Science and Technology Indonesia
e-ISSN:2580-4391 *p*-ISSN:2580-4405
Vol. 11, No. 2, April 2026

Research Paper

Geospatial Intelligence (GEOINT)-Based Cyber Warfare Exposure Index (CWEI) Mapping of Indonesia's Strategic Infrastructure

Anugrah Adityayuda[1*], Asep Adang Supriyadi[1], Syachrul Arief[2]

[1]*Sensing Technology Department, Faculty of Defense Engineering and Technology, Indonesia Defense University, Bogor Regency, West Java, 16810, Indonesia*
[2]*Geospatial Information Authority of Indonesia, Bogor Regency, West Java, 16911, Indonesia*
***Corresponding author**: anugrah.adityayuda@gmail.com

Abstract
The increasing integration of digital systems into critical infrastructure has transformed cyber warfare into a systemic national security risk with strong spatial characteristics. In Indonesia, rapid digitalization and uneven infrastructure development have expanded the cyber-attack surface, while existing studies remain largely qualitative or rely on aggregated national indices that fail to capture subnational exposure patterns. This study addresses this gap by developing a Cyber Warfare Exposure Index (CWEI) based on Geospatial Intelligence (GEOINT) to assess provincial-level exposure across Indonesia. The index integrates seven indicators, energy, transportation, telecommunications, government facilities, internet penetration, night-time light intensity, and urbanization, derived from open-source geospatial data and official statistics. All indicators were normalized using min–max scaling and aggregated through equal-weighted, with robustness tested using Principal Component Analysis (PCA), Pearson correlation, and One-at-a-Time sensitivity analysis. Results reveal strong spatial disparities in cyber warfare exposure, with CWEI values ranging from 0.019 to 0.746. DKI Jakarta exhibits the highest exposure (CWEI = 0.746), followed by West Java (0.573) and Central Java (0.564), while several eastern provinces fall into the very low exposure category. The equal-weighted and PCA-based indices show near-perfect agreement (R^2 = 0.997; r = 0.998), confirming high methodological robustness. Global Moran's I (0.689; p < 0.001) indicates significant positive spatial autocorrelation of exposure. These findings demonstrate that cyber warfare exposure in Indonesia is highly concentrated and spatially structured, underscoring the need for regionally prioritized, risk-based cyber defense strategies.

Keywords
Cyber Warfare, Geospatial Intelligence, Spatial Risk Assessment, Composite Index, Critical Infrastructure, Indonesia

Received: 7 December 2025, Accepted: 4 March 2026
https://doi.org/10.26554/sti.2026.11.2.677-691

1. INTRODUCTION

Digital transformation has shifted the nature of national security threats from predominantly physical threats to a multi-domain threat spectrum encompassing cyberspace. Cyber warfare is no longer limited to sabotaging military information systems, but has expanded to include attacks on strategic civilian infrastructure such as energy grids, transportation systems, telecommunications, and digital government, directly impacting national stability and public safety (Sommer et al., 2023). The cyber era has brought about a new reality in national security, where the unique characteristics of the cyber domain differ fundamentally from traditional conceptualizations of national security, creating a convergence between the virtual and physical worlds that changes the entire national security frame of reference (Reveron and Savage, 2020; Sommer et al., 2023). This study explicitly distinguishes cyber warfare from large-scale cybercrime. Cyber warfare refers to state-linked or state-directed cyber operations targeting strategic infrastructure for geopolitical or national security objectives (Harknett and Smeets, 2022). Cybercrime is primarily financially motivated and conducted by non-state actors (Abrardi et al., 2025). The CWEI is therefore designed to assess exposure to strategic, state-relevant cyber threats rather than generalized cybercriminal activity.

In this context, cyberspace has evolved into a strategic domain closely integrated with physical and social space, forming a complex and interdependent cyber-physical system. Critical infrastructure relies on Information and Communication Technology (ICT) systems to enable the smooth operation of its equipment and facilities (Avtar et al., 2021). These cyber-physical systems are vulnerable to cyberattacks due to their vulnerabilities, making their security a critical issue that requires a multidimensional approach that integrates cybersecurity, information warfare, and civil-military cooperation for effective defense against hybrid threats (Pramono, 2025; Yu et al., 2023).

