



Literary Criticism (3) _Task 1
*“Critical analysis of theoretical
frameworks for cybersecurity
governance in critical infrastructure in
developing countries”*

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (3)

Task 1

Introduction

Hello everyone,
As part of the Literary Criticism 3 course, this presentation focuses on the first step of week 1 of the doctoral work, namely the choice of thesis topic, applied to the field of Information Technology, with a specialization in cybersecurity.

My goal is threefold:

- ☐ Present the chosen thesis topic,
- ☐ Offer a critique of the theoretical framework used by a reference study,
- ☐ Finally, comment on the scope and relevance of this study in the current context.



1. Choice of doctoral thesis topic

The proposed thesis topic is as follows:

"Critical analysis of theoretical frameworks for cybersecurity governance in critical infrastructure of developing countries"

This choice is motivated by several observations:

- The rapid growth of cyber threats,
- The increasing dependence of states on critical information systems (energy, telecommunications, finance),
- And above all, the lack of theoretical models adapted to the realities of developing countries.

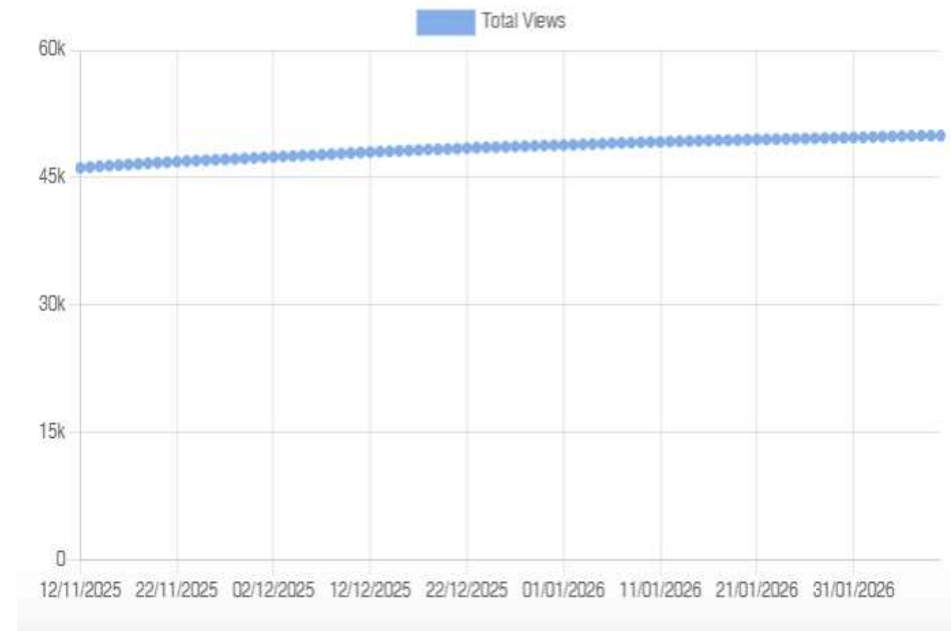
This subject lies at the intersection of:

- ❖ Cybersecurity,
- ❖ Information systems governance,
- ❖ And the critical analysis of scientific and institutional discourse.

2. Critique of the theoretical framework of the chosen study

The reference study analyzed is primarily based on:

- ❑ The cybersecurity governance framework (Cybersecurity Governance Framework),
- ❑ International standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework.



Critical Analysis

From a literary criticism perspective, these frameworks present several limitations:

- They are mostly normative, prescribing what should be done without always analyzing what is realistically feasible.
- They are based on discourses produced in Western contexts, often disconnected from the economic, institutional, and cultural realities of developing countries.
- The theoretical framework sometimes lacks a critical approach, neglecting power relations, political constraints, and technological inequalities.

Thus, the literature tends to universalize models that are not always universally applicable.

3. Scope and relevance of the study

Scope of the Study

The study has an international scope, as it is based on:

- ✓ Global standards,
- ✓ Cybersecurity policies from several countries,
- ✓ And an extensive scientific literature.

However, this scope is also a limitation, as it:

- ✓ Overgeneralizes,
- ✓ And reduces the visibility of specific local contexts.



Relevance

Despite these limitations, the study remains highly relevant because:

- ☐ It provides a solid theoretical foundation,
- ☐ It helps identify gaps between theory and practice,
- ☐ And it paves the way for a critical review, which is precisely the potential contribution of this doctoral thesis.

CONCLUSION

In conclusion, the choice of this thesis topic is fully in line with the spirit of the Literary Criticism 3 course, as it is not just about applying existing theories, but about questioning, critiquing, and contextualizing them.

This critical approach aims to contribute to a more realistic, inclusive, and tailored cybersecurity for the real needs of critical infrastructures in developing countries.

Thank you for your attention.

Cybersecurity Governance & Frameworks

1) NIST (2018).

Framework for Improving Critical Infrastructure Cybersecurity.

National Institute of Standards and Technology.

→ Foundational reference for cybersecurity governance and risk management.

2) ISO/IEC (2022).

ISO/IEC 27001: Information Security Management Systems – Requirements.

International Organization for Standardization.

→ Core international standard often critiqued for its normative and universal approach.

3) von Solms, R., & von Solms, S. (2004).

The 10 deadly sins of information security management.

Computers & Security, 23(5), 371–376.

→ Early but influential critique of managerial approaches to information security.

4) Deibert, R. J. (2019).

The Road to Digital Unfreedom: Three Painful Truths About Social Media.

Journal of Democracy, 30(1), 25–39.

5) Dunn Cavelty, M. (2014).

Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities.

Science and Engineering Ethics, 20(3), 701–715.

6) Creese, S., et al. (2021).

Cybersecurity capacity building: A review of international approaches.

Global Policy, 12(1), 64–76.

Madnick, S., & Kirlappos, I. (2020).

Cybersecurity and the developing world.

Communications of the ACM, 63(10), 28–30.....



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

