

Literary Criticism - RSC813

Assignment : Critique of Research Paper in Terms of Study Terminology/definitions and Literature Review

Prepared by : Abdulaziz Alarfaj

Article title: *“Understanding Local Government Cybersecurity Policy: A Concept Map and Framework”*

1. Study Terminology

1. Clarity and Definition of Terms:

- The paper uses specialized terms like "**Cybersecurity Framework**" (NIST CSF), "**Cybersecurity Governance**", and "**Risk Management**".
- **Observation:** While these terms are widely recognized in the cybersecurity field, some concepts—such as *cybersecurity governance* and *cybersecurity supply chain risk management*—were not clearly defined. Providing explicit definitions would have improved clarity, especially for readers unfamiliar with the field.

2. Consistency in Terminology Usage:

- There is minor inconsistency in the use of "**Cybersecurity**" and "**Information Security**". The paper could have clarified the distinction between these terms since *information security* is a subset of *cybersecurity*, but they are not interchangeable.

3. Chosen Framework:

- The study is centered around the **NIST Cybersecurity Framework (CSF) 2.0** for evaluating local government policies.
- **Observation:** Although NIST CSF is a strong choice, the authors did not justify why it was selected over other frameworks like **COBIT** or **ISO 27001**. A rationale explaining its relevance and suitability for assessing local government policies would have strengthened the argument.

4. Innovation in Terms:

- The study introduces a new concept—a "**Cybersecurity Policy Framework for Local Governments**"—aimed at addressing policy gaps.
- **Observation:** This is a valuable contribution. However, the paper lacks a deeper academic foundation connecting this new framework to existing theories or models in policy development.

2. Literature Review

1. Quantity and Diversity of Sources:

- The paper reviewed a good number of studies from various countries, including **the USA, Australia, and England**.
- **Observation:** While the focus on local government cybersecurity policies was clear, the review could have been enhanced by integrating studies on **technical challenges, social factors, or human elements** affecting local government cybersecurity (e.g., skill gaps, insider threats).

2. Analysis of Research Gaps:

- The paper identifies a clear gap: the "**absence of a unified framework for local government cybersecurity policies**" and emphasizes that most prior studies focus on technical aspects rather than policy content.
- **Observation:** This is a solid identification of a research gap. However, the paper could have strengthened this section by discussing studies that attempted to analyze policies from different perspectives, such as legal or social dimensions.

3. Linking Previous Studies to Current Research:

- The paper effectively uses existing studies to highlight the need for comprehensive cybersecurity policies and justifies the development of a new framework.
- **Observation:** Despite this, a more detailed comparison between the findings of prior studies and the current study's results would have provided stronger support for the proposed framework.

4. Recency of Literature:

- The cited studies are relatively recent (2018–2023), ensuring the research is up-to-date.
- **Observation:** Nevertheless, referencing a few seminal or foundational works in cybersecurity policy could have added historical context and depth to the literature review.

Overall Evaluation

- **Strengths:**

- Clear focus on using a modern cybersecurity framework (NIST CSF 2.0).
- Solid identification of a genuine research gap in local government cybersecurity policies.

- **Weaknesses:**

- Some technical and social terms lacked clear definitions or contextual explanations.
- The literature review could have been broader, incorporating multi-disciplinary perspectives (technical, legal, social).