Indonesia faces a significant digital security paradox, where accelerated ICT infrastructure development, expanded internet penetration, and the implementation of digital government have improved the efficiency of public services and driven economic growth, but simultaneously expanded the attack surface for both state and non-state actors in cyberspace. Empirical evidence shows that Indonesia's internet penetration rate increased dramatically from 25.37% in 2016 to 53.73% in 2020, with a total of 204 million people (73% of the population) connected to the internet (Anggoro et al., 2022). However, this growth is accompanied by various serious cyber threats including cybercrime, scams, phishing, malware injection, and potential cyber warfare, with concrete cases such as the Tokopedia data breach that was traded on the dark web (Marwan et al., 2022; Wibowo et al., 2024).

This paradox is exacerbated by a combination of high reliance on digital infrastructure, uneven institutional capacity, and technical security gaps common in developing countries with intermediate levels of digitalization. Security challenges in implementing Electronic Government Systems (ESBS) arise from the large volume of sensitive information that must be managed (Ibrahim et al., 2020), while Anggoro et al. (2022) reveals the uneven level of ICT vulnerability, particularly in eastern Indonesia. This condition has the potential to threaten national sovereignty and emphasizes the urgency of strengthening national cyber infrastructure and institutions (Aulianisa and Indirwan, 2020).

Cybersecurity literature consistently asserts that critical infrastructure, including energy, transportation, telecommunications, and digital government systems, are prime targets for cyber warfare due to their centralized, interconnected nature and widespread impact on other sectors (Aljohani, 2024; Czuryk, 2023; Venkatachary et al., 2024). The integration of intelligent transportation systems and the proliferation of sensors and Internet of Things (IoT) devices are increasing operational efficiency, but simultaneously expanding cyberattack vectors that could potentially threaten public safety and national security (Alomari et al., 2025; Zeddini et al., 2022). In the spatial dimension, the night-time light (NTL) indicator has been empirically proven to be a strong proxy for economic activity, infrastructure density, and intensity of digital system use, especially in areas with limitations in conventional statistics (Gibson et al., 2020; Zheng et al., 2023b). It is important to emphasize that NTL intensity and internet penetration are employed in this study as proxy indicators of digital activity, infrastructure concentration, and socio-economic intensity, rather than as direct causal drivers of cyber warfare. These indicators reflect the spatial distribution of potential cyber-physical targets and the density of digitally dependent systems, which condition exposure to cyber warfare activities. Their use is therefore aligned with exposure-based assessment frameworks, not causal threat modeling. The level of urbanization also reflects the concentration of complex cyber-physical systems, with urban areas exhibiting a higher reliance on digital infrastructure and energy consumption, thus implying a greater level of cyber exposure (Chang et al., 2025; Marull et al., 2023; Zheng et al., 2023a).

Geospatial approaches are increasingly recognized as an effective analytical framework for integrating physical and digital dimensions in non-kinetic security risk assessments. Studies based on spatial indices and quantitative analyses demonstrate that geospatial data integration can represent the complexity of multidimensional risks more objectively and measurably at regional and national scales, particularly in developing countries with high regional heterogeneity (Maulana et al., 2025; Suhadi et al., 2023). The Geospatial Intelligence (GEOINT) approach enables spatial mapping of strategic infrastructure and digital activities to uncover risk concentration patterns not identified through non-spatial approaches (Adityayuda et al., 2024).

However, most cyber warfare studies still focus on qualitative analysis, incident case studies, or aggregate national indices that fail to capture the spatial variation in vulnerability within a single country. Empirical studies indicate significant digital disparities in Indonesia, with digital transformation and infrastructure concentrated in western metropolitan areas, while transitional regions and eastern Indonesia lag structurally behind (Jaya et al., 2024; Kartiasih et al., 2023). The limitations of this non-spatial approach make GEOINT a relevant framework for integrating spatial data, statistics, and infrastructure indicators in mapping cyber warfare risks territorially (Liu et al., 2022; Setiawan et al., 2024).

Based on these gaps, this study aims to develop a province-based Cyber Warfare Exposure Index (CWEI) in Indonesia to measure the level of cyber warfare exposure based on the spatial concentration of critical infrastructure and digital activity indicators. This study analyzes the spatial distribution patterns and regional clustering of cyber warfare exposure and evaluates the robustness of the composite index through a comparison of equal-weighted schemes and Principal Component Analysis (PCA). The selection of indicators, including energy, transportation, telecommunications, government offices, internet penetration, night light intensity, and urbanization level, is based on consistent literature findings that confirm the close relationship between cyber warfare exposure and dependence on digital infrastructure and the economy (Lasaiba, 2022; Situmorang et al., 2023; Manullang, 2022). All indicators are given equal-weighted to maintain methodological transparency and increase the replicability of research across regions and time (Aulianisa and Indirwan, 2020).

