

Research Issues

RSC811-Assignment 5

Prepared by
Abdulaziz Alarfaj



Part

1

Research Title : العنوان

Title: "An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure"

Field of Study: The title reflects a highly relevant and critical area of study, especially given the increasing cyber threats to critical infrastructure. The paper examines cybersecurity policies for critical infrastructure, a topic of significant importance in today's digital world.

Key Variables:

Dependent Variable: Success or failure of cybersecurity policies for critical infrastructure.

Independent Variables: Nature of the cyber threat, regulatory pressure, and intra-industry competition.

Mediating/Moderating Variables: Historical relationships between industry and government, size and complexity of the sector, and personal relationships among individuals.

Application Scope: The study applies to critical infrastructure sectors in the United States, such as energy, communications, financial services, and others.

Introduction : المقدمة

Clarity of Variables: The introduction effectively outlines the challenges faced by critical infrastructure in the face of cyber threats. The key variables (cyber threat, regulatory pressure, and industry-government collaboration) are clearly presented, with an explanation of how these factors influence the success or failure of policies.

Conciseness: The introduction is concise and comprehensive, providing background on the importance of critical infrastructure and the challenges it faces, while indicating that the study will analyze how these factors interact across different sectors.

Problem Statement : مشكلة الدراسة

Problem Identification: The problem is clearly identified by pointing out that previous studies have not evaluated the effectiveness of current cybersecurity policies for critical infrastructure. The main issue is that current policies rely on voluntary partnerships between the government and private sector, but their effectiveness varies across sectors.

Research Questions: The study seeks to answer questions about the factors that lead to the success or failure of these policies and how they can be improved. The main research questions are implicitly formulated through the analysis of influencing factors.

أهمية الدراسة : Importance of the Study

Theoretical Significance: The study contributes to the existing literature on cybersecurity by analyzing how different factors (such as cyber threats, regulatory pressure, and industry-government collaboration) interact in various sectors.

Practical Significance: The study offers practical recommendations for policymakers on how to improve cybersecurity policies for critical infrastructure, emphasizing the need to consider the unique characteristics of each sector.

أهداف الدراسة : Objectives of the Study

Objectives: The study aims to analyze the factors that influence the success or failure of cybersecurity policies for critical infrastructure and provide recommendations for improving these policies. The objectives are realistic and achievable through the qualitative analysis conducted.

Achievement of Objectives: The study achieves its objectives by analyzing interviews with over 40 policymakers and senior private sector managers, as well as public documents.

Concepts and Definitions : مفاهيم وتعريفات الدراسة

Theoretical Framework: The study relies on concepts such as "cyber threat," "regulatory pressure," and "industry-government collaboration." These concepts are clearly defined, with an explanation of how they interact in the context of critical infrastructure.

Sub-dimensions: The study identifies sub-dimensions such as "nature of the threat," "historical relationships between industry and government," and "size and complexity of the sector." These sub-dimensions were selected based on their potential impact on policy success.

الدراسات السابقة - Previous Studies

Recent Studies: The study cites recent and contemporary studies, focusing on gaps in the current literature, such as the lack of a comprehensive evaluation of the effectiveness of current policies.

Agreements and Disagreements: The study notes that existing literature has focused on the legal and political aspects of cybersecurity but has not evaluated how these policies work in practice. The current study attempts to fill this gap through qualitative analysis.

Hypotheses : فرضيات الدراسة

Hypotheses: The study does not explicitly state hypotheses but analyzes the factors that influence the success or failure of policies. It can be inferred that the study tests the hypothesis that policy success depends on the nature of the cyber threat and regulatory pressure.

Alignment with Title and Variables: The implicit hypotheses are closely aligned with the study's title and variables, as they attempt to explain how these variables interact to achieve success or failure.

نموذج الدراسة : Study Model

Study Model: The study presents an analytical model that illustrates the relationships between different variables (cyber threat, regulatory pressure, industry-government collaboration) and how they influence policy success. The model clearly represents these relationships and indicates the direction of the hypotheses to be tested.

Methodology and Statistical Analysis: منهجية الدراسة و التحليل الاحصائي

Methodology: The study employs a qualitative methodology, conducting interviews with over 40 policymakers and senior private sector managers. Additionally, public documents and government reports were analyzed.

Data Sources: Data were collected through semi-structured interviews and public documents.

Population and Sample: The sample included policymakers and private sector managers in critical infrastructure sectors.

Statistical Methods: The study did not use traditional statistical methods but relied on qualitative data analysis.

Discussion of Results and Recommendations : مناقشة النتائج والتوصيات

Interpretation of Results: The study provides a clear interpretation of the results, showing that policy success largely depends on the nature of the cyber threat and regulatory pressure. It also highlights the importance of industry-government collaboration in improving cybersecurity.

Alignment with Literature: The results align with some existing literature but offer new insights into how different factors interact across sectors.

Achievement of Objectives: The study achieves its objectives by providing practical recommendations for improving cybersecurity policies.

Recommendations: The study recommends considering the unique characteristics of each sector when designing cybersecurity policies and emphasizes the need to strengthen industry-government collaboration.

Future Research: The study suggests further research on how to improve industry-government collaboration in other sectors.

Overall Assessments :

The research paper provides a comprehensive and detailed analysis of cybersecurity policies for critical infrastructure, focusing on the factors that influence their success or failure.

The study is clear in defining its variables and objectives and offers practical recommendations that can be applied in real-world settings.

The paper contributes to the field by addressing gaps in the literature and suggesting future research directions.

Article link :

https://dspace.mit.edu/bitstream/handle/1721.1/140630/10_1111_puar_13322.pdf?sequence=5&isAllowed=y