



Comparative analysis of National Cyber Security Index: A case study of Pakistan and Indonesia

Anwar Sadat^{a,*}, Herman Lawelai^a, Muhammad Younus^{b,c}, Achmad Nurmandi^b

^a Department of Government Studies, Universitas Muhammadiyah Buton, Sulawesi Tenggara 93724, Indonesia

^b Department of Government Affairs and Administration, University of Muhammadiyah Yogyakarta, Yogyakarta 55183, Indonesia

^c Department of Product Research and Software Development, TPL Logistics Pvt Ltd, Karachi 75700, Pakistan

Article Info

Article history:

Received 30 January 2024

Revised 3 March 2024

Accepted 18 March 2024

Available online 25 March 2025

Keywords:

comparative,
cyber security index,
cyber space,
cyber security policy,
internet

Abstract

This research study compares the National Cyber Security Index (NCSI) for Pakistan and Indonesia, two developing countries with fast-expanding digital landscapes. This study attempts to uncover the strengths and weaknesses of each country's cyber security posture and provide insights into potential areas for improvement by studying the NCSI scores and underlying indicators. This study's approach includes a detailed assessment of NCSI data, as well as related literature and policy papers. The study considers both countries' socioeconomic and political settings to understand better the elements driving their cyber security performance. Based on the comparative analysis, this study presents recommendations for both countries to better their cyber security postures. Among them are enhancing legal frameworks, investing in technical infrastructure, encouraging capacity-building efforts, and increasing regional and international cooperation. By implementing these measures, Pakistan and Indonesia can better protect their digital assets and contribute to more secure global cyberspace.

© 2025 Kasetsart University.

Introduction

Rapid advancements in information and communication technology (ICT) have transformed the world into a global village where individuals, businesses, and governments are interconnected via digital networks. (Veena et al., 2022, p. 1) The invention of smart low-power devices and ubiquitous Internet connectivity have facilitated the shift of many labour-intensive jobs

into the digital domain. (Alahmadi et al., 2022, p. 1) This connectivity has resulted in numerous advantages, including enhanced communication, greater access to information, and increased economic growth (Mishra et al., 2022, p. 26). Nonetheless, it has exposed nations to cyber threats, which can severely affect national security, economic stability, and social well-being. In order to protect their critical infrastructure, sensitive data, and citizens from cyber attacks, nations worldwide

* Corresponding author.

E-mail address: anwarsadat685@gmail.com (Sadat, A.).

<https://doi.org/10.34044/j.kjss.2025.46.1.01>

2452–3151/© 2025 Kasetsart University.

are concentrating more and more on enhancing their cyber security capabilities (Bilen & Özer, 2021a, p. 1). Cyber risk encompasses a broad spectrum of risks to digital systems, such as data breaches or full-fledged cyber attacks on the electric grid (Falco et al., 2019, p. 1).

The National Cyber Security Index (NCSI) is a comprehensive framework that evaluates nations' cyber security posture based on various indicators, including legal, technical, and organizational measures, capacity development, and international cooperation (Kumar et al., 2022, p. 12). The NCSI provides policymakers, researchers, and other stakeholders with a valuable resource for evaluating the efficacy of national cybersecurity strategies, identifying areas for development, and fostering international collaboration (Hijji & Alam, 2022, p. 18). In this context, the present study seeks to conduct a comparative analysis of the NCSI in Pakistan and Indonesia, two emerging economies in the Asia-Pacific region (Attatfa et al., 2020, p. 61). Due to their strategic significance, increasing digitalization, and shared challenges in the cyber domain, these nations have been selected for the case study. In recent years, Pakistan, a South Asian nation with a population of over 220 million, has experienced a rapid expansion of its ICT infrastructure and internet penetration (Alqahtani, 2022, p. 3). By 2025, the country's digital economy is projected to contribute substantially to its overall GDP, reaching \$36 billion. Cyberespionage, cyber terrorism, and cybercrime threaten Pakistan's national security and economic development (Tubis et al., 2020, p. 19). In response, the government has undertaken several initiatives to strengthen its cyber security capabilities, including establishing a National Cyber Security Policy, establishing a dedicated cyber security agency, and implementing several capacity-building programs (Škiljić, 2020, p. 59).

Indonesia, the largest economy in Southeast Asia, has also seen increased internet usage and digital services, with over 170 million internet users and a swiftly expanding e-commerce sector. The nation's digital economy is expected to reach \$124 billion by 2025, making it one of the region's fastest-growing markets (Venkatachary et al., 2021, p. 1).

Nonetheless, Indonesia has been confronted with a variety of cyber threats, such as cyber warfare, cybercrime, and cyber radicalization, that have the potential to undermine its national security, social harmony, and economic prosperity. The Indonesian government has adopted a National Cyber Security Strategy, established a National Cyber and Crypto Agency, and launched several capacity-building

initiatives to address these issues. The comparative analysis of the NCSI for Pakistan and Indonesia will be conducted using a mixed-methods approach that incorporates quantitative and qualitative data to provide a comprehensive understanding of the cyber security performance of the countries (Alamri et al., 2022, p. 25). The quantitative analysis will include collecting and comparing NCSI scores and rankings for both nations and examining individual indicators to determine their cyber security strengths and vulnerabilities (Burke & Saxena, 2021, p. 1).