This study systematically examines how geospatial intelligence can be integrated to measure cyberwarfare exposure at the provincial level in Indonesia. Specifically, it seeks to identify which provinces exhibit the highest levels of cyberwarfare exposure based on the spatial concentration of critical infrastructure and digital activity indicators. Furthermore, it explores the spatial patterns and distribution characteristics of cyberwarfare vulnerabilities across Indonesia, with particular attention to geographic clustering and regional disparities. Finally, it evaluates the robustness of the proposed composite index approach by comparing an equal-weighted aggregation

method with a data-driven weighting scheme using PCA.

Based on existing literature and preliminary observations, this study hypothesizes that provinces with a higher density of critical infrastructure will exhibit significantly higher levels of cyberwarfare exposure. Furthermore, provinces located in Java are expected to dominate the Very High exposure category due to the concentration of economic activity, digital infrastructure, and government systems in these regions. Conversely, provinces in Eastern Indonesia are hypothesized to be dominated by the Low exposure category due to limited digital infrastructure, lower internet penetration, and reduced urbanization rates. Furthermore, this study suggests that an equal-weighted composite index will exhibit a strong positive correlation with the PCA-derived weights index ($R^2 > 0.90$), thus demonstrating the robustness of the indicator selection and aggregation strategy.

2. EXPERIMENTAL SECTION

2.1 Data Collection and Characteristics

This study uses a quantitative approach with all provinces in Indonesia as the unit of analysis. The data used represents the dimensions of infrastructure exposure to cyber warfare, constructed from seven main indicators such as energy, transportation, telecommunications, government offices, internet penetration, nighttime light intensity, and urbanization level. Data on energy, transportation, telecommunications, and government infrastructure were obtained through spatial extraction and aggregation from the open-source OpenStreetMap (OSM) database, which has been widely used in critical infrastructure mapping studies and spatial risk analysis due to its coverage and up-to-date data (OpenStreetMap, 2025). Night light intensity indicators are taken from the Visible Infrared Imaging Radiometer Suite (VIIRS) sensor, which is widely used as a proxy for economic activity and infrastructure density (Elvidge et al., 2013). Urbanization rate data is sourced from the Global Human Settlement Layer (GHSL) (Pesaresi et al., 2024), while internet penetration data was obtained from the official report of the Indonesian Internet Service Providers Association (APJII) (APJII Indonesia, 2024).

In this study, exposure refers to the spatial presence and concentration of potential cyber warfare targets, vulnerability denotes weaknesses in defense mechanisms, and risk reflects the probability and impact of realized attacks. CWEI is explicitly constructed as an exposure index and does not directly measure vulnerability or realized cyber risk. Indicators related to cyber defense capacity, such as security operations centers, intrusion detection systems, or cyber workforce readiness, were excluded due to limited data availability and classification constraints. As a result, CWEI focuses on infrastructure-centric exposure rather than defensive capability, which should be addressed in complementary assessments.

Table 1 summarizes the data sources and indicators used in constructing the CWEI. The selection of indicators is based on consistent literature findings from the past five years, which emphasize that cyber warfare exposure is closely correlated with critical infrastructure density, digital activity intensity, and cyber-physical system concentration. The use of open-source data and official statistics ensures transparency, replicability, and the feasibility of applying the methodology to developing country contexts.

The seven indicators selected in this study represent the main dimensions of cyber warfare exposure, encompassing critical physical infrastructure, digital infrastructure, and the spatial characteristics of human activity. Energy, transportation, telecommunications, and government indicators reflect cyber-physical systems that are the primary targets of strategic cyber operations. Meanwhile, internet penetration, nighttime light intensity, and urbanization levels serve as proxy indicators that capture the intensity of digital interactions, the density of economic activity, and the complexity of urban systems. This combination of direct and proxy indicators is designed to ensure comprehensive exposure coverage without excessive redundancy. All data is converted to the provincial level through a spatial join and statistical aggregation process, resulting in each indicator having a single representative value per province. This approach enables consistent and comparative spatial analysis across administrative regions and supports multi-source data integration within a GEOINT framework.

2.2 Data Processing

The data processing stage begins with normalizing all indicators using the min-max normalization method to eliminate scale differences between variables. Based on Starovoitov and Golub (2021), input data is often presented in different dimensions, requiring conversion to a single representation through normalization. This method ensures that no single variable dominates the analysis due to its original scale. Research shows that data normalization can improve classification accuracy and enable meaningful comparisons between indicators with different units of measurement. Normalization is performed using the equation:

$$X'_{ij} = \frac{X_{ij} - X_{j,\min}}{X_{j,\max} - X_{j,\min}} \quad (1)$$

where the standardized indicator value, is the original indicator value for the province in indicator, and are the minimum and maximum values of indicator, respectively $X'_{ij}X_{ij}ijX_{j,\min}$ $X_{j,\max}j$.

