Chapter 6
Artificial Intelligence and Cybersecurity Prospects and Confronts

Anya Behera
https://orcid.org/0009-0005-2809-5931
Alliance University, India

A. Vedashree
Alliance University, India

M. Rupesh Kumar
https://orcid.org/0000-0002-6229-6885
Alliance University, India

Kamal Upreti
https://orcid.org/0000-0003-0665-530X
Christ University, India

ABSTRACT

The advancement of artificial intelligence has made robust cybersecurity essential. As governments implement various policies to protect citizens, the utilization of AI by governmental agencies has significantly increased. Despite this, there is a significant gap between theoretical knowledge of AI and cybersecurity as separate fields and their practical integration. The challenge lies in the rapid evolution of both AI and cybersecurity, which often outpaces the legislative process, rendering many regulatory efforts outdated before they are fully realized. Due to the lack of dedicated laws for these dynamic areas, achieving optimal results is difficult. Therefore, it is crucial to explore how AI can be leveraged to improve cybersecurity. By using appropriate safeguards, AI can autonomously protect against threats like

DOI: 10.4018/979-8-3693-5728-6.ch006

viruses, misuse, and hacking attacks. This paper examines the role of technology in AI and cybersecurity and investigates how AI can optimize cybersecurity, the opportunities & challenges of AI in cybersecurity, regulatory bodies, and strategies to merge these fields.

1. INTRODUCTION

Artificial intelligence is broadly defined as computer systems that exhibit capabilities traditionally associated with human intelligence, including perception, understanding, learning, reasoning, and problem-solving. AI encompasses the development of these systems to perform tasks that typically require human intelligence, such as decision-making and object detection. (Tripathi and Ghatak, 2018). AI encompasses domains such as machine learning, deep learning, neural networks, natural language processing, object detection, knowledge-based expert systems, solving complex problems, increasing accuracy, and performing high-level computations.

Cybersecurity is an evolving field of study that focuses on protecting networks, systems, and data from malicious cyber threats. Cyber threats like theft, disruption, damage, and unauthorised access. It involves using a variety of technologies, processes, and strategies such as to assure integrity, obtainability of digital facts and figures as well as the confidentiality to protect sensitive information from unauthorized access or misuse. Cybersecurity encompasses a range of technical and non-technical activities and measures designed to safeguard the infrastructure of cyberspace. This protection extends to devices, software, and the information they contain and communicate, guarding them against all possible threats (Cavelty, 2018). Through the help of encryption algorithm, the data's can be well protected through converting it into a format which is not easily readable. To protect and secure the ongoing data safeguarding networks are needed. To protect, identify, secure and response immediately to any attempt of illegal access or any sceptical activities, the customers should be given knowledge and education of best practices so that they can deal, identify, and respond to any suspicious and potential risk arising in the network. As technology is evolving day by day and more people are getting connected through online platforms, cyberattacks have become more frequent and sophisticated. It is essential that organizations should start protecting their data, networks, systems, and users from cyber threats. This requires a comprehensive approach to cybersecurity that would include legal protection, preventive measures, and responsive plans.