# Chapter 11
# Natural Language Processing for Cyber Threat Intelligence in a Quantum World

**Hewa Majeed Zangana**
https://orcid.org/0000-0001-7909-254X
*Duhok Polytechnic University, Iraq*

**Firas Mahmood Mustafa**
*Duhok Polytechnic University, Iraq*

**Shuai Li**
*University of Oulu, Finland*

**Jamal N. Al-Karaki**
https://orcid.org/0009-0000-7833-3970
*Zayed University, UAE*

## ABSTRACT

*The intersection of natural language processing (NLP) and cyber threat intelligence (CTI) is gaining momentum as cybersecurity paradigms evolve to address the challenges posed by quantum computing. This chapter explores how advancements in NLP, particularly through the deployment of large language models (LLMs), can be leveraged to enhance CTI in a quantum-aware context. It discusses the capabilities of NLP systems to process vast amounts of threat data, identify patterns, and predict potential risks while considering the implications of quantum technologies on cybersecurity frameworks. Furthermore, the chapter highlights the role*

DOI: 10.4018/979-8-3373-1102-9.ch011

*of quantum-aware NLP tools in detecting advanced persistent threats, optimizing response strategies, and ensuring the resilience of digital ecosystems in the face of quantum-enabled cyber threats. By integrating LLMs with quantum computing principles, this research provides insights into the future of CTI and its evolution to counteract complex cyber challenges.*

## 1. INTRODUCTION

The rapid evolution of technology has revolutionized the way we interact with data and systems, introducing unprecedented challenges and opportunities in cybersecurity. As advancements such as large language models (LLMs), quantum computing, and artificial intelligence (AI) converge, they are reshaping the landscape of cybersecurity by enhancing both defensive and offensive capabilities. This chapter explores these transformative innovations, focusing on their potential to revolutionize the detection and mitigation of cyber threats.

### 1.1 The Role of Large Language Models in Cybersecurity

LLMs, such as GPT-3 and its successors, are increasingly recognized for their ability to process and analyze vast amounts of textual data. Their applications extend to vulnerability detection, threat analysis, and anomaly detection, marking a significant departure from traditional methods (Gholami & Omar, 2024). Recent studies have emphasized their role in automating tasks such as malware detection and phishing analysis, thereby reducing human error and response times (Omar & Zangana, 2025).

### 1.2 Quantum Computing: A Double-Edged Sword

Quantum computing represents a paradigm shift in computational power, capable of solving problems that were previously intractable for classical systems. However, this capability also introduces significant risks to traditional cryptographic systems, as quantum algorithms can potentially break widely used encryption protocols (Sodiya et al., 2024; How & Cheah, 2023). Simultaneously, quantum technologies are being explored for developing quantum-resistant algorithms, heralding a new era of cybersecurity innovation (Bishwas & Sen, 2024).

# Estimating Importance From Web Reviews Through Textual Description and Metrics Extraction

Roney Lira de Sales Santos, Carlos Augusto de Sa, Rogerio Figueredo de Sousa, Rafael Torres Anchiêta, Ricardo de Andrade Lira Rabeloand Raimundo Santos Moura (2021). *Natural Language Processing for Global and Local Business (pp. 154-179).*

www.irma-international.org/chapter/estimating-importance-from-web-reviews-through-textual-description-and-metrics-extraction/259788