After normalization, the CWEI index is calculated using an equal-weighted approach, where each indicator is given an equal-weighted. This approach was chosen to maintain objectivity, avoid normative bias, and increase the transparency and replicability of the model. The use of an equal-weighted approach in the construction of the CWEI is based on methodological and epistemological considerations. In the context of cyber warfare, there is no empirical data on the relative importance of different types of infrastructure at the national scale. Therefore, giving equal-weighted to all indicators was chosen to avoid normative bias and implicit assumptions about the priority of certain threats. This approach is in line with the

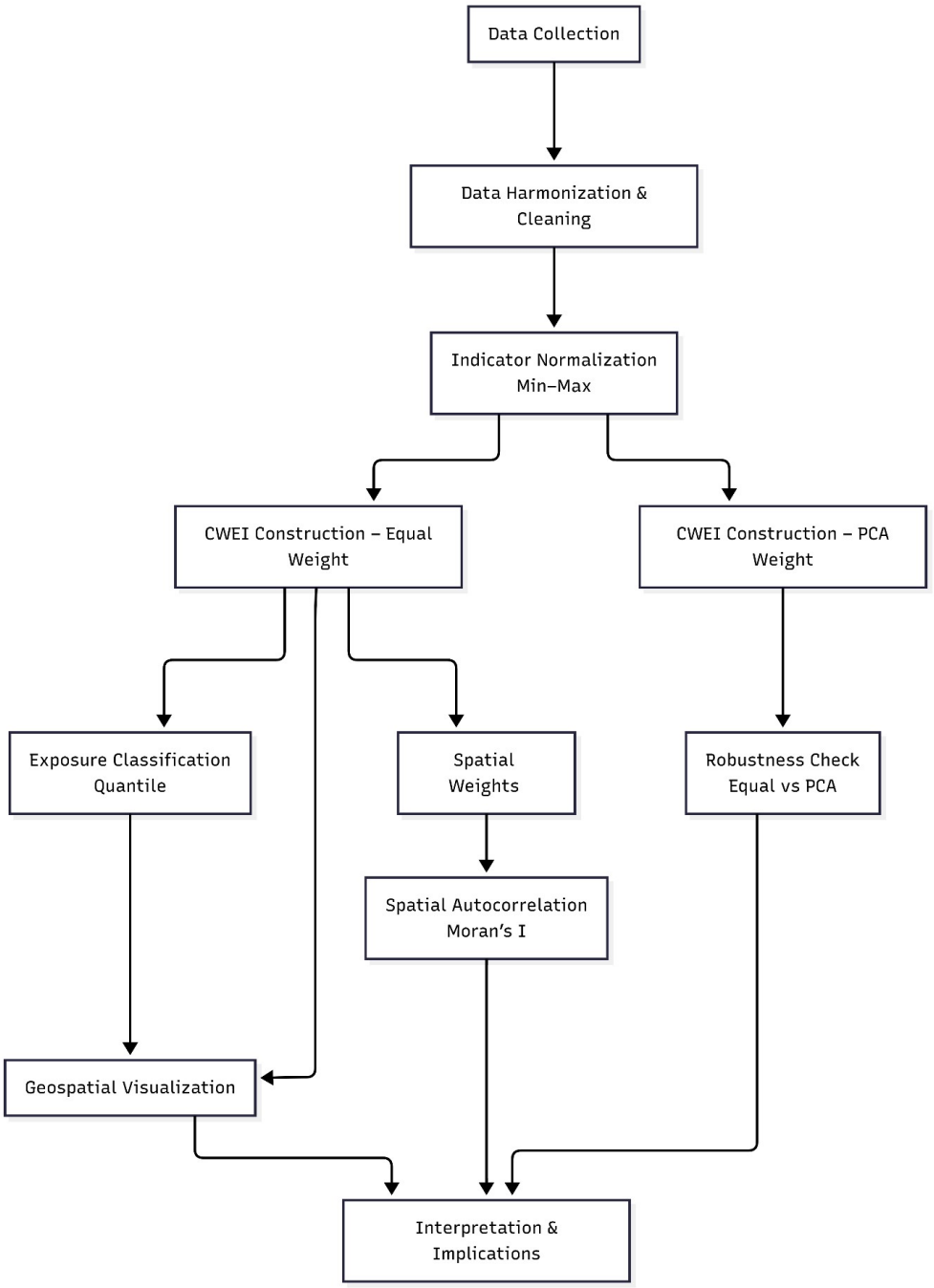

Figure 1. Research Framework

principle of methodological prudence and is widely used in risk and security indices when the causal relationships between variables are complex and interdependent (w_j=1/7) (Decancq and Lugo, 2013; Gasser, 2020). The CWEI formula is formulated as follows:

$$CWEI_i = \sum_{j=1}^{n} w_j X'_{ij} \quad (2)$$

with as the number of indicators. The CWEI values were then classified into five exposure classes (very low to very high) using the quantile classification method to facilitate spatial interpretation and interprovincial comparisons n = 7.

