VOLUME 1, ISSUE 1 (2024)
PJSET
PHILIPPINE JOURNAL OF SCIENCE, ENGINEERING, AND TECHNOLOGY

RESEARCH ARTICLE

Assessing the Philippine National Cybersecurity Plan 2022 for SMEs: Challenges and Opportunities

Matthew Henry P. Bibangco[1]* | Elson B. Manahan[1]

[1]University of the Philippines Diliman, Roxas Ave, Quezon City, Metro Manila, 1101, Philippines
***Correspondence:** mpbibangco@alum.up.edu.ph

Article History:
Received: Nov 14, 2023
Revised: Feb 20, 2024
Accepted: Mar 31, 2024

Keywords:
Cybersecurity Compliance
Cyber Resilience Measures
Global Cybersecurity Agenda
ICT Infrastructure Security
National Cybersecurity Strategy

Presented during the 1st Bacolod City Local Governance Resource Center Research Forum at Talisay City, Philippines on November 23, 2023; Awarded Best Paper

Abstract

In response to the escalating demands of the Information and Communications Technology (ICT) sector, the Philippine Department of Information and Communications Technology introduced the National Cybersecurity Plan (NCSP) 2022 in May 2017. Amid rising cyber threats targeting the BPO and Offshore Gaming sectors, the NCSP 2022's robust framework is crucial for national economic security. The critical nature of this plan highlights its foundational role in national development, propelled by an increasing dependency on ICT solutions. This study aims to rigorously evaluate the alignment of the NCSP 2022 with the International Telecommunications Union's Global Cybersecurity Agenda (GCA) through a comprehensive benchmarking of its five pillars: legal measures, technical and procedural measures, organizational structure, capacity building, and international cooperation. Using a mixed-methods approach, this study combines quantitative data from an extensive spectrum of scholarly articles, official reports, and industry standards on cybersecurity, supplemented by qualitative insights from expert interviews. The findings reveal that while the NCSP 2022 excels in organizational structure and capacity building, it requires legal measures and international cooperation improvements. Regardless, the assessment yielded an impressive cumulative compliance score of 88.5%, showing a significant adherence to the GCA standards. Despite its robust alignment with global benchmarks, the findings underscore the need for policymakers to prioritize the development of a cybersecurity legislative framework, offering professionals more straightforward guidelines for compliance.

1 | INTRODUCTION

In the digital age, the Internet and Information and Communication Technology (ICT) have become pivotal forces, driving innovation, fostering global connectivity, and facilitating economic growth by democratizing access to information. The International Telecommunication Union (ITU) underscores this transformation, reporting a consistent annual increase of approximately 10% in global internet users, a testament to the growing digital dependence [1], [2]. This trend is particularly pronounced in the Philippines, where internet penetration rates have soared, ranking Filipinos among the world's most avid internet users, with an average daily screen time surpassing ten hours [3]. However, while indicating new opportunities, this digital integration has also heightened vulnerabilities to cyber threats, introducing complex challenges, particularly in Business Process Outsourcing and Philippine Offshore Gaming Operators [4]. The significant rise in web attacks and data breaches underscores the urgent need for robust and comprehensive cybersecurity measures to protect sensitive data and ensure national security [5], [6]. Moreover, the strategic targeting of governmental infrastructures by cybercriminals amplifies the necessity for national cybersecurity strategies (NCSS) to protect sensitive data and ensure national security [7], [8].

Recognizing these cybersecurity challenges, the Republic of the Philippines has proactively developed the National Cybersecurity Plan (NCSP) 2022 to enhance the nation's cyber resilience and readiness by establishing a coherent framework

Cite as: M.P. Bibangco & E.B. Manahan, "Assessment of the Philippine National Cybersecurity Plan 2022," PJSET, vol. 1, no. 1, pp. 1-9, 2024.

to tackle digital-era challenges [9]. Despite existing efforts, a gap persists in the scholarly evaluation of how national strategies like the NCSP 2022 align with global cybersecurity standards, such as the ITU's Global Cybersecurity Agenda (GCA); hence, this study seeks to fill this gap by benchmarking the NCSP 2022 against the GCA's five pillars [10], [11]. This analysis aims to identify the strengths and weaknesses within the NCSP 2022, offering policymakers actionable data to refine and enhance the country's cybersecurity posture.

The remainder of this paper is organized as follows: Section II reviews related studies and establishes the theoretical framework guiding this research. Section III details the methodology for benchmarking the NCSP 2022 against global standards. The results and discussion are presented in Section IV. Finally, Section V concludes the paper with recommendations and suggestions for future research.

2 | RELATED STUDIES

A. Overview of Global Cybersecurity Threats

Cybersecurity has evolved into an ever-shifting battlefield, reflecting the complexity and sophistication of threats that challenge individuals, organizations, and nations across the globe. The cyber risk landscape is characterized by diverse threats, including phishing, web-based attacks, malware, denial of service attacks, zero-day vulnerabilities, cross-site scripting, and Internet of Things (IoT) vulnerabilities [12]. This spectrum of threats has expanded to include advanced persistent threats, ransomware, exploits targeting IoT devices, and social engineering tactics, indicating a shift towards more sophisticated challenges that require innovative and adaptable defense strategies [13].

In the future, cybersecurity is expected to confront an escalation in threat complexity. Emerging vulnerabilities associated with IoT, potential misuse of artificial intelligence and machine learning, quantum computing risks, supply chain disruptions, cloud security vulnerabilities, and persistent challenges such as phishing and social engineering signal a forthcoming era where cyber-attacks reach unprecedented complexity [14]. This evolving landscape requires a shift towards a cybersecurity posture that is both proactive and evolutionary, adapting continuously to mitigate the rising complexity of cyber threats [15].

The implications of cybersecurity threats extend beyond data breaches, impacting national security and economic stability. Cyber-attacks on the financial and banking sectors illustrate the economic consequences of such threats, leading to significant financial losses and diminishing trust in digital financial systems [16]. The deliberate targeting of critical infrastructure and governmental institutions by adversaries elevates cybersecurity from a technical dilemma to a crucial national security issue. Cyberterrorism is now considered a threat to state security in specific contexts [17].