The qualitative analysis will review pertinent policy documents, academic literature, and expert opinions to understand the contextual factors influencing individual nations' cyber security capabilities and challenges (Luo et al., 2022, p. 2). This study will contribute to the existing corpus of knowledge on national cyber security by comparing the performance of Pakistan and Indonesia in the National Cyber Security Initiative (NCSI). The study will also provide policymakers, practitioners, and researchers in both nations with valuable insights to inform the development and implementation of more effective cybersecurity strategies and measures (Kotenko et al., 2023, p. 4). In addition, the study will facilitate international cooperation and knowledge sharing among countries in the Asia-Pacific region and beyond as they endeavor to create a more secure and resilient cyberspace for everyone. Given the growing significance of cyber security in the digital age, the comparative analysis of the National Cyber Security Index for Pakistan and Indonesia is a timely and pertinent research endeavor. By analyzing the cyber security posture of these two emerging economies, the study will cast light on their strengths and weaknesses and provide valuable lessons for other nations in the region and worldwide. The findings of this study will ultimately contribute to the global endeavor to improve cyber security and promote safer and more secure cyberspace for everyone (Sarker et al., 2019, p. 1).

Literature Review

Comparative analysis of national cyber security indexes has become an increasingly vital area of study as nations endeavor to improve their cyber security capabilities and safeguard their critical infrastructure (Savaş & Karataş, 2022, p. 15). Humans built cyberspace to enhance communication and link the world's interconnected infrastructures. It enabled more than half of the world's population to share data via

a networked system (Krause et al., 2021, p. 13). The increasing threat in cyberspace created new concerns for civilisations throughout the world, with the ability to compromise people's security. This literature review will concentrate on the case studies of Pakistan and Indonesia, investigating the existing literature on their respective cyber security indices and comparing their strengths and weaknesses (Kim et al., 2023, p. 17).

The National Cyber Security Index (NCSI) is a global initiative designed to assess and compare the cyber security capabilities of nations. The NCSI is based on a comprehensive set of indicators categorized into three primary groups: legal, technical, and organizational (Krishna et al., 2021, p. 1713). As the importance of the digital economy grows, so does the demand for cybersecurity. The presence of cyber dangers is unavoidable as technology advances. Cybersecurity is becoming increasingly important as cyber domination grows. National-level policies are being established to offer the essential foundation and infrastructure to safeguard cyberspace, allowing governments to capitalise on and progress the digital economy. Cybersecurity is a critical component of national security (Ullah et al., 2022, p. 17). Researchers and policymakers have utilized the index extensively to evaluate the efficacy of national cybersecurity strategies and identify areas for improvement (Venter et al., 2019, p. 1).

Several studies have examined Pakistan's cyber security landscape and its position in the NCSI in the context of Pakistan conducting an exhaustive analysis of Pakistan's cyber security capabilities, highlighting the nation's progress in implementing legal and organizational measures. Nonetheless, the study identified several obstacles, such as the absence of a centralized cyber security agency and inadequate technical measures to safeguard critical infrastructure (Abbas et al., 2022, p. 1).

Using the NCSI framework, several studies evaluated Pakistan's cyber security posture. They determined that the country has made significant strides in recent years, especially in cybercrime legislation and establishing a national Computer Emergency Response Team (CERT). However, the authors also noted that Pakistan's aggregate NCSI ranking remains relatively low, indicating that Pakistan's cyber security capabilities require further enhancement. (Gamec et al., 2021, p. 1) The use of such systems gives a positive economic effect and provides additional benefits from various points of view. At the same time, due to a large number of threats and challenges to cyber security, it is necessary to detect attacks on sensor systems in a timely manner. Cybersecurity indices evaluate information security and

defence against attacks. Global cybersecurity indices examine and rate nations based on their governmental institutions' activity. There are four global cybersecurity indices: the Digital Economy and Society Index (DESI), the Global Cybersecurity Index (GCI), the National Cybersecurity Index (NCSI), and the National Cyber Power Index (Lallie et al., 2021, p. 1).

Several studies have examined Indonesia's cyber security landscape and its position within the NCSI. In comparing Indonesia's cyber security capabilities with those of other ASEAN nations, it was found that Indonesia ranked in the middle of the pack regarding its NCSI score. The study underscored the need for Indonesia to invest in developing its technical capabilities and strengthen its legal and organizational measures. (Rubasundram & Rasiah, 2019, p. 1).

