



Task 7 : Title of the study
The Impact of Artificial Intelligence on
Cyberattack Detection and Critical
Network Security in the Comoros

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University





Research Skills (3)

ALI MMADI

PhD student - Midocean University

www.midocean.ae

السلام عليكم ورحمة الله وبركاته

In this presentation, I will discuss the data collection methodology for my study in cybersecurity.

Data collection is an essential step in scientific research, as it allows testing hypotheses and obtaining reliable results.

It relies on several methods such as questionnaires, interviews, or observation. For this exploratory study, I chose to use a questionnaire as the main data collection tool.

This questionnaire is based on two main variables: the use of artificial intelligence and the capacity to detect cyberattacks.



Presentation of variables

The first variable is the use of artificial intelligence in cybersecurity. This variable represents the modern technologies used to analyze data and detect threats.

The second variable is the ability to detect cyberattacks in critical networks.

This variable measures the effectiveness of security systems in identifying attacks and protecting sensitive infrastructures.

These two variables are connected because artificial intelligence can enhance the performance of detection systems.

Questionnaire questions – Variable 1

To measure the first variable, I proposed the following five questions:

- 1) Does your organization use artificial intelligence technologies for cybersecurity?
- 2) How often are artificial intelligence systems used to monitor the network?
- 3) Do you think that artificial intelligence improves the performance of security systems?
- 4) Are AI-based tools easy to use in your organization?
- 5) Does artificial intelligence allow the detection of unknown or new threats?

These questions allow for the collection of data on the actual use of artificial intelligence and its perceived effectiveness.

Questionnaire questions – Variable 2

For the second variable , the proposed questions are as follows:

- 1) Does your current system effectively detect cyberattacks?
- 2) How long does it take to detect an attack on your network?
- 3) Have you ever experienced cyberattacks that were not detected in time ?
- 4) Does the current detection system reduce security risks?
- 5) Are you satisfied with the level of security of your critical network?

These questions help assess the actual ability to detect cyberattacks.

Link with the hypotheses

These questions are designed to test the hypotheses formulated previously, notably:
There is a statistically significant relationship between the use of artificial intelligence and the improvement of the ability to detect cyberattacks.

In conclusion,
this questionnaire constitutes a simple but effective tool for collecting data in an exploratory study.

It allows for the analysis of the relationship between artificial intelligence and cybersecurity in critical networks.

The expected results will contribute to improving cybersecurity strategies in the Comoros .

Thank you for your attention ,Wa Billahi Tawfiq.

Reference Frameworks

- 1) Research Skills 3 Course Lecture 7 Dr. Saniya Sabaa at Midocean University year 2026
- 2) Uma Sekaran & Roger Bougie (2016).
Research Methods for Business: A Skill-Building Approach
- 3) John Creswell (2014).
Research Design: Qualitative, Quantitative, and Mixed Methods Approaches
- 4) Earl Babbie (2013).
The Practice of Social Research
- 5) National Institute of Standards and Technology (2018)
- 6) Ibrahim Sarker (2021).
Machine Learning for Intelligent Cybersecurity: A Comprehensive Survey.
Journal of Big Data
- 7) International Telecommunication Union (2023).
Global Cybersecurity Index Report



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