To classify CWEI values into five spatial exposure classes, this study used a quantile classification scheme. The quantile classification method divides all provinces into a number of classes, each with an equal number of observations (provinces). In other words, each class represents a certain percentile of the

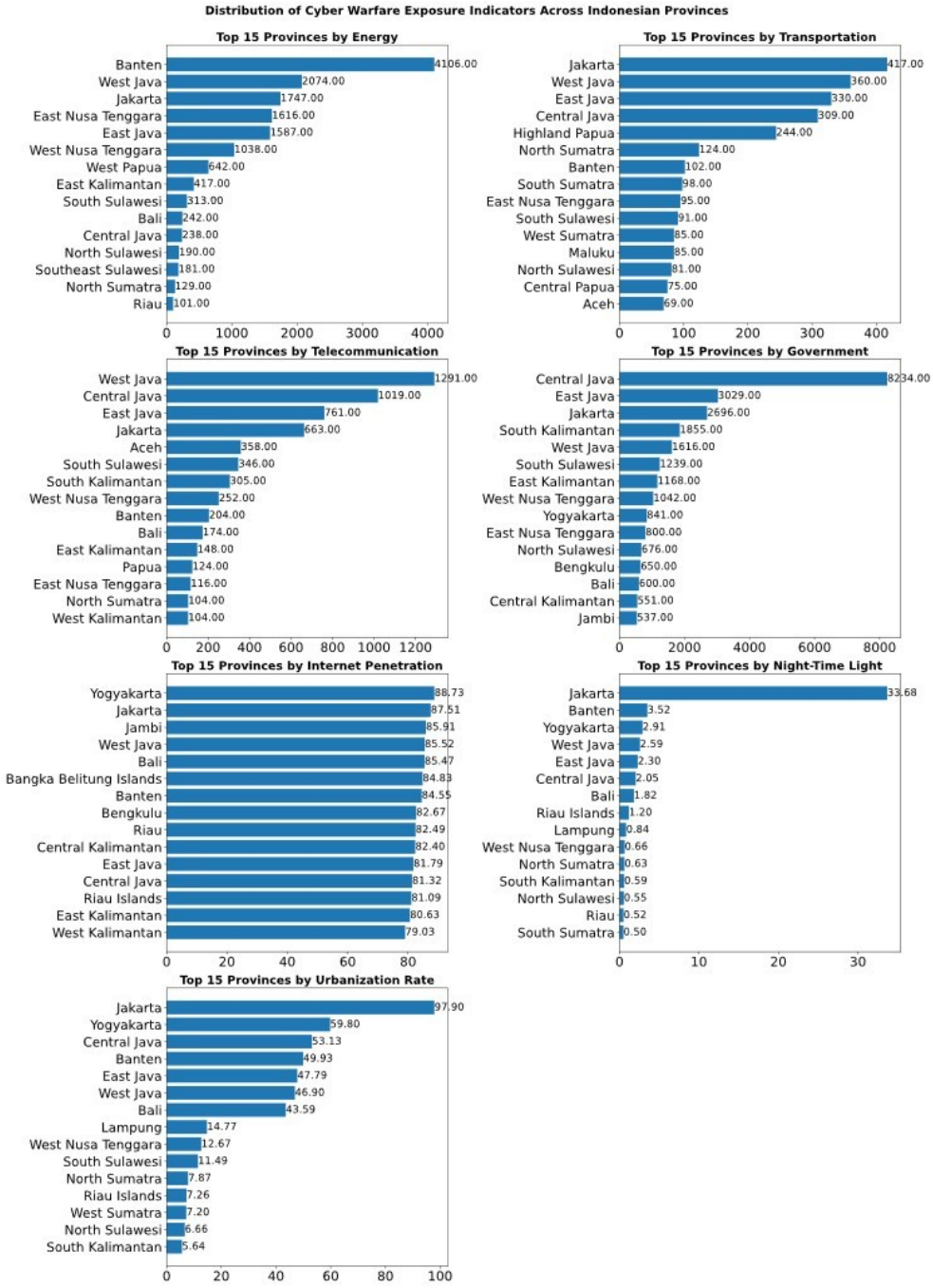

Figure 2. Data Distribution per Province

value distribution, so that each class has a statistically balanced database. This approach differs from the equal interval or natural breaks method, because quantiles do not divide the range of values absolutely or attempt to find "natural grouping" in the data, but rather emphasize the ordinal distribution of values and uniform visual representation on choropleth maps in a geospatial context (Li and Shan, 2022).