Using the NCSI as a benchmark, Yuliana and Hasibuan (2022) the current best practice of information security governance in the Indonesian national government is still inadequate according to various related studies still siloed and scattered and leading to vulnerabilities in the various digital services provided. Therefore, this study aims to develop a best practice framework for managing information security that is aligned with the needs of Indonesia's digital government. This research started by looking for the main framework of information security governance. Then the main components that resulted from that were benchmarked with other Information Security Governance (ISG examined the challenges and opportunities for Indonesia in enhancing its cyber security capabilities. The authors identified several enhancement areas, including a more comprehensive legal framework, establishing a national cyber security agency, and developing a robust cyber security workforce (Yuliana & Hasibuan, 2022, p. 4).

Comparative investigations of the cyber security indexes of Pakistan and Indonesia are uncommon in the existing literature. A few studies, however, have attempted to compare the cyber security capabilities of these two nations (Elmaghraby & Losavio, 2014, p. 1). Comparing cyber security in South and Southeast Asia, including Pakistan and Indonesia, according to the study, both nations confront similar challenges regarding their cyber security capabilities, such as the need for more robust legal frameworks and more effective organizational measures.

Using the NCSI framework, Ahmad et al. (2021, p. 1) compared the cyber security capabilities of Pakistan and Indonesia, concluding that both countries have made progress in recent years but still face significant challenges in their cyber security posture.

According to the authors, both nations could benefit from increased regional cooperation and knowledge sharing to enhance their cyber security capabilities.

In summary, the existing literature on the comparative analysis of national cyber security indexes, particularly in the context of Pakistan and Indonesia, emphasizes the significance of legal, technical, and organizational measures for enhancing a nation's cyber security capabilities. Despite the fact that both nations have made progress over the past few years, there is still room for development in their overall cybersecurity posture. Future research could identify best practices and lessons learned from other nations to inform the creation of more effective cyber security strategies for Pakistan and Indonesia.

According to Figure 1, the average release of cybersecurity policies between 2014 and 2023 has shown a rising trend since 2017, peaking in 2022. However, there was a decline in publications in 2023. This shift can be attributed to the pressing cybersecurity concerns in Indonesia and Pakistan, where cybercrime has escalated to concerning levels, prompting urgent action in the realm of cybersecurity policy.

Methodology

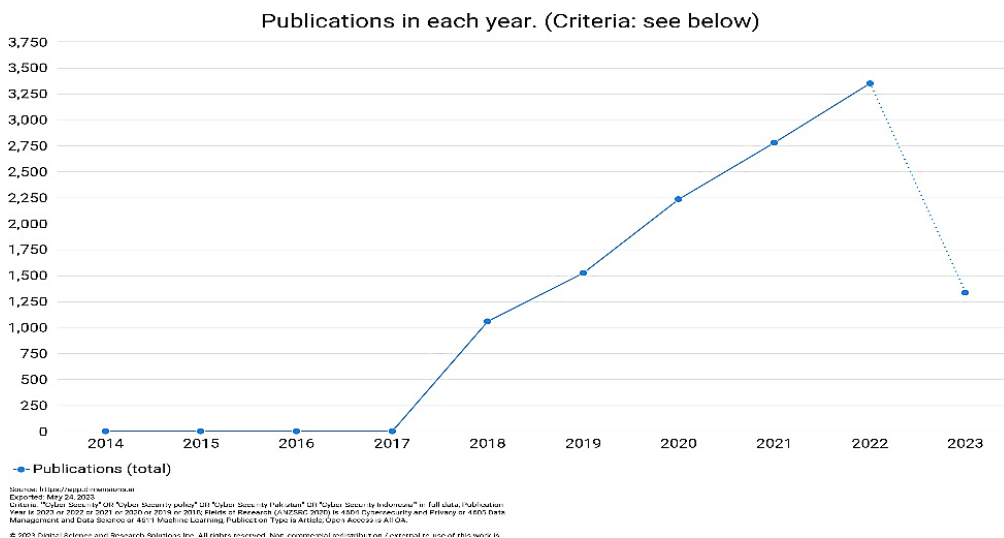
This article provides a comparative analysis of Pakistan and Indonesia's National Cyber Security Index (NCSI). It aims to evaluate and compare these two nations' cyber security capabilities and preparedness by

analyzing the NCSI framework's numerous indicators. Following is a description of the methodology used to conduct this comparative analysis.

The gathered data were analyzed using a comparative methodology. Each selected indicator was evaluated independently for each nation, and the results were compared to determine similarities, differences, strengths, and weaknesses. Statistical methods, such as descriptive analysis and comparative ranking, were applied to the data to extract meaningful insights.

Comparative research is a powerful tool for understanding the differences and similarities between different groups, variables, or situations. This paper examines the cybersecurity frameworks of Pakistan and Indonesia using comparative research approaches to get vital insights into their strengths and limitations. The study examines crucial variables such as legislative measures, institutional capabilities, public-private partnerships, and international collaboration. These aspects play an important role in determining each country's ability to successfully confront cyber threats, suggesting areas for development that can boost overall cyber resilience (Wylde et al., 2022, p. 6).

