K. Hiekkanen, “Ethical Guidelines for Solving Ethical Issues and Developing AI Systems,” *Product-Focused Software Process Improvement*, pp. 331–346, 2020, doi: https://doi.org/10.1007/978-3-030-64148-1_21

[10] W. Villegas-Ch and J. García-Ortiz, “Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence,” *Electronics*, vol. 12, no. 18, p. 3786, Jan. 2023, doi: https://doi.org/10.3390/electronics12183786

[11] N. Kaloudi and J. Li, “The AI-Based Cyber Threat Landscape,” *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–34, Feb. 2020, doi: https://doi.org/10.1145/3372823

[12] P. Faruki*et al.*, “Android Security: A Survey of Issues, Malware Penetration, and Defenses,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 998–1022, 2015, doi: https://doi.org/10.1109/COMST.2014.2386139

[13] C. S. Adigwe, N. R. Mayeke, S. O. Olabanji, O. J. Okunleye, P. C. Joeaneke, and O. O. Olaniyi, “The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks,” *Asian journal of economics, business and accounting*, vol. 24, no. 3, pp. 289–306, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i31287

[14] D. J. Fitzpatrick, W. L. Gorr, and D. B. Neill, “Keeping Score: Predictive Analytics in Policing,” *Annual Review of Criminology*, vol. 2, no. 1, pp. 473–491, Jan. 2019, doi: https://doi.org/10.1146/annurev-criminol-011518-024534

[15] K. Inkpen, S. Chancellor, M. De Choudhury, M. Veale, and E. P. S. Baumer, “Where is the Human?,” *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, May 2019, doi: https://doi.org/10.1145/3290607.3299002

[16] Trend Micro, “Equifax Reveals Extent of 2017 Data Breach, Details Number of Stolen Records - Security News - Trend Micro USA,” *www.trendmicro.com*, May 09, 2018. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/equifax-reveals-extent-of-2017-data-breach-number-of-stolen-records

[17] O. O. Olaniyi, “Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447

[18] F. A. Ezeugwa, O. O. Olaniyi, J. C. Ugonnia, A. S. Arigbabu, and P. C. Joeaneke, “Artificial Intelligence, Big Data, and Cloud Infrastructures: Policy Recommendations for Enhancing Women’s Participation in the Tech-Driven Economy,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 1–16, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61158

[19] H. Ueno, “Artificial Intelligence as Dual-Use Technology,” pp. 7–32, Jan. 2023, doi: https://doi.org/10.1007/978-3-031-22371-6_2

[20] P. Khapra, “Evolution of Cybercrime and Deepfakes - Exploring Intervention Strategies of International Organizations against AI Threats - ProQuest,” *www.proquest.com*, 2022. https://www.proquest.com/openview/f50c69507802aace197ec39a079b92b8/1?pq-origsite=gscholar&cbl=2035897 (accessed Jan. 05, 2024)

[21] U. T. I. Igwenagu, A. A. Salami, A. S. Arigbabu, C. E. Mesode, T. O. Oladoyinbo, and O. O. Olaniyi, “Securing the Digital Frontier: Strategies for Cloud Computing Security, Database Protection, and Comprehensive Penetration Testing,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 60–75, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61162

[22] C. Horan and H. Saiedian, “Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions,” *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 580–596, Sep. 2021, doi: https://doi.org/10.3390/jcp1040029

[23] A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway—With Me in It,” *WIRED*, Jul. 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[24] A. Giannaros*et al.*, “Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 493–543, Sep. 2023, doi: https://doi.org/10.3390/jcp3030025

[25] O. O. Olaniyi, F. A. Ezeugwa, C. G. Okatta, A. S. Arigbabu, and P. C. Joeaneke, “Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies,” *Archives of current research international*, vol. 24, no. 5, pp. 124–139, Apr. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5690

[26] S. Musch, M. Borrelli, and C. Kerrigan, “The EU AI Act: A Comprehensive Regulatory Framework for Ethical AI Development,” *Social Science Research Network*, Aug. 23, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4549248

[27] O. O. Olaniyi, O. O. Omogoroye, F. G. Olaniyi, A. I. Alao, and T. O. Oladoyinbo, “CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, p. 32, 2024, doi: https://doi.org/10.9734/JERR/2024/v26i61160

[28] M. M. Maas and J. J. Villalobos , “International AI Institutions: A Literature Review of Models, Examples, and Proposals,” *Social Science Research Network*, Sep. 22, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579773