Cartographically, the quantile classification method is often used to reveal relative spatial patterns when the focus of the analysis is on regional rankings rather than absolute differences in values. This is important in the context of this research because the CWEI is a composite index that aggregates various indicators with a skewed distribution of values. With quantiles, each class has a balanced number of provinces in the analysis, so the exposure class map is not dominated by outliers and facilitates relative comparisons between regions (Li and Shan, 2022).

2.3 Robustness and Sensitivity Test

As part of the robustness check, the results of the equal-weighted CWEI were compared with an alternative index constructed using PCA. PCA was used to identify the dominant variance structure in the data and generate indicator weights based on pure statistics without any normative assumptions, in line with the findings Alqararah (2023) which shows PCA as an effective weighting-aggregation method to reduce subjectivity in the construction of composite indicators. Wu et al. (2022) strengthen this approach by showing that PCA is effective as a dimensionality reduction technique for identifying critical variables in risk and emergency assessments.

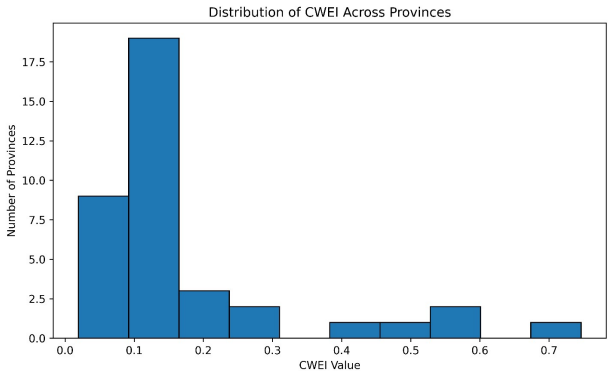

Figure 3. Histogram of CWEI Distribution Across Provinces (Skewness)

In constructing composite indices such as the CWEI, the choice of weighting scheme is a major source of methodological uncertainty. The index methodology literature emphasizes that indicator weights often contain normative elements or implicit assumptions that can potentially influence the final results and rankings of regions (Nardo et al., 2008). Therefore, this study not only adopts an equal-weighted approach to maintain transparency and replicability, but also complements it with a sensitivity test as a mechanism for evaluating the model's robustness. Sensitivity analysis was conducted using the One-at-a-Time (OAT) approach, where the weight of each indicator is systematically varied (±10%) while other indicators are held constant, to observe the stability of CWEI scores and rankings. This approach is in line with recommendations (Nardo et al., 2008) which places sensitivity testing as an essential component in the validation of multidimensional indexes, as well as with the analytical framework proposed by Decancq and Lugo (2013), which emphasizes that a robustness evaluation of weight variations is necessary to ensure that substantive conclusions are not solely based on specific weighting assumptions. Thus, the application of the OAT sensitivity test in this study serves to strengthen the methodological legitimacy of the CWEI and increase confidence in the spatial interpretation of cyber warfare exposure between provinces.

2.4 CWEI Development Framework

This study uses a structured methodological framework to measure and map provincial-level cyberwarfare exposure in Indonesia through the development of the CWEI. The research framework is shown in Figure 1.

The process began with multi-source data collection covering critical infrastructure indicators, digital and economic activity metrics, and provincial geospatial boundaries, followed by data harmonization and cleaning to ensure consistency and comparability. All indicators were normalized using min-max normalization to eliminate scale effects. The CWEI was then constructed using two parallel approaches: a composite index with equal-weighted to ensure transparency and interpretability, and a PCA-derived weights scheme to provide a data-driven benchmark for resilience assessment. The use of equal-weighted inherently involves normative assumptions regarding indicator importance. However, this approach enhances transparency, minimizes subjective bias, and facilitates replication. Robustness checks using PCA-derived weights confirm that the resulting spatial patterns are not sensitive to weighting schemes.