For this research, data were collected from the e-Governance Academy Foundation held and developed NCSI, a reliable and authoritative source. The data used for the analysis encompass a vast array of variables, including legal frameworks, institutional arrangements, technical measures, initiatives for capacity development, and international cooperation in the field of cyber security.



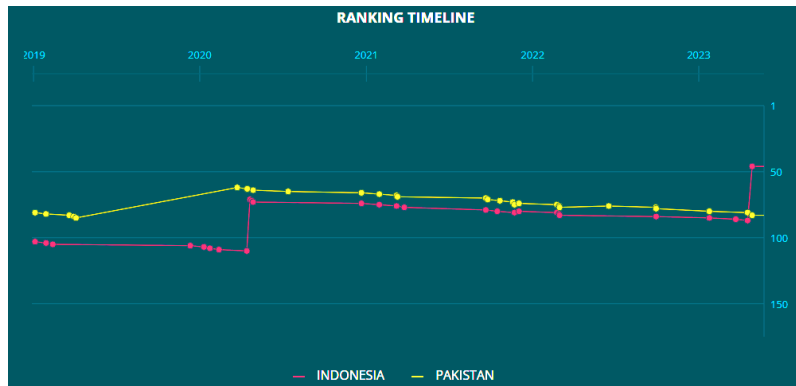


Figure 2 Ranking timeline

A subset of the numerous indicators included in the NCSI framework was selected for comparison between Pakistan and Indonesia. Relevance, availability of data, and the ability to capture the fundamental aspects of cyber security preparedness in each country served as the selection criteria. The selected indicators include legal and policy frameworks, incident response capabilities, public-private partnerships, and international cooperation.

Results

Based on the extensive research and analysis conducted on this topic, the discovered outcomes will be discussed in detail in the section listed below;

Comparing National Cyber Security Index

National Cyber Security Index (NCSI) is a global index which gauges a country's readiness to prevent cyber threats and manage cyber incidents. It is created and maintained by the e-Governance Academy Foundation, a non-profit organization in Estonia. The NCSI is comprised of twelve primary categories and forty-six subcategories. The index is routinely updated, and the scores are derived from publicly available data.

Challenges

Figure 3 depicts the National Cyber Security Index Scores of Pakistan and Indonesia, which were analyzed carefully. The following are some of the most important factors underlying the trend of the countries' scores;

- Both nations have limited financial and human resources devoted to cyber security, impeding their ability to develop and implement comprehensive cyber security strategies.
- In both nations' public and private sectors, there is a general dearth of awareness regarding cyber security risks and best practices.
- Inadequate legal frameworks: Both nations have cyber security laws and regulations, but they may not be comprehensive enough to address the ever-changing cyber threat landscape.
- Both nations could benefit from increased international cooperation and information exchange to combat cyber threats more effectively.

Improvements

Both Pakistan and Indonesia can strengthen their overall cyber security posture by taking the following steps:

Rank	Country	National Cyber Security Index	Digital development	Difference
47.	Indonesia	63.64	47.41	16.23
83.	Pakistan	42.86	32.23	10.63

Figure 3 NCSI Score of Pakistan and Indonesia

- Allocate additional funds to cyber security initiatives, including infrastructure, training, and research.
- Encourage government, private sector, and academic collaboration in developing and implementing effective cybersecurity strategies.
- Existing cyber security laws and regulations should be reviewed and updated to ensure they are comprehensive and current.
- Implement awareness campaigns and training programs at the national level to educate the public and private sectors on cyber security risks and best practices.

Discussion

Comparing National Cyber Security Index Indicators

Comparing cyber security policy development indicator

This indicator evaluates whether a country has a national cyber security strategy, policy, and legal framework, as well as the quality of those elements.

Challenges

Figure 4 depicts the Cyber Security Policy Development Scores of Pakistan and Indonesia, which were analyzed carefully. The following are some of the most important factors underlying the trend of the countries' scores;

- Implementation: Despite a policy, the NCSP's implementation has been sluggish, and many of the program's goals have not been fully accomplished.
- The legal framework: Pakistan's legislative framework for cyber security is still developing, and there are holes in both the legislation and its enforcement.

- Strengthening the legal framework: For improved cyber security, updating it and ensuring its effective enforcement is essential.

- Conducting awareness campaigns and promoting cyber security education can contribute to developing a more secure digital environment.

Improvements

- Strengthening Pakistan's legal framework must be updated to address emergent cyber threats and ensure effective enforcement.

- Capacity building: Investing in education and training programs is essential to cultivate a competent cybersecurity workforce.

- Strengthening the legal framework: For improved cyber security, updating it and ensuring its effective enforcement is essential.

- Conducting awareness campaigns and promoting cyber security education can contribute to developing a more secure digital environment.

Comparing educational and professional development indicators

This indicator evaluates the quantity of cybersecurity education and training programs available in a country and the quality of those programs.

Challenges

Figure 5 Depicts the Educational and Professional Development Scores of Pakistan and Indonesia, which were analyzed carefully. The following are some of the most important factors underlying the trend of the countries' scores;

- Few institutions offer cybersecurity training programs.
- Lack of public awareness regarding the significance of cybersecurity education.