The international dimension of cybersecurity is highlighted by the increasing efforts of states to develop comprehensive defensive and offensive cyber capabilities, underscoring the strategic significance of cyberspace in both national and international security arenas [18]. Collaborative endeavors, such as the ASEAN-Singapore Cybersecurity Centre of Excellence, illustrate the collective effort to enhance regional cybersecurity defenses. These initiatives recognize the universal challenge cyber threats pose and the necessity for coordinated, cross-border responses [19].

B. Global Cybersecurity Strategies and Frameworks

ITU has played a crucial role in developing a comprehensive cybersecurity framework through its GCA. It is organized around five foundational pillars: legal measures, technical measures, organizational structures, capacity building, and international cooperation. These pillars are designed to foster a unified approach to cybersecurity, highlighting the necessity for a collective international response to the threats posed by cyber vulnerabilities and advocating for the bolstering of global network infrastructure security. While direct literature focusing exclusively on the ITU's GCA was not identified in the recent search, the widespread acknowledgment of the framework highlights its essential contribution to steering cybersecurity initiatives.

NCSS exhibits considerable variation across different countries, mirroring diverse national priorities, cyber threat landscapes, and governance models. A comprehensive NCSS is critical in combating cyber threats, representing a fundamental measure for protecting digital assets and national security. Effective strategies are characterized by the integration of legal, technological, organizational, and procedural components specifically adapted to meet the unique challenges and contexts of each nation [20], [21], [22]. For instance, the cybersecurity strategy in the United States delineates a distinct security policy for governmental and military networks and advocates for international cooperation in cybersecurity matters. It formulates a robust defensive strategy to deter potential adversaries. The National Institute for Standards and Technology (NIST) Cybersecurity Framework in the U.S. further exemplifies a policy framework tailored for critical infrastructure sectors aimed at managing and mitigating cybersecurity risks below the threshold of armed conflict, thereby exemplifying a national effort to enhance cybersecurity resilience [23], [24].

Moreover, international cooperation is a pivotal element in reinforcing national cybersecurity stances. Ukraine's strategic partnership with the North Atlantic Treaty Organization (NATO) in cybersecurity matters reflects a mutual dedication to confronting the evolving cybersecurity threat landscape through joint efforts and capacity-building initiatives. A comparative analysis of the European Union's and NATO's cybersecurity strategies with those of individual nations highlights the significance of synchronizing national policies with broader international frameworks. Such alignment is instrumental in ensuring unified actions against cyber threats, capitalizing on shared expertise and resources [25], [26].

C. Cybersecurity in the Philippines

The Republic of the Philippines has experienced substantial growth in ICT and digitalization, transitioning significantly towards a more interconnected and digitally enabled society. This evolution has played a crucial role in propelling economic development, broadening access to information, and enhancing global connectivity. Nonetheless, the swift pace of digitalization introduces several challenges, particularly in cybersecurity, where safeguarding digital assets and infrastructures is paramount. The increasing digital footprint of the Philippines has made it a target for cybercriminals, showing the urgent need for comprehensive cybersecurity measures. Additionally, integrating digital technologies across various sectors has magnified the potential impact of cyber incidents, making developing resilient cybersecurity frameworks a national priority.

A range of challenges attributable to the growing dependence on digital technologies and the internet marks the cybersecurity landscape in the Philippines. The country confronts various cyber threats that pose risks to national security, economic stability, and the privacy of its citizens. Among the primary challenges in implementing efficacious cybersecurity measures are the complexity of cyber-attacks, the absence of a comprehensive legal framework, and a pressing need for heightened cybersecurity awareness and expertise [27]. The Philippine government's strategies to strengthen national security through cyber initiatives reflect a proactive stance. However, these efforts highlight ongoing vulnerabilities and underscore the critical need for a robust cybersecurity infrastructure [28].

Several strategies have been advocated to cultivate cybersecurity awareness and innovation among academics and the wider population. These include employing Scientometric analysis to gauge and navigate the cybersecurity research landscape, bridging cybersecurity with other academic disciplines, selecting research topics with significant appeal and relevance, and incorporating machine learning and IoT technologies into cybersecurity research endeavors [19]. These approaches are intended to promote a holistic understanding and foster the development of innovative solutions to address cyber threats effectively.

D. Philippine National Cybersecurity Plan (NCSP) 2022

The NCSP 2022 of the Philippines embodies a comprehensive and strategic framework designed to protect the country's ICT infrastructure against evolving and increasingly sophisticated cyber threats [4]. It integrates a broad spectrum of risk management practices, advocates for developing national cybersecurity standards, and promotes the formation of international partnerships. This initiative adopts a holistic approach to cybersecurity, addressing aspects from prevention and detection to response and recovery. An essential element of this plan is the emphasis on capacity building and workforce development, aimed at cultivating a continuous supply of skilled cybersecurity professionals. Moreover, it highlights the critical role of public-private partnerships in establishing a resilient cybersecurity posture, acknowledging the necessity of collaborative efforts to mitigate cyber risks effectively [4].

ITU has established GCA as a conceptual model for understanding the global cybersecurity domain and a practical guide for national and international action to foster a more secure and safe information society [2]. The GCA outlines seven main goals, continually refined and updated by the work of the High-Level Experts Group on Cybersecurity, to advance a model of cybercrime legislation, endorse national strategies, establish minimum security criteria, facilitate a global incident response framework, endorse a universal digital identity system, and promote capacity-building for a collaborative approach to cybersecurity [2].