[29] B. Shneiderman, “Bridging the Gap Between Ethics and Practice,” *ACM Transactions on Interactive Intelligent Systems*, vol. 10, no. 4, pp. 1–31, Nov. 2020, Available: https://dl.acm.org/doi/abs/10.1145/3419764

[30] M. Pathak, “Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act.,” *Social Science Research Network*, vol. 10, no. 1, Jan. 2024, doi: https://doi.org/10.2139/ssrn.4718891

[31] M. Wörsdörfer, “The E.U.’s artificial intelligence act: an ordoliberal assessment,” *AI and ethics*, Aug. 2023, doi: https://doi.org/10.1007/s43681-023-00337-x

[32] O. O. Olaoye, F. U. Quadri, and O. O. Olaniyi, “Examining the Role of Trade on the Relationship between Environmental Quality and Energy Consumption: Insights from Sub Saharan Africa,” *Journal of economics, management and trade*, vol. 30, no. 6, pp. 16–35, Apr. 2024, doi: https://doi.org/10.9734/jemt/2024/v30i61211

[33] M. Francisco and Björn-Ola Linnér, “AI and the governance of sustainable development. An idea analysis of the European Union, the United Nations, and the World Economic Forum,” *Environmental Science & Policy*, vol. 150, pp. 103590–103590, Dec. 2023, doi: https://doi.org/10.1016/j.envsci.2023.103590

[34] S. Islam, Z. Lee, Adha Shaleh, and Han Sen Soo, “The United Nations Environment Assembly resolution to end plastic pollution: Challenges to effective policy interventions,” *Environment, Development and Sustainability*, vol. 26, Aug. 2023, doi: https://doi.org/10.1007/s10668-023-03639-6

[35] E. Hine and L. Floridi, “Artificial intelligence with American values and Chinese characteristics: a comparative analysis of American and Chinese governmental AI policies,” *AI & SOCIETY*, vol. 39, Jun. 2022, doi: https://doi.org/10.1007/s00146-022-01499-8

[36] Angela Huyue Zhang, “The Promise and Perils of China’s Regulation of Artificial Intelligence,” *Social Science Research Network*, vol. 2, Jan. 2024, doi: https://doi.org/10.2139/ssrn.4708676

[37] X. Chen and T. Oakes, “Time-Space Companions: Digital Surveillance, Social Management, and Abuse of Power During the Covid-19 Pandemic in China,” *Critical Asian Studies*, vol. 55, no. 2, pp. 1–24, Mar. 2023, doi: https://doi.org/10.1080/14672715.2023.2191248

[38] Y. Walter, “Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences,” *Discover Artificial Intelligence*, vol. 4, no. 1, Feb. 2024, doi: https://doi.org/10.1007/s44163-024-00109-4

[39] A. A. Salami, U. T. I. Igwenagu, C. E. Mesode, O. O. Olaniyi, and O. B. Oladoyinbo, “Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 304–323, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51156

[40] M. Milano, B. O’Sullivan, and M. Gavanelli, “Sustainable Policy Making: A Strategic Challenge for Artificial Intelligence,” *AI Magazine*, vol. 35, no. 3, p. 22, Sep. 2014, doi: https://doi.org/10.1609/aimag.v35i3.2534

[41] A. Valdivia, J. C. Serrajòrdia, and A. Swianiewicz, “There is an elephant in the room: towards a critique on the use of fairness in biometrics,” *AI and Ethics*, vol. 3, Dec. 2022, doi: https://doi.org/10.1007/s43681-022-00249-2

[42] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, “Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601

[43] A. D. Samuel-Okon and O. O. Abejide, “Bridging the Digital Divide: Exploring the Role of Artificial Intelligence and Automation in Enhancing Connectivity in Developing Nations,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 165–177, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61170

[44] T. Hagendorff, “The Ethics of AI Ethics: An Evaluation of Guidelines,” *Minds and Machines*, vol. 30, no. 1, pp. 99–120, Feb. 2020, doi: https://doi.org/10.1007/s11023-020-09517-8

[45] C. S. Adigwe, O. O. Olaniyi, S. O. Olabanji, O. J. Okunleye, N. R. Mayeke, and S. A. Ajayi, “Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 126–146, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41269

[46] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, “Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale,”

Asian Journal of Research in Computer Science, vol. 17, no. 5, pp. 85–107, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441

[47] S. Schmid, T. Riebe, and C. Reuter, "Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D," *Science and Engineering Ethics*, vol. 28, no. 2, Mar. 2022, doi: https://doi.org/10.1007/s11948-022-00364-7