Figure 4 Cyber security policy development score of Pakistan and Indonesia

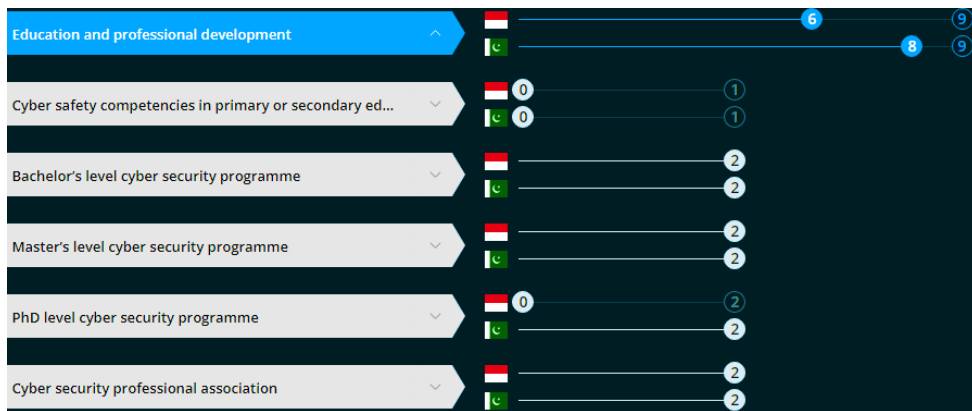


Figure 5 Educational and professional development score of Pakistan and Indonesia

- Few advanced cybersecurity courses and training programs are available.
- To develop pertinent curricula and training programs, there is insufficient collaboration between academia, industry, and government.
- Few qualified cybersecurity professionals can teach and train the next generation.

Improvements

- Enhance the quality of extant programs and expand the number of institutions offering cybersecurity programs.
- Promote the significance of cybersecurity education by launching awareness campaigns.
- Create advanced cybersecurity courses and training programs to meet the industry's evolving requirements.
- Encourage collaboration between academia, industry, and the government to develop relevant curriculum and training programs.
- Offer incentives to recruit qualified cybersecurity instructors and trainers for the next generation.

Comparing protection of digital services indicator

Digital security is the resources employed to safeguard your online identity, data, and other assets. These tools

include web services, antivirus software, smartphone SIM cards, biometrics, and personal devices with security features.

Challenges

Figure 6 depicts the Protection of Digital Services Scores of Pakistan and Indonesia, which were analyzed carefully. The following are some of the most important factors underlying the trend of the countries' scores;

- The legal framework protecting digital services is inadequate.
- Implementation of insufficient security measures for vital information infrastructure.
- Lack of public education and awareness regarding cyber security best practices.
- Low public education and awareness regarding cyber security best practices.
- Insufficient resources and expertise in cyber security.

Improvements

- Create and implement a comprehensive legal framework to safeguard digital services.
- Implement international standards and best practices to bolster the security of the critical information infrastructure.

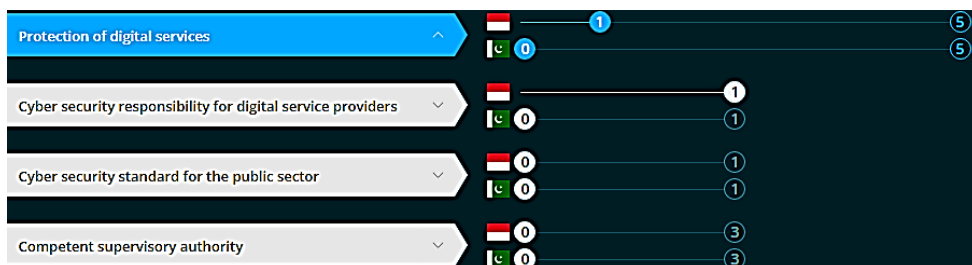


Figure 6 Protection of digital services score of Pakistan and Indonesia

- Increase public cyber security awareness and education through campaigns and training.
- Increase public cyber security awareness and education through campaigns and training.
- Invest in the development of indigenous expertise and resources in cyber security.

Comparing the protection of personal data indicator

Personal data protection is essential to cybersecurity and involves preventing unauthorized access, use, or disclosure of an individual's personal information. It typically includes data privacy, data security, and legal frameworks regulating personal data collection, storage, and processing.

Challenges

Figure 7 depicts the Protection of Personal Data Scores of Pakistan and Indonesia, which were analyzed carefully. The following are some of the most important factors underlying the trend of the countries' scores;

- **Inadequate Legal Framework:** Pakistan's legal framework for data protection presented obstacles. During the NCSI evaluation, Pakistan lacked comprehensive data protection laws. This lack of comprehensive legal provisions contributed to the vulnerability of personal data protection.
- **Data Privacy Awareness:** Indonesia confronted obstacles to individuals' and organizations' data privacy awareness. Few individuals understood their rights and the significance of protecting personal data. This ignorance contributed to security vulnerabilities and data breaches.
- **Regulatory Framework Deficits:** Indonesia's regulatory framework for data protection presented obstacles. While there were data protection laws in the country, there were voids and inconsistencies in their implementation and enforcement. This circumstance resulted in inadequate protection of personal information.