1. Develop a model of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures and create a framework for legislative harmonization for interested countries.
2. Global endorsement of national strategies and a generic policy model to deal with cybercrime by creating appropriate national and regional organizational structures.
3. Development of a strategy for establishing globally accepted minimum security criteria and accreditation schemes for software applications and systems through cooperation with existing national and regional public and private sector initiatives.
4. Creation of a global framework for watch, warning, and incident response to ensure cross-border coordination between new and existing initiatives.
5. Creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries.
6. Developing a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and the areas mentioned earlier.
7. Development of a global multi-stakeholder strategy and framework for international cooperation and coordination in the abovementioned areas.

E. Gap and Research Imperative

Despite the increasing complexity of cyber threats, existing literature points to a significant gap in evaluating national cybersecurity strategies against international benchmarks. This deficiency marks a crucial area for academic exploration and policy formulation, particularly in regions with high cybersecurity stakes for national security, such as the Philippines [30]. Furthermore, the discourse within cybersecurity research has predominantly focused on cyber warfare, sometimes neglecting vital aspects such as cyber peace and the resilience of cybersecurity frameworks in the face of evolving threats [31]. Recent studies have underscored the importance of adopting a multidisciplinary approach to cybersecurity that integrates technological, societal, and policy dimensions to comprehensively address the diverse nature of cyber threats [32]. Nonetheless, there remains an acute need for more research to benchmark national cybersecurity strategies, like the Philippines' NCSP 2022, against international frameworks such as ITU's GCA.

Benchmarking national cybersecurity strategies against global standards is essential for multiple reasons. Primarily, it offers a structured method to assess the effectiveness and thoroughness of a national strategy in countering the contemporary cyber threat landscape. Such evaluations are indispensable for ensuring that nations are adequately prepared to mitigate cyber threats and strengthen their cyber resilience. The GCA by the ITU presents a globally acknowledged framework for this evaluation, underscoring the importance of incorporating legal, technical, and procedural measures, organizational structures, capacity building, and international cooperation within cybersecurity efforts [33]. Furthermore, benchmarking enables the identification of strengths and potential weaknesses within national strategies, illuminating areas needing strategic improvements to better align with global best practices.

The scholarly community has also highlighted the significance of collaboration among various stakeholders in propelling cybersecurity research and education forward to keep pace with the rapidly evolving landscape of cyber threats [34]. Integrating cybersecurity principles into university curricula is critical in developing a workforce adept at addressing current and emergent cybersecurity challenges.

This collaborative and educational advancement is pivotal in fortifying national and global cybersecurity postures, preparing the next generation of cybersecurity professionals to navigate and secure the increasingly digitalized global landscape [35].

3 | METHODOLOGY

A. Research Design

This study is grounded in a qualitative research design, specifically leveraging the benchmarking method to critically assess the alignment of the NCSP 2022 of the Philippines with the ITU's GCA. The selection of a qualitative approach was motivated by the objective to delve deep into the qualitative nuances of the NCSP 2022 and the GCA framework, enabling a rich, contextual analysis beyond mere numerical comparisons. Benchmarking was chosen for its utility in conducting systematic and comprehensive comparisons, allowing for the examination of the NCSP 2022 against the backdrop of internationally recognized standards and best practices in cybersecurity.

The benchmarking process undertaken in this study was methodical and multi-phased. The NCSP 2022 document was initially reviewed to identify its core components and objectives. Concurrently, an in-depth analysis of the GCA framework was performed, focusing on its foundational pillars and the specific criteria outlined by the ITU's GCI computation methodology. This dual analysis established the basis for comparison and set the stage for the subsequent benchmarking analysis.

Following the preparatory review, the study employed a detailed benchmarking framework, which involved mapping the objectives and initiatives of the NCSP 2022 against each of the five pillars of the GCA. This mapping was guided by the GCI's computation methodology, as outlined by [36], which provided a structured approach to evaluating the alignment and compliance with global cybersecurity standards. In addition, the study incorporated expert insights and secondary data sources, including academic literature, official reports, and relevant cybersecurity best practices, to further substantiate the benchmarking analysis.

B. Data Collection Process

The data collection process for this study was meticulously designed to ensure a comprehensive understanding of the alignment between the NCSP 2022 of the Philippines and the ITU's GCA. This process encompassed reviewing secondary sources and conducting expert interviews, offering a dual approach to data gathering that leverages the depth and breadth of existing knowledge alongside expert perspectives.

The secondary data collection phase involved a review of scholarly articles, official reports, policy documents, and recognized best practices within cybersecurity. This review targeted publications from reputable sources within the last five years, ensuring relevance and timeliness in the context of rapidly evolving cybersecurity landscapes. The selection of sources was guided by specific criteria, focusing on those that offered insights into:

- Global cybersecurity standards and frameworks, particularly those relating to the ITU's GCA.
- The implementation and assessment of national cybersecurity strategies, emphasizing methodologies related to data analytics, digital forensics, and threat modeling.
- Case studies or evaluations of cybersecurity initiatives demonstrating practical applications of the GCA's pillars.

This literature review contextualized the study within the current state of cybersecurity research and identified relevant indicators for evaluating the NCSP 2022 against the GCA's pillars. These indicators were then categorized and weighted based on their recurrence in the literature and perceived impact on effective cybersecurity strategy implementation, providing a structured framework for subsequent analysis. The primary data collection phase featured a semi-structured interview with the Director of the DICT Cybersecurity Bureau. This interview was conducted following a pre-defined protocol that aimed to explore:

- The strategic objectives and key initiatives of the NCSP 2022.
- Perspectives on the challenges and successes in aligning the NCSP 2022 with international cybersecurity standards, including the GCA.
- Insights into the process of developing and implementing cybersecurity measures within the Philippines and the role of international cooperation and partnerships.

The selection of the Director of the DICT's Cybersecurity Bureau as the primary interviewee was based on their central role in the formulation and execution of the NCSP 2022, ensuring authoritative insights into the plan's objectives, challenges, and achievements. The interview was complemented by additional consultations with cybersecurity experts and practitioners to validate findings and enhance the study's empirical base.

