

# Chapter 6

## Future Trends in Generative AI for Cyber Defense: Preparing for the Next Wave of Threats

**Azeem Khan**

 <https://orcid.org/0000-0003-2742-8034>

*University Islam Sultan Sharif Ali, Brunei*

**Noor Zaman Jhanjhi**

 <https://orcid.org/0000-0001-8116-4733>

*TUSB, Malaysia*

**Haji Abdul Hafidz B. Haji Omar**

*University Islam Sultan Sharif Ali, Brunei*

**Dayang H. T. B. A. Haji Hamid**

 <https://orcid.org/0000-0003-2484-5211>

*University Islam Sultan Sharif Ali, Brunei*

**Ghassan A. A. Abdulhabeib**

*University Islam Sultan Sharif Ali, Brunei*

### ABSTRACT

*The chapter entitled “Future Trends and Challenges in Cybersecurity and Generative AI,” presents a comprehensive exploration of the changing dynamics at the intersection between the rapidly growing landscape of the interconnectivity of various devices— the Internet of Things and the innovations piloted by advancements in*

DOI: 10.4018/979-8-3693-6135-1.ch006

*generative artificial intelligence. In the following background-focused analysis, the significance of the enactment of new levels of security details in this fast-growing and virulently expansive landscape is emphasized, with generative AI ultimately serving as the highlight. The conversation consequently shifts to threats. This includes a detailed depiction of new cybersecurity threats rooted in advancements in AI, featuring AI malicious actors and incidents, such as the increasingly popular phenomenon of ransomware-as-a-service as mirror illustrations of the dynamic and multifaceted character of these threats.*

## **I. INTRODUCTION**

### **A. Overview of Generative AI in Cyber Defense**

As depicted in Figure 1.0, Generative AI is a type of artificial intelligence that uses deep learning models to generate new data instances from known data instances, or training data. Cybersecurity with generative AI is a game changer: it creates attacks threats actively, as well as in synthetic form; it can compose complex defense mechanisms and from this groundwork enables cybersecurity tasks to be automated. The main impact of this duality is particularly evident here -- boosting cyber defenses and being used by attackers to create much more sophisticated, they are still natural, threats. On the back end, generative AI can help by letting you poke around in enriched data and security data — catching anomalies a threat one might miss if using traditional methods. The incidents are then responded to, and threat hunts carried out and finally, Automation drives done Although generative AI does pose a potential threat: the technology enables one to mimic different attack methods in cyberspace and thus organizations may despite being under attack apply diverse forms of security reinforcement to keep themselves safe from forthcoming dangers. But generative AI technology also has hazards on the offensive side. Hackers can use it to turn out Miami emails, problems with new feather, even deep fakes that escape initial detection techniques. In our cybersecurity environment, the tool is equally useful for both defenders and attackers because it can discover system vulnerabilities (Sindiramutty, Prabakaran, Jhanjhi, Ghazanfar, et al., 2025; Vemuri, Thaneeru, & Tatikonda, 2024).

32 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/future-trends-in-generative-ai-for-cyber-defense/374395](http://www.igi-global.com/chapter/future-trends-in-generative-ai-for-cyber-defense/374395)

## Related Content

---

### Using Probabilistic Models to Assess and Enhance Information Security

Maria Lapina, Alina Raisovna Bagautdinova and Irina Pykhtina (2026). *Navigating Technological Advancement in the VUCA and BANI World* (pp. 81-96).

[www.irma-international.org/chapter/using-probabilistic-models-to-assess-and-enhance-information-security/395670](http://www.irma-international.org/chapter/using-probabilistic-models-to-assess-and-enhance-information-security/395670)

### An Assessment on Inflation Risk and Its Effects on Business Operations

Ümit Hacolu, Hasan Dinçer and Burcu Parlak (2018). *Risk and Contingency Management: Breakthroughs in Research and Practice* (pp. 60-80).

[www.irma-international.org/chapter/an-assessment-on-inflation-risk-and-its-effects-on-business-operations/192369](http://www.irma-international.org/chapter/an-assessment-on-inflation-risk-and-its-effects-on-business-operations/192369)

### Health and Safety in Events Management

Ian Arnott (2020). *Legal, Safety, and Environmental Challenges for Event Management: Emerging Research and Opportunities* (pp. 119-137).

[www.irma-international.org/chapter/health-and-safety-in-events-management/252723](http://www.irma-international.org/chapter/health-and-safety-in-events-management/252723)

### Impact of Financial Risk Ratios on Profitability of Multinational vs. Domestic Pharmaceuticals in India

Kaushik Chakraborty (2014). *International Journal of Risk and Contingency Management* (pp. 54-68).

[www.irma-international.org/article/impact-of-financial-risk-ratios-on-profitability-of-multinational-vs-domestic-pharmaceuticals-in-india/115819](http://www.irma-international.org/article/impact-of-financial-risk-ratios-on-profitability-of-multinational-vs-domestic-pharmaceuticals-in-india/115819)

### Delivering Brown-Field Projects in the Petrochemical Industry: Challenges and Recommended Solutions

Mohammed Shafique Malik (2021). *International Journal of Risk and Contingency Management* (pp. 39-45).

[www.irma-international.org/article/delivering-brown-field-projects-in-the-petrochemical-industry/289396](http://www.irma-international.org/article/delivering-brown-field-projects-in-the-petrochemical-industry/289396)