Improvements

- Pakistan enacted data protection legislation after recognizing the need for an all-encompassing data

protection framework. Pakistan has addressed this issue since the NCSI 2020 assessment by passing the Personal Data Protection Bill in 2020. This legislation seeks to protect personal information and expand privacy rights.

- Pakistan has taken measures to strengthen its institutional capacity for data protection. The Pakistan Personal Data Protection Authority's (PPDPA) establishment in 2020 is a positive development. The PPDPA is responsible for regulating and enforcing the country's data protection laws, thereby enhancing personal data protection.

- Indonesia has taken measures to strengthen its data protection legislation. The Personal Data Protection Bill was enacted in 2020 to provide a more comprehensive legal framework for data protection. The bill contains provisions on consent, data transfer, and data subject rights.

Comparing cyber incidents response indicator

A cyber incident response plan is a document that details an organization's actions in the event of a data breach or other type of security incident. Given the growing threat of cybercrime, these strategies are essential to an organization's information security and business continuity measures.

Challenges

Figure 8 depicts the Cyber Incidents Response Scores of Pakistan and Indonesia, which were analyzed carefully. The following are some of the most important factors underlying the trend of the countries' scores;

- **Limited Coordination:** Limited coordination among cyber incident response stakeholders is one of Pakistan's most significant challenges. This dearth of collaboration hinders the efficiency and promptness of cyber incident response.
- Pakistan confronts difficulties establishing a comprehensive legal framework for cyber incident response. The response process and investigations can be hampered without defined laws and regulations regarding cyber incidents.



Figure 7 Protection of personal data score of Pakistan and Indonesia

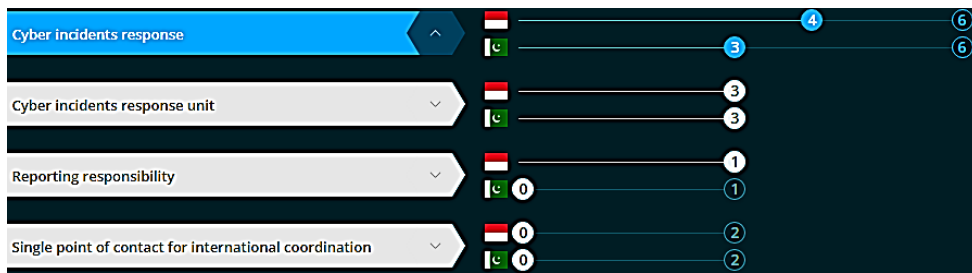


Figure 8 Cyber incidents response score of Pakistan and Indonesia

- **Fragmented Response System:** Indonesia confronts difficulties due to a fragmented cyber incident response system. Inefficiency and delays in responding to cyber incidents may result from the absence of a centralized coordination mechanism and defined roles and responsibilities among relevant agencies.

- **Capacity Development:** Like Pakistan, Indonesia confronts a dearth of qualified cybersecurity professionals. Enhancing the capacity and expertise of extant response teams and fostering collaboration between the public and private sectors is essential for effective incident response.

- **Public Awareness:** Limited public awareness of cybersecurity and cyber incident reporting impedes timely identification and response. Raising awareness among individuals and institutions is essential for a proactive and effective response.

Improvements

- **Pakistan** can focus on enhancing coordination among various stakeholders, such as government agencies, law enforcement agencies, and private sector organizations. Establishing dedicated cyber response teams and facilitating information sharing can enhance incident response capabilities.

- **Skill Development:** Investing in cybersecurity education and training programs should close the skills disparity. Collaboration with academia, industry, and

international partners can facilitate the development of a skilled workforce capable of effectively managing cyber incidents.

- **Capacity Enhancement:** Investing in cybersecurity education, training programs, and professional certifications can assist in addressing the skills gap. Government, academia, and industry can collaborate to foster the development of a competent cybersecurity workforce.

- **Public Awareness Campaigns:** Indonesia can initiate public awareness campaigns to educate individuals and organizations on the significance of cybersecurity, safe online practices, and reporting cyber incidents. This can cultivate a culture of proactive incident reporting and bolster response efforts overall.

Comparing fight against cybercrime indicator

Cybercrime incidents frequently result in the seizure of personal information or the interruption of customer service, which in many countries may constitute a crime or lead to regulatory actions.

Challenges

Figure 9 depicts the Fight Against Cybercrime Scores of Pakistan and Indonesia, which were analyzed carefully. The following are some of the most important factors underlying the trend of the countries' scores;



Figure 9 Fight against cybercrime score of Pakistan and Indonesia

- Pakistan confronts difficulties in enacting comprehensive cybercrime legislation and enforcing it effectively. There is a need for more robust legal frameworks to combat cybercrimes and strengthen law enforcement capacities.