C. Data Analysis

The compliance scoring was grounded in a methodology that mirrors empirical research practices in cybersecurity. Such practices typically involve synthesizing data across various cyber-attack types and defense strategies to foster improvements in cybersecurity behaviors and practices [39]. This study adopted a similar approach by meticulously evaluating the NCSP 2022's adherence to each of the GCA's pillars, as shown in Table 1.

TABLE 1. ITU's Five Pillars of GCA and Weight.

No	Indicator	Weight
1	Legal Framework	20%
2	Technical Measure	20%
3	Organizational Structures	20%
4	Capacity Building	20%
5	International Cooperation	20%

To ensure a balanced and equitable evaluation, weights were assigned to each GCA's pillars, reflecting their relative importance in a comprehensive cybersecurity strategy. According to the ITU, a panel of experts was convened to determine the appropriate weighting for each pillar and its corresponding indicators. Each expert contributed their assessment of the weights, with the final weighting for each

pillar calculated as an average of these expert opinions, resulting in an equal distribution across the five pillars.

The evaluation framework for assessing compliance levels was inspired by methodologies used in the analysis of cybersecurity training programs, which emphasize the significance of categorizing and quantifying the effectiveness of cybersecurity measures. Following the approach suggested by Hewaidy and Mutawaa [41], the level of compliance was classified into four distinct levels that allowed for a detailed analysis of the NCSP 2022's strengths and areas for improvement concerning each of the GCA's pillars.

The compliance levels were determined based on a comprehensive analysis of how the NCSP 2022's initiatives and measures fulfilled the criteria associated with each GCA pillar. The findings from this analysis were then aggregated to calculate a cumulative compliance score for the NCSP 2022, providing a quantitative measure of its alignment with the GCA's standards. By employing this structured and systematic approach to compliance scoring, the study offers a rigorous assessment of the NCSP 2022's alignment with international cybersecurity standards. This analysis highlights the plan's areas of strength but also identifies critical gaps and opportunities for enhancement, thereby contributing valuable insights to policymakers and stakeholders in the ongoing effort to strengthen the Philippines' cybersecurity posture.

TABLE 2. Four Levels of Compliance.

Domain	Interpretation	Implication
>80%	High level	A high number of requirements fully complied
60%-79%	Intermediate level	Majority of the requirements were complied but lower than 80%
40%-59%	Low level	The number of requirements complied with is almost the same as those that still need to comply.
<40%	Non-compliant	There is a massive gap between the requirements and those complied with.

4 | RESULTS AND DISCUSSION

The evaluation of the NCSP 2022 against ITU's GCA has unveiled a notable degree of alignment, with the NCSP 2022 demonstrating substantial compliance across a broad spectrum of cybersecurity measures. An in-depth analysis of 25 distinct indicators—ranging from legislative frameworks and technical measures to the efficacy of public-private partnerships and the implementation of cybersecurity best practices—revealed that the NCSP 2022 complies with 21 of these indicators. This compliance encompasses a comprehensive array of cybersecurity domains, underscoring the Philippines' concerted efforts to enhance its cybersecurity infrastructure and policy landscape.

However, the evaluation also identified areas requiring further attention and development. The NCSP 2022 showed only partial compliance with the indicator related to establishing a standardization body, a critical component for ensuring consistency and interoperability of cybersecurity practices across different sectors. Furthermore, complete compliance was not achieved in three key areas: enacting specific legislation targeting spam, developing incentive mechanisms to encourage cybersecurity compliance and innovation, and active participation in international fora. These gaps highlight potential vulnerabilities and underscore the importance of continuous improvement in the Philippines' cybersecurity strategy.

The cumulative compliance score of 88.5% represents a high level of adherence to the GCA's comprehensive requirements, marking a significant advancement from the Philippines' performance in the 2018 GCI score [2]. This improvement reflects the country's ongoing commitment to strengthening its cybersecurity posture in alignment with global standards and practices.

A closer examination of the compliance levels across the GCA's five pillars provides additional insights. The NCSP 2022 exhibited high compliance in four pillars: technical measures, organizational structures, capacity building, and international cooperation. Such high levels of compliance suggest that the Philippines possesses a robust and practical framework for addressing a wide range of cybersecurity threats, showcasing the nation's proactive approach to enhancing its cybersecurity capabilities.

Conversely, the legal framework pillar achieved an intermediate level of compliance at 66.7%, indicating a need for further enhancements in the legislative domain. This finding points to the critical role of comprehensive and up-to-date legal measures in underpinning a nation's cybersecurity strategy. Strengthening the legal framework could involve introducing more specific cybersecurity laws, updating existing legislation to address emerging threats, and efforts to ensure that legal measures are fully aligned with international standards and practices.

A. Legal Framework

Strengths. The NCSP 2022's legal foundation is firmly rooted in established laws, notably the Cybercrime Prevention Act of 2012 (RA 10175) and the subsequent establishment of the Cybercrime Investigation and Coordinating Center (CICC). These measures exemplify the Philippines' commitment to crafting a legally robust cybersecurity framework that aligns with global standards and practices, mirroring developed nations like the United Kingdom in its approach to legislating cyberspace activities [5], [10], [22]. Additionally, the plan's focus on enhancing the capacity of law enforcement agencies, as recommended by the ITU and supported by other studies [21][39], represents a holistic strategy to combat cybercrime. This strategy emphasizes the importance of advanced investigative capabilities and recognizes the value of international collaboration in addressing cyber threats. This dual approach ensures that the legal framework of the NCSP 2022 is both comprehensive and practical, facilitating a coordinated response to cybersecurity challenges.

Weaknesses. However, the analysis also reveals critical areas where the NCSP 2022's legal framework could be further strengthened. One notable shortfall is the plan's reliance on existing legislation without introducing new measures to address emerging threats, such as spam and other cyber nuisance [27][28]. This oversight suggests a significant gap in the current legal framework, potentially limiting the effectiveness of the Philippines' cybersecurity efforts. Compared to its ASEAN counterparts, the Philippines appears to lag in developing specific cybersecurity legislation, highlighting an urgent need for dedicated laws that address the

evolving landscape of cyber threats [26][27]. The absence of specific legislation for spam, incentive mechanisms for cybersecurity compliance and innovation, and active engagement in international cybersecurity discussions points to areas that require immediate attention.

