



TASK 6 – RESEARCH SKILLS 3

Proposed title with variables

**The Role of Artificial Intelligence in Detecting
Cyberattacks and Improving the Security of Critical
Networks in the Comoros**

**Field:
Cybersecurity**

Prepared by

ALI MMADI, PhD student-Midocean University



Research Skills (3)

According to the concept of Task 6, we formulate 3 main hypotheses and one secondary.

Task 6

ALI MMADI

PhD student - Midocean University

www.midocean.ae

السلام عليكم ورحمة الله وبركاته

In this presentation, I will present the research hypotheses related to my future doctoral thesis entitled:

"Detection and Prevention of Cyberattacks in Critical Networks in the Comoros."

With the rapid increase of digital transformation in the world, critical infrastructures such as government networks, banks, telecommunications systems, and energy networks have become major targets for cyberattacks.

Developing countries, including the Comoros, face significant challenges in cybersecurity due to the lack of technological resources and specialized expertise. For this reason, the use of advanced technologies such as artificial intelligence becomes essential to improve the detection and prevention of cyberattacks.

In this study, we focus on two main variables: artificial intelligence in the detection of cyberattacks and the security of critical networks.



Research variables

This research includes two main variables.

The first variable is the independent variable, which is the use of artificial intelligence in the detection of cyberattacks. Artificial intelligence allows for the analysis of large amounts of network data and the identification of suspicious behaviors or anomalies that may indicate an attack.



The second variable is the dependent variable, which is the security of critical networks.

Critical networks include essential infrastructures such as government networks, financial institutions, telecommunications systems, and energy infrastructures. The relationship between these two variables is important, as the improvement of detection technologies can directly contribute to strengthening the security of critical infrastructures.

Research hypotheses

Based on the scientific literature and previous studies in the field of cybersecurity, this research proposes three main hypotheses and one secondary hypothesis.

The first main hypothesis is that the use of artificial intelligence improves the ability to detect cyberattacks in critical networks.

This means that AI-based systems can detect attacks more quickly and more effectively than traditional systems.

The second main hypothesis is that detection systems based on artificial intelligence reduce response time to cyberattacks.

Indeed, machine learning technologies can automatically analyze suspicious behaviors and trigger real-time alerts, allowing network administrators to intervene quickly.

The third main hypothesis is that the integration of artificial intelligence into cybersecurity systems strengthens the overall security level of critical networks.

This can help reduce the risks of data breaches, service disruptions, and financial losses.

Finally, the proposed secondary hypothesis is that the effectiveness of artificial intelligence in detecting cyberattacks depends on the quality of the data used and the learning algorithms.

This means that accurate and well-structured data can significantly improve the performance of AI-based detection systems.

In conclusion, this research aims to analyze the role of artificial intelligence in improving the detection of cyberattacks and the protection of critical networks in the Comoros.

The proposed hypotheses will help examine the relationship between the use of artificial intelligence and the enhancement of critical infrastructure security.

The results of this study could contribute to strengthening national cybersecurity strategies and supporting secure digital transformation in the Comoros.

Thank you for your attention ,Wa Billahi Tawfiq.

Reference Frameworks

- 1) Ian Goodfellow, Yoshua Bengio, & Aaron Courville (2016).
Deep Learning. MIT Press. [s://doi.org/10.1109/SP.2010.25](https://doi.org/10.1109/SP.2010.25)
- 2) Srinivas Mukkamala, Andrew Sung, & Ajith Abraham (2005).
Intrusion Detection Systems Using Neural Networks and Support Vector Machines.
IEEE International Joint Conference on Neural Networks
Deep Learning-Based Intrusion Detection System for Cyber Security.
- 3) Ibrahim Sarker (2021).
Machine Learning for Intelligent Cybersecurity: A Comprehensive Survey.
Journal of Big Data
- 4) National Institute of Standards and Technology (2018).
Framework for Improving Critical Infrastructure Cybersecurity.
- 5) Somesh Jha, Wenke Lee, & Salvatore Stolfo (2002).
Learning Patterns of Normal System Calls for Intrusion Detection.
Proceedings of the USENIX Security Symposium



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

