Chapter 9
Strategies for Combating Criminal Use and Abuse of Artificial Intelligence

Kathirvel Ayyaswamy
https://orcid.org/0000-0002-5347-9110
Saveetha Engineering College, India

Naren Kathirvel
Anand Institute of Higher Technology, India

Maria Manuel Vianny
Panimalar Engineering College, Chennai, India

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.

DOI: 10.4018/979-8-3693-7041-4.ch009

Copyright © 2025, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited.

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, (Varnosfaderani &. Forouzanfar, 2024). 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, (Sadaf *et al.,* 2023). 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 (2020), 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, (Aliman, Kester, & Yampolskiy, 2021) (Butt *et al*., 2021) (Straub, 2018). Similarly, Azhar (2016) 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 (2021) 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, (Balasubramaniam *et al*., 2020). 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, (Villegas-Ch & García-Ortiz,2023). 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:

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/strategies-for-combating-criminal-use-and-abuse-of-artificial-intelligence/368386

Related Content

Examining the Awareness and Persuasive Effects of Online WOM
Irina Grinberg, Sanjib Bhuyan, Yanhong Jinand Lei Wang (2015). *International Journal of Online Marketing (pp. 1-19).*
www.irma-international.org/article/examining-the-awareness-and-persuasive-effects-of-online-wom/127068

Educating for Peace: From Pieces to Peace
Maria Lai-Ling Lam (2018). *International Journal of Technology and Educational Marketing (pp. 1-15).*
www.irma-international.org/article/educating-for-peace/207681

Web 2.0 Technologies and Marketing
Dora Simõesand Sandra Filipe (2015). *Trends and Innovations in Marketing Information Systems (pp. 1-23).*
www.irma-international.org/chapter/web-20-technologies-and-marketing/139905

Lighting the Fires of Entrepreneurialism?: Constructions of Meaning in an English Inner City Academy
Philip A. Woodsand Glenys J. Woods (2011). *International Journal of Technology and Educational Marketing (pp. 1-24).*
www.irma-international.org/article/lighting-fires-entrepreneurialism/52076

An Assessment of Blockchain and Artificial Intelligence as Transformational Technologies in Marketing
Seprianti Eka Putri (2022). *Developing Relationships, Personalization, and Data Herald in Marketing 5.0 (pp. 178-191).*
www.irma-international.org/chapter/an-assessment-of-blockchain-and-artificial-intelligence-as-transformational-technologies-in-marketing/306103