To bridge these gaps, the Philippines could benefit from a comprehensive review and update of its cybersecurity legislation, taking cues from international best practices and the legislative frameworks of leading nations in cybersecurity. Developing dedicated laws targeting specific aspects of cyber threats, such as spam, would enhance the legal framework's effectiveness and signal the country's proactive stance in safeguarding its digital domain. Additionally, introducing incentive mechanisms could motivate stakeholders to adhere to cybersecurity standards and contribute to a more resilient national cybersecurity infrastructure. Finally, increasing participation in international forums and collaborations would provide the Philippines with insights into global cybersecurity trends, facilitating the alignment of its legal framework with international norms and standards.

B. Technical Measures

Strengths. The NCSP 2022 of the Philippines exemplifies a commendable commitment to safeguarding the nation's digital landscape through its comprehensive engagement with technical cybersecurity measures. By aligning with international standards, notably the NIST Cybersecurity Framework, the NCSP 2022 ensures high protection for stakeholders across various sectors. This alignment not only enhances the resilience of the Philippines' cybersecurity infrastructure but also fosters trust and cooperation among international partners [13], [16], [37].

The NCSP 2022 proactive stance is further evidenced by incorporating advanced security technologies, essential in the ever-evolving realm of cyber threats. Establishing national and sector-specific Computer Emergency Response Teams (CERTs) is a critical step toward a centralized and coordinated response mechanism for cyber incidents. Such structures are pivotal in facilitating rapid response and recovery operations, thereby mitigating the impact of cyber-attacks [13], [16], [37].

Moreover, its dedication to research and development (R&D) signifies an investment in the future of cybersecurity in the Philippines. By prioritizing R&D and engaging with threat intelligence centers, the Plan actively contributes to the global cybersecurity knowledge base, ensuring that the Philippines remains at the forefront of cyber defense technologies and strategies. This forward-looking approach is instrumental in adapting to and pre-empting emerging cybersecurity challenges [20], [38].

Weaknesses. Despite these significant strengths, the NCSP 2022's approach to technical measures reveals areas necessitating further refinement. A notable concern is its need for greater specificity in applying and integrating certain security technologies. This vagueness leads to inconsistencies in implementation and could potentially undermine the overall effectiveness of the cybersecurity strategy. A more detailed guideline on deploying these technologies would enhance the Plan's comprehensiveness and efficacy [14], [35].

The absence of a national cybersecurity standardization body is also identified as a critical gap within the NCSP 2022. Standardization is paramount in ensuring uniformity and interoperability among cybersecurity solutions, which is especially crucial in a digital ecosystem as diverse as the Philippines'. Establishing such a body would facilitate the adoption of emerging standards and contribute to the secure development and deployment of next-generation technologies. Addressing this gap is essential for maintaining a resilient and adaptive cybersecurity framework capable of countering contemporary and future cyber threats [14], [35].

C. Organizational Structures

Strengths. The NCSP 2022 establishes a solid organizational foundation for the Philippines' cybersecurity initiatives by clearly articulating its objectives and the strategic designation of authorities responsible for the plan's implementation. This structure is pivotal for ensuring cybersecurity measures are systematically and efficiently executed across national infrastructures. The plan's emphasis on risk management, as evidenced by the development of risk assessment methodologies and regular risk evaluation cycles, aligns with global best practices and ITU's recommendations, promoting a security culture that is both resilient and adaptable to evolving cyber threats [23], [24], [30].

Moreover, establishing programs for national cyber drills represents a significant strength of the NCSP 2022. These drills serve as practical exercises to test the effectiveness of existing cybersecurity protocols and the readiness of cybersecurity personnel to respond to incidents. Such initiatives enhance the skills and competencies of cybersecurity teams and foster a proactive stance towards cyber resilience, preparing the nation for potential cyber incidents through the simulation of real-world attack scenarios [23], [24].

Weaknesses. Despite these strengths, the NCSP 2022 presents areas requiring further development, particularly concerning budget allocation and formulating a national contingency plan for cybersecurity emergencies. The plan's documentation lacks specific details on the distribution of financial resources among various cybersecurity initiatives, raising questions about the adequacy and efficiency of funding in supporting the nation's cybersecurity objectives. Adequate budgeting is crucial for implementing effective cybersecurity measures, including procuring advanced technological tools, conducting training programs, and maintaining cybersecurity infrastructures [31], [34].

Furthermore, a detailed national contingency plan for cybersecurity emergencies must be developed. Such a plan is essential for outlining the procedures and responsibilities of different stakeholders in the event of a cyber incident, ensuring a coordinated and effective response. Developing a comprehensive contingency plan would enhance the nation's capability to manage and mitigate the impacts of cyber incidents, thereby reducing potential damages and recovery times. This gap underscores the need for a strategic approach to crisis management, incorporating lessons learned from past incidents and aligning with international standards for emergency response and recovery [31], [34].

The organizational structures pillar of the NCSP 2022 demonstrates the Philippines' commitment to establishing a robust framework for national cybersecurity efforts. However, identifying weaknesses in budget allocation and emergency planning highlights opportunities for strategic enhancements. Addressing these areas can further strengthen the nation's cybersecurity posture by ensuring the availability of necessary resources and the readiness to respond to cyber incidents effectively.

To overcome these challenges, it is recommended that future revisions of the NCSP include a more detailed financial plan that aligns with the strategic objectives of the cybersecurity initiatives. Additionally, developing a

comprehensive national contingency plan, incorporating international best practices, and tailoring it to the specific cybersecurity landscape of the Philippines would be a critical step forward. These enhancements will contribute to a more resilient and responsive organizational structure that is better equipped to safeguard the nation against cyber threats.