[48] B. T. Familoni, "CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS," *Computer Science & IT Research Journal*, vol. 5, no. 3, pp. 703–724, Mar. 2024, doi: https://doi.org/10.51594/csitrj.v5i3.930

[49] M. Anderljung and J. Hazell, "Protecting Society from AI Misuse: When are Restrictions on Capabilities Warranted?," *Arxiv*, Mar. 2023, doi: https://doi.org/10.48550/arxiv.2303.09377

[50] Salman Muneer, U. Farooq, A. Athar, Muhammad Ahsan Raza, T. M. Ghazal, and Shadman Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis," *Journal of engineering*, vol. 2024, pp. 1–16, Apr. 2024, doi: https://doi.org/10.1155/2024/3909173

[51] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, "Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596

[52] C. Fontes, E. Hohma, C. C. Corrigan, and C. Lütge, "AI-powered public surveillance systems: why we (might) need them and how we want them," *Technology in Society*, vol. 71, no. 0160-791X, p. 102137, Nov. 2022, doi: https://doi.org/10.1016/j.techsoc.2022.102137

[53] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, "Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. ," vol. 17, no. 5, pp. 108–124, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5442

[54] A. K. Tyagi, "Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications," *www.igi-global.com*, 2024. https://www.igi-global.com/chapter/blockchain-and-artificial-intelligence-for-cyber-security-in-the-era-of-internet-of-things-and-industrial-internet-of-things-applications/336079

[55] M. Naz *et al.*, “A Secure Data Sharing Platform Using Blockchain and Interplanetary File System,” *Sustainability*, vol. 11, no. 24, p. 7054, Dec. 2019, doi: https://doi.org/10.3390/su11247054

[56] S. O. Olabanji, “AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423

[57] S. Trilles, Sahibzada Saadoon Hammad, and Ditsuhi Iskandaryan, “Anomaly detection based on Artificial Intelligence of Things: A Systematic Literature Mapping,” *Internet of Things*, vol. 25, pp. 101063–101063, Jan. 2024, doi: https://doi.org/10.1016/j.iot.2024.101063

[58] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, A. S. Abidemi, T. O. Oladoyinbo, and O. O. Olaniyi, “AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424

[59] A. A. Ahmed and M. Echi, “Hawk-Eye: An AI-Powered Threat Detector for Intelligent Surveillance Cameras,” *IEEE Access*, vol. 9, pp. 63283–63293, 2021, doi: https://doi.org/10.1109/ACCESS.2021.3074319

[60] O. O. Olaniyi, O. J. Okunleye, S. O. Olabanji, C. U. Asonze, and S. A. Ajayi, “IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience,” *Asian Journal of Research in Computer Science*, vol. 16, no. 4, pp. 354–371, Dec. 2023, doi: https://doi.org/10.9734/ajrcos/2023/v16i4397

[61] A. Jobin, M. Ienca, and E. Vayena, “The global landscape of AI ethics guidelines,” *Nature Machine Intelligence*, vol. 1, no. 9, pp. 389–399, Sep. 2019, Available: https://www.nature.com/articles/s42256-019-0088-2

[62] J. Hutson, “Rethinking Plagiarism in the Era of Generative AI,” *Journal of intelligent communication*, vol. 4, no. 1, Apr. 2024, doi: https://doi.org/10.54963/jic.v4i1.220

[63] S. Nikolic *et al.*, “ChatGPT versus engineering education assessment: a multidisciplinary and multi-institutional benchmarking and analysis of this generative artificial intelligence tool to investigate assessment integrity,” *European Journal of Engineering Education*, vol. 48, no. 4, pp. 1–56, May 2023, doi: https://doi.org/10.1080/03043797.2023.2213169

[64] O. O. Olaniyi, O. J. Okunleye, and S. O. Olabanji, “Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature,” *Current Journal of Applied Science and Technology*, vol. 42, no. 25, pp. 10–18, Aug. 2023, doi: https://doi.org/10.9734/cjast/2023/v42i254181

[65] O. O. Olaniyi, S. O. Olabanji, and O. J. Okunleye, “Exploring the Landscape of Decentralized Autonomous Organizations: A Comprehensive Review of Blockchain Initiatives,” *Journal of Scientific Research and Reports*, vol. 29, no. 9, pp. 73–81, Sep. 2023, doi: https://doi.org/10.9734/jsrr/2023/v29i91786