- Awareness and Capacity Building: The general public and organizations lack awareness regarding cybercrime and cybersecurity. Inadequate funding for capacity-building programs impedes the development of qualified cybersecurity professionals.

- Legislation and Law Enforcement: Indonesia confronts challenges in enacting effective legislation to keep up with rapidly evolving cyber threats. The nation must strengthen its legal framework to address emergent cybercrime trends adequately.

- Public-Private Collaboration: There is a need for enhanced collaboration between the public and private sectors in sharing information, coordinating incident response, and implementing cybersecurity measures.

Improvements

- Legal Reforms: Pakistan should prioritize the enactment and implementation of comprehensive cybercrime legislation covering a broad range of cyber offenses, including hacking, identity theft, and data breaches.

- Capacity Development: Investments should be made in cybersecurity education and training programs to improve the skills and knowledge of professionals. Public awareness campaigns can inform individuals of cyber threats and preventative measures.

- Pakistan should establish strong partnerships with international organizations, neighboring nations, and industry stakeholders to share information, best practices, and expertise in combating cybercrime.

- Legal Framework: Indonesia should review and update its cybercrime regulations to address current and emerging threats effectively. The legislation should encompass a variety of cybercrimes, such as financial fraud, identity theft, and data intrusions.

Establishing robust partnerships between government agencies, organizations in the private sector, and civil society is crucial. These alliances can facilitate information sharing, collaborative research, and coordinated efforts to combat cybercrime.

Conclusion

In conclusion, this study compares and contrasts Pakistan's and Indonesia's National Cyber Security Indices.

The report sheds light on different nations' difficulties in safeguarding their respective online spaces. According to the findings of the research, Indonesia has a higher national cyber security index ranking than Pakistan does at the current time. An examination of Indonesia's information security index reveals that the nation as a whole has made great strides toward enhancing the cyber security architecture of its institutions, most notably its public universities. In addition, the study stresses the need for composite indicators to quantify catastrophe risk, vulnerability, and resilience.

Recommendation

According to the study's findings, data availability is one of the most critical challenges in developing sub-national indices. According to the Global Trends research findings, protecting national security will not just involve fighting against armies and arsenals; it will also demand defending against the competition for political influence, governance models, technological preeminence, and strategic advantage. The likelihood of a significant conflict occurring is low because international collaboration and the development of new technologies make it possible for the world to be self-sufficient, resilient, and defend itself. In general, this study sheds light on the current level of cyber security in Pakistan and Indonesia. Additionally, it stresses the necessity of continuing efforts to improve cyber security infrastructure and establish efficient composite indicators for measuring cyber security.

Conflict of Interest

The authors declare that there is no conflict of interest.

Acknowledgments

The research work of this article was supported by Achmad Nurmandi from the University of Muhammadiyah Yogyakarta. The researcher would like to express his immense gratitude to his supporters who have provided all necessary insight and expertise for assistance in this research.