D. Capacity Building

Strengths. The NCSP 2022's strategic focus on capacity building through awareness, education, and cross-sector collaboration represents a pivotal alignment with the core tenets of globally recognized cybersecurity frameworks. The introduction of the Cybersecurity Outreach Project exemplifies a proactive commitment to raising public and organizational cybersecurity awareness. By engaging various stakeholders, including government entities, private sector organizations, and the general populace, this initiative seeks to broaden the understanding of cybersecurity risks and promote best practices across the board. Additionally, the plan's emphasis on research and development signifies an investment in the future of cybersecurity in the Philippines. Encouraging innovation through R&D initiatives supports the creation of advanced cybersecurity solutions, ultimately contributing to a robust national cybersecurity infrastructure [18], [19], [32].

These efforts underscore the NCSP 2022's recognition of the importance of cultivating a comprehensive cybersecurity culture, wherein awareness and education serve as the foundation for a resilient cybersecurity posture. The focus on fostering collaboration across different sectors further amplifies the plan's strength, leveraging diverse expertise and resources to address complex cybersecurity challenges.

Weaknesses. However, the evaluation of the NCSP 2022 reveals certain areas for improvement in the capacity-building domain, particularly regarding the incentivization of cybersecurity solution development and the allocation of financial resources and investments in cybersecurity initiatives. The absence of targeted incentives for developing and adopting innovative cybersecurity solutions highlights a gap in NCSP 2022's approach to encouraging technological advancement and solution-oriented research within the cybersecurity field [17], [33].

Moreover, the need for explicit provisions for financial and resource investments in capacity-building activities raises concerns about the sustainability and scalability of the initiatives outlined in the NCSP 2022. While the plan acknowledges the need for capacity building, the effectiveness of such initiatives is inherently tied to the availability of adequate funding and resources. Ensuring a consistent and targeted allocation of financial resources towards capacity-building initiatives is essential for achieving long-term goals and aligning with global best practices in cybersecurity education, training, and infrastructure development [17], [33].

The strengths of the NCSP 2022 in capacity building reflect a comprehensive understanding of the critical role that awareness, education, and collaboration play in enhancing national cybersecurity resilience. The initiatives undertaken, such as the Cybersecurity Outreach Project and a focus on research and development, are commendable steps toward building a knowledgeable and prepared cybersecurity workforce and community.

However, to fully realize these initiatives' potential and ensure alignment with international standards, the NCSP 2022 must address the identified areas for improvement. Implementing targeted incentives for cybersecurity innovation and ensuring adequate financial and resource investments in capacity-building efforts are crucial steps that can significantly enhance the effectiveness of the Philippines' cybersecurity strategy.

Enhancing the incentivization mechanisms for cybersecurity solution development could involve partnerships with academic institutions, private sector entities, and international organizations to foster an ecosystem conducive to innovation. Similarly, establishing clear budgetary commitments and exploring alternative funding mechanisms, such as public-private partnerships, could support sustained capacity-building efforts.

E. International Cooperation

Strengths. The NCSP 2022's approach to international cooperation represents a foundational pillar in its strategic framework, signifying the Philippines' recognition of cyber threats as a transnational challenge that necessitates global collaboration. This commitment is aligned with the ITU guidelines, which advocate for cross-border cooperation in cybersecurity efforts [25]. The NCSP 2022's initiatives in fostering public-private partnerships and its active role in international cybersecurity agreements are commendable efforts that position the Philippines as a proactive participant in the global cybersecurity ecosystem.

Such engagement leverages collective intelligence and resources and facilitates the integration of the Philippines into a more comprehensive network of cybersecurity knowledge and best practices. This alignment with successful strategies employed by other nations underscores the Philippines' dedication to a cohesive global response to cyber threats, enhancing its cyber defense capabilities while contributing to international cybersecurity resilience [29], [36]. The strategic importance of international cooperation in cybersecurity cannot be overstated, as it extends beyond mere information exchange to encompass collaborative actions against shared threats, capacity building, and the harmonization of cybersecurity standards and policies at the global level.

Weaknesses. Despite these strengths, the NCSP 2022 exhibits certain limitations in its emphasis on active participation in regional and international cybersecurity events. This relative underemphasis could hinder the Philippines' ability to leverage the benefits of international cybersecurity networks fully. Active and consistent participation in such events is crucial for staying abreast of the latest developments, emerging threats, and innovative cybersecurity solutions. It also serves as a platform for the Philippines to share its experiences, challenges, and successes, thereby contributing to and shaping the global cybersecurity discourse [40], [41].

The limited focus on engagement in regional and international forums may result in missed opportunities for the Philippines to assert its interests and perspectives on key cybersecurity issues, including policy coordination, cybercrime legislation harmonization, and the development of international cybersecurity norms. Enhanced engagement in these forums is essential for fostering stronger ties with other nations and international organizations, facilitating mutual support, and ensuring that the country is adequately represented in decisions that shape the global cybersecurity landscape.

The NCSP 2022 could benefit from a more strategic and concerted approach to increasing its presence and participation in global cybersecurity discussions and events to bolster its international cooperation efforts. This might

involve establishing dedicated programs or initiatives to send representatives to crucial international forums regularly and hosting international cybersecurity conferences and workshops in the Philippines. Such initiatives would elevate the Philippines' profile in the global arena and provide valuable opportunities for capacity building and establishing strategic partnerships.

Furthermore, enhancing mechanisms for public-private collaboration on international cybersecurity efforts can amplify the Philippines' influence and effectiveness in global cybersecurity initiatives. This includes fostering closer cooperation with multinational corporations, international cybersecurity organizations, and foreign governments to develop joint strategies, conduct collaborative research, and engage in defense mechanisms against cyber threats.

5 | CONCLUSION

The NCSP 2022 marks a significant advancement in the Philippines' cybersecurity infrastructure, especially in making a resilient and secure digital environment. This strategic blueprint acknowledges the nation's unique cybersecurity challenges and opportunities, shaped by its distinct priorities, cultural contexts, and institutional frameworks. By devising a tailored approach that resonates with the nation's specific conditions, the NCSP 2022 sets forth a holistic roadmap to strengthen the Philippines' cybersecurity capabilities, crucial to the country's overarching nation-building and development agenda.