Equal-weighted CWEIs were classified into exposure levels using Quantile Classification, allowing comparison of relative risks across provinces. Spatial dependence was examined through the K-Nearest Neighbors (KNN) spatial weight matrix, chosen to accommodate Indonesia's archipelagic geography, and evaluated using Global Moran's I to identify spatial autocorrelation patterns. Finally, CWEI values were visualized through thematic geospatial mapping, and all analysis results, including index construction, robustness testing, and spatial statistics, were integrated to generate policy-relevant interpretations regarding the spatial structure of Cyber Warfare exposure. Table 2 summarizes the analysis techniques employed in this study.

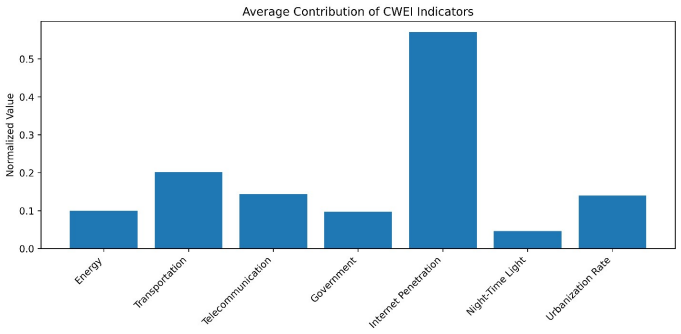

Figure 4. Contribution of CWEI Indicators

3. RESULTS AND DISCUSSIONS

3.1 Descriptive Statistics of CWEI Indicators

Descriptive statistical analysis was conducted to provide an initial understanding of the characteristics, distribution, and level of variation of the indicators that make up the CWEI at the

Table 1. Data Sources and Indicators for CWEI Construction

Indicator	Data Source	Resolution	Year	Relevance
Energy Infrastructure	OSM	Spatial (Point)	2025	Energy infrastructure is a primary target of cyber warfare due to its critical nature and systemic impact across sectors.
Transportation Infrastructure	OSM	Spatial (Point)	2025	Modern transportation systems rely on digital systems and are vulnerable to cyber intrusions with public safety implications.
Telecommunication	OSM	Spatial (Point)	2025	Telecommunications serve as the backbone of all cyber and digital government activities.
Government offices	OSM	Spatial (Point)	2025	Representation of state asset concentration and digital administration system.
Internet Penetration	APJII	Provincial Statistics	2024	Proxy of connectivity intensity and potential attack surface.
Night-Time Light (NTL)	VIIRS	Raster	2024	Empirical proxies of economic activity and digital infrastructure density.
Urbanization Rate	GHSL	Raster	2024	Urbanization reflects the concentration of complex cyber-physical systems.

provincial level in Indonesia. Table 3 presents the minimum, maximum, mean, standard deviation, and other distribution measures for each indicator, which collectively represent the dimensions of infrastructure and socio-digital exposure to cyber warfare risk.

Table 3 presents descriptive statistics for the seven normalized indicators used in the construction of the CWEI. All indicators were scaled to a range of 0-1 to ensure comparability across dimensions. The results indicate substantial heterogeneity among the indicators, as reflected in their mean values and higher-order moments. Indicators related to infrastructure and governance, such as Energy and Governance, exhibit relatively low mean values accompanied by high positive skewness and kurtosis, indicating that high levels of exposure are concentrated in a limited number of provinces. In contrast, Internet Penetration exhibits a relatively high mean value (0.571) and negative skewness, indicating a more even distribution and wider access across regions. The mean NTL radiation exhibits extreme skewness (5.697) and kurtosis (31.280), reflecting the strong spatial concentration of economic activity in metropolitan areas. Overall, these distributional properties justify the use of composite normalization and aggregation, as the raw indicator values will be dominated by a small number of highly urbanized provinces.

Analysis of the distribution shape shows that most indicators have positive skewness, indicating an asymmetric distribution with a long positive slope. This pattern indicates that only a small number of provinces have very high indicator scores, while the majority of provinces are at low to medium levels. This finding confirms that cyber warfare exposure in Indonesia is not randomly distributed, but rather concentrated in regions with high strategic infrastructure intensity, cyber-physical system complexity, and high economic activity.