References

- Abbas, M. W., Hussain, M., Akhtar, S., Ismail, T., Qamar, M., Shafiq, Z., & Esatbeyoglu, T. (2024). Bioactive compounds, antioxidant, anti-inflammatory, anti-cancer, and toxicity assessment of *Tribulus terrestris*—In Vitro and In Vivo studies. *Antioxidants*, (2022), 11, 1160. <https://doi.org/10.3390/antiox13040471>
- Ahmad, M. O., Ahad, M. A., Alam, M. A., Siddiqui, F., & Casalino, G. (2021). Cyber-physical systems and smart cities in india: Opportunities, issues, and challenges. *Sensors*, 21(22). <https://doi.org/10.3390/s21227714>
- Alahmadi, A. N., Rehman, S. U., Alhazmi, H. S., Glynn, D. G., Shoaib, H., & Solé, P. (2022). Cyber-security threats and side-channel attacks for digital agriculture. *Sensors (Basel, Switzerland)*, 22(9), 3520. <https://doi.org/10.3390/s22093520>
- Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity risk management framework for blockchain identity management systems in health IoT. *Sensors (Basel, Switzerland)*, 23(1), 218. <https://doi.org/10.3390/s23010218>
- Alqahtani, M. A. (2022). Cybersecurity awareness based on software and e-mail security with statistical analysis. *Computational Intelligence and Neuroscience*, 2022, 6775980. <https://doi.org/10.1155/2022/6775980>
- Attatfa, A., Renaud, K., & Paoli, S. De. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science*, 176, 60–69. <https://doi.org/10.1016/j.procs.2020.08.007>
- Bilen, A., & Özer, A. B. (2021). Cyber-attack method and perpetrator prediction using machine learning algorithms. *PeerJ Computer Science*, 7, e475. <https://doi.org/10.7717/peerj-cs.475>
- Burke, G., & Saxena, N. (2021). Cyber risks prediction and analysis in medical emergency Equipment for Situational Awareness. *Sensors (Basel, Switzerland)*, 21(16), 5325. <https://doi.org/10.3390/s21165325>
- Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491–497. <https://doi.org/10.1016/j.jare.2014.02.006>
- Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Disciplinary barriers impede cyber risk research. *Science*, 366(6469), 1066–1069. <https://doi.org/10.1126/science.aaz4795>
- Gamec, J., Basan, E., Basan, A., Nekrasov, A., Fidge, C., & Sushkin, N. (2021). An adaptive protection system for sensor networks based on analysis of neighboring nodes. *Sensors (Basel, Switzerland)*, 21(18), 6116. <https://doi.org/10.3390/s21186116>
- Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for remote working employees. *Sensors (Basel, Switzerland)*, 22(22), 8663. <https://doi.org/10.3390/s22228663>
- Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey. *Sensors*, 23(7), 3681. <https://doi.org/10.3390/s23073681>
- Kotenko, I., Fedorchenko, E., Novikova, E., & Jha, A. (2023). Cyber attacker profiling for risk analysis based on machine learning. *Sensors (Basel, Switzerland)*, 23(4), 2028. <https://doi.org/10.3390/s23042028>
- Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: challenges and opportunities. *Sensors (Basel, Switzerland)*, 21(18), 6225. <https://doi.org/10.3390/s21186225>
- Krishna, B., Krishnan, S., & Sebastian, M. P. (2021). Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective. *Information Systems Frontiers*, 25(5), 1713–1741. <https://doi.org/10.1007/s10796-022-10280-7>
- Kumar, A., Dhabliya, D., Agarwal, P., Aneja, N., Dadheech, P., Jamal, S. S., & Antwi, O. A. (2022). Cyber-internet security framework to conquer energy-related attacks on the internet of things with machine learning techniques. *Computational Intelligence and Neuroscience*, 2022, 8803586. <https://doi.org/10.1155/2022/8803586>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, p. 105, 102248. <https://doi.org/10.1016/j.cose.2021.102248>
- Luo, F., Zhang, X., Yang, Z., Jiang, Y., Wang, J., Wu, M., & Feng, W. (2022). Cybersecurity testing for automotive domain: A survey. *Sensors*, 22(23), 9211. <https://doi.org/10.3390/s22239211>
- Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors (Basel, Switzerland)*, 22(2), 538. <https://doi.org/10.3390/s22020538>
- Rubasundram, G. A., & Rasiah, R. (2019). Corruption and good governance: An analysis of ASEAN's E-governance experience. *Journal of Southeast Asian Economies*, 36(1), 57–70. <https://doi.org/10.1355/ae36-1f>
- Sarker, K., Rahman, H., Farzana Rahman, K., Arman, S., Biswas, S., & Bhuiyan, T. (2019). A comparative analysis of the cyber security strategy of Bangladesh. *International Journal on Cybernetics & Informatics*, 8(2), 1–21. <https://doi.org/10.5121/ijci.2019.8201>
- Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review*, 3(1), 7–34. <https://doi.org/10.1365/s43439-021-00045-4>
- Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats. *International Cybersecurity Law Review*, 1(1–2), 51–61. <https://doi.org/10.1365/s43439-020-00014-3>
- Tubis, A. A., Werbińska-Wojciechowska, S., Góralczyk, M., Wróblewski, A., & Ziętek, B. (2020). Cyber-attacks risk analysis method for different levels of automation of mining processes in mines based on fuzzy theory use. *Sensors*, 20(24), 7210. <https://doi.org/10.3390/s20247210>
- Ullah, F., Ullah, S., Naeem, M. R., Mostarda, L., Rho, S., & Cheng, X. (2022). Cyber-threat detection system using a hybrid approach of transfer learning and multi-model image representation. *Sensors (Basel, Switzerland)*, 22(15), 5883. <https://doi.org/10.3390/s22155883>
- Veena, K., Meena, K., Kuppusamy, R., Teekaraman, Y., Angadi, R. V., & Thelkar, A. R. (2022). Cybercrime: Identification and prediction using machine learning techniques. *Computational Intelligence and Neuroscience*, 2022, 8237421. <https://doi.org/10.1155/2022/8237421>
- Venkatachary, S. K., Alagappan, A., & Andrews, L. J. B. (2021). Cybersecurity challenges in the energy sector (virtual power plants) - Can edge computing principles be applied to enhance security? *Energy Informatics*, 4(1), 5. <https://doi.org/10.1186/s42162-021-00139-7>

- Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as “the three R’s.” *Heliyon*, 5(12), e02855. <https://doi.org/10.1016/j.heliyon.2019.e02855>
- Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy, and blockchain: A review. *SN Computer Science*, 3(2), 127. <https://doi.org/10.1007/s42979-022-01020-4>
- Yuliana, R., & Hasibuan, Z. A. (2022). Best practice framework for information technology security governance in Indonesian government. *International Journal of Electrical and Computer Engineering*, 12(6), 6522–6534. <https://doi.org/10.11591/ijece.v12i6.pp6522-6534>