When benchmarked against the ITU's GCA, the NCSP 2022 stands out as a comprehensive framework that delineates the Philippines' aspirations for cybersecurity capability and articulates strategic initiatives for the effective and optimal implementation of cybersecurity measures. This analysis, however, unveils pivotal areas requiring further enhancement, particularly highlighting the need for a dedicated cybersecurity law. Such a law would address gaps within the legal framework related to cybercrime, electronic commerce, intellectual property rights, data protection, and privacy concerns, strengthening the nation's cybersecurity posture.

Drawing inspiration from Singapore's exemplary performance in the GCI, which reflects its robust and committed approach to cybersecurity, the Philippines could benefit from benchmarking its efforts in legal reforms and across all facets of cybersecurity. This includes embracing technological advancements and fostering innovation to stay abreast of the ever-evolving global cybersecurity landscape.

Despite the areas identified for improvement, the NCSP 2022 adequately addresses the core needs of the national cybersecurity framework. However, the ultimate success of this strategic plan is contingent upon its effective execution and the collaborative engagement of all stakeholders involved. With a concerted effort and diligent implementation, the Philippines' aspiration to ascend in the GCI rankings to the 12th position appears within reach, signaling the potential to establish a safe, secure, and empowering cyberspace for government entities, businesses, and individuals alike.

As the NCSP 2022 is in its early stages of implementation, continuous monitoring and evaluation become paramount to gauge its impact comprehensively and identify critical success factors and areas for further refinement. This underscores the necessity for ongoing research efforts to assess the outcomes of the NCSP 2022 and explore the determinants of its effectiveness. Such scholarly endeavors will contribute valuable insights for improving the Philippines' cybersecurity strategy and enrich the global discourse on national cybersecurity planning and implementation.

In conclusion, the NCSP 2022 represents a critical milestone in the Philippines' commitment to enhancing its cybersecurity framework. By addressing the highlighted areas for improvement and leveraging international best practices, the Philippines can reinforce its cybersecurity defenses, paving the way for a more secure and resilient digital future.

ACKNOWLEDGMENT

We sincerely thank Prof. Serafin Talisayon, Ph.D., for his guidance throughout the study. Special thanks to Mr. El Jireh Bibangco, MSCS, for his valuable contributions to the methodology, results, and discussion sections.

REFERENCES

[1] ITU, "Measuring digital development: Facts & Figures 2019," *ITU Hub*, 2020. Available: https://www.itu.int/hub/2020/05/measuring-digital-development-facts-figures-2019/

[2] ITU, "Global Cybersecurity Index 2020," ITU Publications, 2020. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[3] R. Adel, "Filipinos were world's heaviest internet users in 2018, report says," Philstar, January 31, 2019. Available: https://www.philstar.com/business/technology/2019/01/31/1889736/filipinos-are-worlds-heaviest-internet-users-2018-report-says

[4] DICT, "National Cybersecurity Plan 2022," Department of Information and Communications Technology, 2017. [Online]. Available: https://dict.gov.ph/national-cybersecurity-plan-2022/

[5] Semantec, "ISTR Internet Security Threat Report," vol. 24, Symantec Corporation, February 2019. [Online]. Available: https://www.phishingbox.com/downloads/Symantec-Security-Internet-Threat-Report-ISRT-2019.pdf

[6] Verizon, "2019 Data Breach Investigations Report," 2019. Available: https://www.spambrella.com/wp-content/uploads/2020/05/Verizon-2019-Data-Breach-Investigations-Report.pdf

[7] Fortinet, "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," 2023. Available: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-2023-threat-landscape.pdf

[8] K. Bissel & L. Ponemon "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study – Unlocking the Value of Improved Cybersecurity Protection," MySecurity Marketplace. https://mysecuritymarketplace.com/reports/ninth-annual-cost-of-cybercrime-study/

[9] DICT, "Memorandum Circular No. 003 series of 2017 – National Cybersecurity Plan 2022," Department of Information and Communications Technology, 2017. Available: https://dict.gov.ph/national-cybersecurity-plan-2022/

[10] ITU, "Global Cybersecurity Agenda (GCA)," www.itu.int. Available: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

[11] A. Ntoko, "Global Cybersecurity Agenda (GCA) A framework for international cooperation." [Online]. Available: https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf

[12] C. Opris, "Cybercrime Evolution and Current Threats," 2022. [Online]. Available: https://www.ijisc.com/authors/cristian-opris/

[13] D. Dave, G. Sawhney, P. Aggarwal, N. Silswal, & D. Khut, "The New Frontier of Cybersecurity: Emerging Threats and Innovations," 2023. Available: https://dx.doi.org/10.1109/ICT60153.2023.10374044.

[14] R. Ramakrishnan, M. Leethial, & S. Monisha, "The Future of Cybersecurity and Its Potential Threats," International Journal for Research in Applied Science & Engineering Technology, vol. 11, issue 7, 2023. Available: https://dx.doi.org/10.22214/ijraset.2023.54603.

[15] S. Pandey & M. Kumar, "Cybersecurity Trends and Challenges," 2023. [Online]. Available: https://dx.doi.org/10.55041/ijsrem25323.

[16] A. Tsvetanova & M. Stefanova, "Key Cybersecurity Threats," Mathematics, Computer Science, and Education, vol. 5, issue 1, 2022. [Online]. Available: http://journals.uni-vt.bg/mcse/eng/vol5/iss1/art4.

