Chapter 5
The Criminal Application of Artificial Intelligence:
How Offenders Are Exploiting AI to Facilitate, Enhance, or Conceal Crime

Petros Violakis
http://orcid.org/0000-0002-6789-0592
Rabdan Academy, UAE

ABSTRACT

The rapid evolution of Artificial Intelligence (AI) has not only transformed industries and governance but has also introduced novel methods for criminal exploitation. This chapter investigates how offenders leverage AI technologies to facilitate, enhance, and conceal criminal activity. Grounded in criminological and socio-technical theories—including Routine Activity Theory and Cyber Routine Activity Theory, Rational Choice Theory, Script Theory, and Dual-Use Technology Theory—the study develops a comprehensive offender classification framework based on motivation, technical skill, role, and access model. Through a 15-question empirical questionnaire distributed among professionals in law enforcement, cybersecurity, and academia, the research examines offender profiles, AI misuse patterns, and systemic gaps in detection and policy. The chapter concludes with policy recommendations that emphasize AI-specific detection tools, regulation of generative models, and offender-targeted intervention strategies.

DOI: 10.4018/979-8-3373-5228-2.ch005

INTRODUCTION

The speed and spread of Artificial Intelligence (AI) has changed modern societies dramatically in every area including governance, commerce, communication, education and security. AI systems are now being used to assist a myriad of useful applications ranging from data analysis to automation to predictive decision-making and generative content production. Yet the same technologies that improve productivity, innovation and public service delivery are creating new potential for criminal exploitation. As access to AI tools becomes more widespread, scalable, and embedded in the daily digital space, offenders become more capable of using them to support, enrich and mask criminal efforts. This constitutes an emerging challenge for criminology, cybersecurity, and public policy, with fundamental conceptions of offending being challenged by technologies that automatically obscure deception, increase reach, and minimize operational effort and make them more difficult to detect.

The criminal exploitation of AI must be viewed in the context of an extended historical development of digitally enabled offending. Earlier phases of cyber-enabled crime were already influenced by the use of automation, scripting, phishing kits, botnets, malware reuse and cybercrime-as-a-service server infrastructures, all of which have facilitated the process of offenders industrialising new forms of deception, expanding the ways in which targets are selected, and lowering the demand for advanced bespoke expertise. What is different in the current phase of AI is not that earlier models of cybercrime have been fully replaced, but that an increasing number of systems able to produce persuasive text, realistic synthetic media, adaptive and automated decision support, are available at low cost and with only minimum technological know-how requirements. In this sense, AI is continuing a broader trend where digital tools have made it easier to identify targets, act as means of imitation of trusted communication and also serve as a means of organising criminal activity (Yamin, Ullah, Ullah, & Katt, 2021; Kaur, Gabrijelčič, & Klobučar, 2023; Choi, Dearden, & Parti, 2024; Treleaven, et al., 2023; NCSC, 2024).

Recent scholarship suggests that the technology of generative, as well as machine-learning systems, has been aiding this transition by making sophisticated forms of deception and targeting accessible to a far more extensive pool of users. Schmitt and Flechais highlight how generative AI is enhancing social engineering through its capacity for realistic content creation, sophisticated targeting and personalisation, and automatic attack infrastructures (Schmitt & Flechais, 2024), whereas Parti, Dearden and Choi (2023) highlight the fact that AI can increase criminal activity during the stages of reconnaissance, targeting, execution, and concealment (Choi, Dearden, & Parti, 2024). Broader cybersecurity scholarship has also argued that AI is a dual-use capability, which can enhance defensive detection, but also increases adversarial