[66] S. Sharma, “Trustworthy Artificial Intelligence: Design of AI Governance Framework,” *Strategic Analysis*, vol. 47, no. 5, pp. 1–22, Dec. 2023, doi: https://doi.org/10.1080/09700161.2023.2288994

[67] O. O. Olaniyi and D. S. Omubo, “The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management,” *International journal of innovative research and development*, Jun. 2023, doi: https://doi.org/10.24940/ijird/2023/v12/i5/may23001

[68] C. Curtis, N. Gillespie, and S. Lockey, “AI-deploying organizations are key to addressing ‘perfect storm’ of AI risks,” *AI and Ethics*, vol. 3, May 2022, doi: https://doi.org/10.1007/s43681-022-00163-7

[69] O. O. Olaniyi, C. U. Asonze, S. A. Ajayi, S. O. Olabanji, and C. S. Adigwe, “A Regressional Study on the Impact of Organizational Security Culture and Transformational Leadership on Social Engineering Awareness among Bank Employees: The Interplay of Security Education and Behavioral Change,” *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 23, pp. 128–143, Dec. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i231176

[70] J. C. Ugonnia, O. O. Olaniyi, F. G. Olaniyi, A. A. Arigbabu, and T. O. Oladoyinbo, “Towards Sustainable IT Infrastructure: Integrating Green Computing with Data Warehouse and Big Data Technologies to Enhance Efficiency and Environmental Responsibility,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 247–261, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51151

[71] S. Rangaraju, “SECURE BY INTELLIGENCE: ENHANCING PRODUCTS WITH AI-DRIVEN SECURITY MEASURES,” *EPH - International Journal of Science And Engineering*, vol. 9, no. 3, pp. 36–41, Dec. 2023, doi: https://doi.org/10.53555/ephijse.v9i3.212

[72] M. Brown and A. Brown, “Legacy Set Free: Emancipating the Works of Oscar Brown, Jr.,” *Portable Gray*, vol. 2, no. 1, pp. 5–21, Mar. 2019, doi: https://doi.org/10.1086/704022

[73] OVIC, “Artificial Intelligence and Privacy - Issues and Challenges,” *Office of the Victorian Information Commissioner*, Aug. 2018. https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/

[74] C. F. Kerry, “Protecting privacy in an AI-driven world,” *Brookings*, Feb. 10, 2020. https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/

[75] United Nations, “Regulation essential to curb AI for surveillance, disinformation: rights experts | UN News,” *news.un.org*, Jun. 02, 2023. https://news.un.org/en/story/2023/06/1137302#:~:text=Regulation%20essential%20to%20curb%20AI%20for%20surveillance%2C%20disinformation%3A%20rights%20experts (accessed May 27, 2024)

[76] D. P. and S. Hoffman, “Geopolitical implications of AI and digital surveillance adoption,” *Brookings*, Jun. 21, 2022. https://www.brookings.edu/research/geopolitical-implications-of-ai-and-digital-surveillance-adoption/

[77] cbranley, “The West, China, and AI surveillance,” *Atlantic Council*, Dec. 18, 2020. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-west-china-and-ai-surveillance/ (accessed May 27, 2024)

[78] S. Feldstein, “The Global Expansion of AI Surveillance,” *Carnegie Endowment for International Peace*, Sep. 17, 2019. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

[79] NIST, “AI Risk Management Framework,” *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, Jan. 2023, doi: https://doi.org/10.6028/nist.ai.100-1

[80] N. A. Team, “NIST Trustworthy & Responsible AI Resource Center,” *airc.nist.gov*, 2023. https://airc.nist.gov/playbook (accessed May 27, 2024)

[81] NIST, “AI Risk Management Framework Concept Paper This Artificial Intelligence Risk Management Framework (AI RMF) concept paper incorporates input from the Notice of Request for Information (RFI) released by the National Institute of,” 2021. Available: https://www.nist.gov/system/files/documents/2021/12/14/AI%20RMF%20Concept%20Paper_13Dec2021_posted.pdf

[82] N. A. Team, “NIST Trustworthy & Responsible AI Resource Center,” *airc.nist.gov*, Dec. 31, 2021. https://airc.nist.gov/crosswalk (accessed May 27, 2024)

[83] N. A. Team, “NIST Trustworthy & Responsible AI Resource Center,” *airc.nist.gov*. https://airc.nist.gov/roadmap (accessed May 27, 2024).

[84] N. A. Team, “NIST Trustworthy & Responsible AI Resource Center,” *airc.nist.gov*. https://airc.nist.gov (accessed May 27, 2024)