[17] P. Kobetc, "Cyberterrorism as the most important threat to the national security of the Russian Federation and its main warnings," National Security and Strategic Planning, vol. 1, no. 37, 2022. [Online]. Available: https://futurepubl.ru/en/nauka/article/50622/view

[18] T.R. Shejin & K.T. Sudheer, "A Review on Major Cyber Threats and Recommended Counter Measures," 2023. [Online]. Available: https://doi.org/10.22214/ijraset.2023.49764

[19] A.S. Salsabila, M.D. Fikri, M.S. Andika, & N.A. Harahap, "Potential and Threat Analysis Towards Cybersecurity in South East Asia," Journal of ASEAN Dynamics and Beyond, vol. 1, no. 1, 2020. [Online]. Available: https://jurnal.uns.ac.id/adab/article/view/46794

[20] E. Tanriverdiyev, "The State of the Cyber Environment and National Cybersecurity Strategy in Developed Countries," Studia Bezpieczenstwa Narodowego National Security Studies, vol. 23, no. 1, 2022. [Online]. Available: https://dx.doi.org/10.37055/sbn/149510.

[21] H. Elkhannoubi & M. Belaïssaoui, "A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification," in IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2015. [Online]. Available: https://dx.doi.org/10.1109/ISDA.2015.7489156.

[22] S. Ghernouti-Hélie, "A National Strategy for an Effective Cybersecurity Approach and Culture," in 5th International Conference on Availability, Reliability, and Security, 2010. [Online]. Available: https://dx.doi.org/10.1109/ARES.2010.119.

[23] D. S. Smith, "Securing Cyberspace: Approaches to Developing an Effective Cyber-Security Strategy," 2011. [Online]. Available: https://apps.dtic.mil/sti/tr/pdf/ADA565052.pdf

[24] S. J. Shackelford, "Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk," 2015. [Online]. Available: https://digitalcommons.chapman.edu/cgi/viewcontent.cgi?article=1376&context=chapman-law-review

[25] O. Poliakov, "Activation of international cooperation in the field of cybersecurity: the ways of improvement in today's realities," 2021. [Online]. Available: https://dx.doi.org/10.37750/2616-6798.2021.2(37).238348.

[26] D. Štitilis, P. Pakutinskas, & I. Malinauskaite, "EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis," Journal of Information Technology & Politics, 2017. [Online]. Available: https://dx.doi.org/10.1057/s41284-016-0083-9.

[27] A. Pamela, H. Fabe, & E. Zarcilla-Genecela, "The Philippines' Cybersecurity Strategy: Strengthening partnerships to enhance cybersecurity capability," Routledge Companion to Global Cyber-Security Strategy, 2021. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-29/philippines-cybersecurity-strategy-amparo-pamela-fabe-ella-zarcilla-genecela.

[28] I. S. Simbolon, "Inisiatif Siber dalam Konteks Keamanan Siber di Filipina," 2017. [Online]. Available: https://jurnalprodi.idu.ac.id/index.php/PA/article/view/99.

[29] C. H. Godoy, N. J. R. Diego, R. E. Tagumasi, J. C. Lerit, & J. A. Costales, "Cybersecurity Scientometric Analysis: Mapping of Scientific Articles using Scopus API for Data Mining and Webscrapping," 2022. [Online]. Available: https://dx.doi.org/10.1109/DSIT55514.2022.9943876.

[30] H. Tecklenburg & J. da Cruz, "The Nationalization of Cybersecurity: The Potential Effects of the Cyberspace Solarium Commission Report on the Nation's Critical Infrastructure," 2023. [Online]. Available: https://www.usmcu.edu/Portals/218/JAMS%2014_1_Spring2023_da%20cruz.pdf.

[31] J. Burton & G. Christou, "Bridging the gap between cyberwar and cyberpeace," International Affairs, vol. 97, issue 6, 2021. [Online]. Available: https://dx.doi.org/10.1093/ia/iiab172.

[32] T. V. Benzel, "Cybersecurity research for the future," Communications of the ACM, vol. 64, no. 1, 2020. [Online]. Available: https://dx.doi.org/10.1145/3436241.

[33] L. I. Millett, B. Fischhoff, & P. Weinberger, "Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions," Consensus Study Report, 2017. [Online]. Available: https://dx.doi.org/10.17226/24676.

[34] F. Chang, "Hacked but Don't Know It: Confronting the Cybersecurity Challenge," Kentucky Scholarship Online, 2020. [Online]. Available: https://dx.doi.org/10.5810/KENTUCKY/9780813179001.003.0013.

[35] W. Maconachy & D. Kinsey, "Cybersecurity Education: A Mandate to Update," The Journal of The Colloquium for Information Systems Security Education, vol. 9, no. 1, 2022. [Online]. Available: https://dx.doi.org/10.53735/cisse.v9i1.138.

[36] D. McMarrow, "Science of Cyber-Security," The George Washinton University, 2010. [Online]. Available: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-039.pdf.

[37] J.M. Chang, D.R. Kuhn, & T.R. Weil, "Cyberthreats and Security," IEEE IT Professional, vol. 20, no. 3, pp. 6-10, 2018. [Online]. Available: https://dx.doi.org/10.1109/MITP.2018.032501744.

[38] Y. Ivanova, "A methodology for empirical research and analysis in cybersecurity," Yearbook of the Telecommunications, vol. 22, no. 9, pp. 56-64, December 2022. [Online]. Available: https://dx.doi.org/10.33919/ytelecomm.22.9.4.

[39] S. Bordoff, Q. Chen, & Z. Yan, "Cyber Attacks, Contributing Factors, and Tackling Strategies: The Current Status of the Science of Cybersecurity," International Journal of Cyber Behavior, Psychology and Learning, vol. 7, no. 4, pp. 79-93, October 2017. [Online]. Available: https://dx.doi.org/10.4018/IJCBPL.2017100106.

[40] S. Nasir, "Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions," Proceedings of the Conference on Security and Management (SAM), pp. 1-6, July 2023. [Online]. Available: https://dx.doi.org/10.22624/aims/csean-smart2023p18.

[41] A. Hewaidy & A. Al Mutawaa, "Disclosure level and compliance with IFRSs: an empirical investigation of Kuwaiti companies," International Business & Economics Research Journal, vol. 9, no. 5, 2010. [Online]. Available: https://clutejournals.com/index.php/IBER/article/view/566.