

**Erman Ace M. Cerujano**

**COE – 3B**

## **Final Assignment 2**

National Cybersecurity Plan (NSCP) of The Philippines by DICT.

The National Cybersecurity Plan (NSCP), introduced by the Department of Information and Communications Technology (DICT) in The Philippines, seeks to tackle the increasing threats in the digital realm. This analysis delves into the NSCP's goals, strategies for implementation, hurdles, and its potential influence on the country's cybersecurity stance.

Amidst the swift digitization and global interconnection, cybersecurity has become a pivotal issue for countries across the globe. Acknowledging the imperative to bolster its digital security, the Philippines introduced the National Cybersecurity Plan (NSCP) under the guidance of the Department of Information and Communications Technology (DICT). This study scrutinizes the NSCP through the lens of the IMRAD format, exploring its fundamental elements and evaluating its effectiveness in protecting the nation's cyber resources.

The NSCP's core aim is to bolster The Philippines' cybersecurity resilience through a comprehensive framework spanning prevention, detection, response, and recovery mechanisms. Through delineating clear goals and strategies, the plan endeavors to diminish cyber threats, strengthen infrastructure protection, and foster cybersecurity awareness across various sectors.

This critique utilizes a qualitative analysis methodology, drawing insights from academic literature, governmental publications, and expert viewpoints to assess the strengths and weaknesses of the NSCP. Key areas of examination include its alignment with international standards, coherence in implementation strategies, engagement with stakeholders, and adaptability to evolving cyber threats.

The NSCP demonstrates a commendable dedication to tackling cybersecurity issues in The Philippines. Its multifaceted approach, which integrates policy frameworks, capacity-building programs, and public-private partnerships, reflects a nuanced understanding of the intricate nature of cyber threats. Additionally, the plan's emphasis on fostering collaboration among governmental bodies, industry stakeholders, and civil society highlights a concerted effort to establish a resilient cyber environment.

However, several drawbacks undermine the NSCP's efficacy. Firstly, while the plan articulates ambitious goals, its implementation faces challenges due to resource limitations and bureaucratic obstacles. Constraints such as insufficient funding, shortage of personnel, and administrative hurdles impede the timely execution of cybersecurity initiatives, thereby limiting the plan's practical effectiveness. Moreover, the lack of robust enforcement mechanisms and accountability measures raises concerns regarding the plan's long-term viability.

The NSCP represents a significant stride towards enhancing The Philippines' cybersecurity resilience, yet its success hinges on overcoming implementation obstacles and fostering a culture of cyber resilience. To address resource constraints, continuous investment in cybersecurity infrastructure and human capital is essential. Additionally, enhancing coordination mechanisms and promoting inter-agency cooperation can facilitate smoother execution of cybersecurity measures. Furthermore, strengthening regulatory frameworks and establishing rigorous monitoring mechanisms are crucial to ensure compliance and accountability among stakeholders.

In summary, the NSCP embodies a proactive approach to bolstering cybersecurity in The Philippines. However, its effectiveness depends on addressing implementation challenges and enhancing collaboration across sectors. Through concerted efforts from government, industry, and civil society, The Philippines can navigate the evolving cyber threat landscape and emerge as a resilient digital nation.