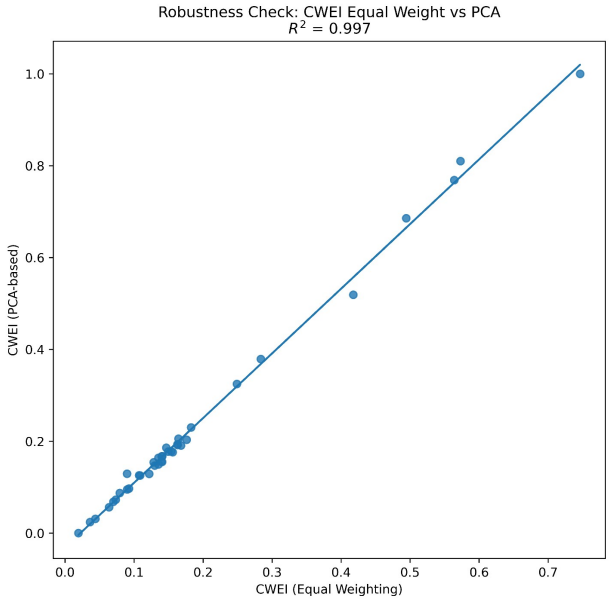

Figure 5. Scatter Plot Equal-Weighted Vs PCA

Overall, the descriptive statistics in Table 3 provide strong empirical justification for the CWEI composite index approach. Variation across indicators and across provinces underscores the need for a quantitative and spatial approach to mapping cyber warfare exposure territorially. These results also provide an important methodological basis for further analysis, both in spatial mapping of the CWEI and in testing the robustness of the model through comparison with the PCA approach.

Table 2. Framework and Analysis Techniques

Stage	Method	Objective
Normalization	Min–Max Scaling	Equalizing the indicator scale
Aggregation	Equal-Weighted	Transparency and replicability
Robustness	Principal Component Analysis (PCA)	Data structure validation
Classification	Quantile	Spatial interpretation
Spatial Autocorrelation	Moran's I (KNN)	Geographic cluster detection
Sensitivity	OAT Weighting	Index stability test

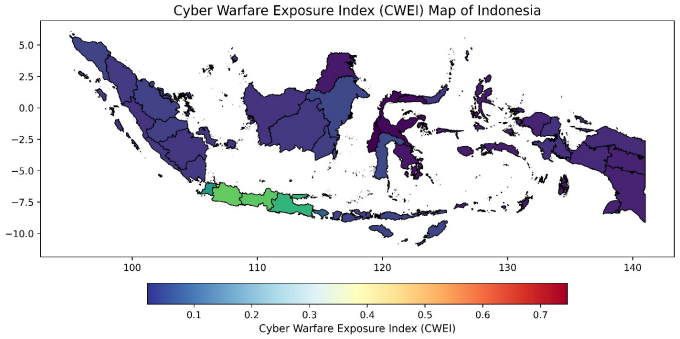

Figure 6. CWEI Indonesia Map

3.2 CWEI Indicator Levels Across Provinces

A disparity analysis of the CWEI indicators was conducted to identify spatial inequality patterns in the distribution of strategic infrastructure and socio-digital characteristics across provinces in Indonesia. The vertical bar graph visualization in Figure 2 reveals stark differences between regions, both on an absolute scale and in the pattern of provincial rankings for each indicator. These results confirm that exposure to cyber warfare is highly localized and influenced by the concentration of specific strategic functions.

Infrastructure indicators, such as energy, transportation, telecommunications, and government facilities, show clear dominance by a small number of provinces. DKI Jakarta consistently ranks at the top across almost all indicators, particularly telecommunications and digital government, reflecting its role as the center of state administration and a key node in the national information network. Provinces on the island of Java, particularly West Java, Central Java, and East Java, also show high indicator scores, indicating a large concentration of cyber-physical systems and public service infrastructure. In contrast, most provinces in Eastern Indonesia and the archipelago region show relatively low indicator scores and tend to be distributed at the bottom of the distribution. This pattern suggests that while these regions have lower absolute exposure to cyber warfare, they also potentially have limited cyber defense capacity and system redundancy, which could increase functional vulnerability in the event of a regional-scale cyber disruption. Internet penetration and urbanization indicators show a different pattern of disparity compared to hard infrastructure. The bar chart shows that while urban provinces on the island of Java remain in the top group, the gap between provinces is relatively narrow. This shows that basic access to digital technology has spread more widely, but this has not necessarily been accompanied by an increase in adequate system security capacity and cyber governance.

Table 4 provides information on provincial-level CWEI scores obtained from Equal-Weighted and PCA, along with categorical classifications of exposure levels. The results show a clear spatial hierarchy of exposure, with DKI Jakarta consistently ranking highest under both weighting schemes, followed by the larger provinces in Java, such as West Java, Central Java, and East Java. Provinces classified as having Very High exposure are largely characterized by high population density, high infrastructure intensity, and concentrated economic activity. In contrast, provinces in eastern Indonesia, particularly in the regions of Papua, Maluku, and Sulawesi, exhibit significantly lower CWEI values and are classified as Low to Very Low exposure. The inclusion of the Exposure Level category improves interpretation by translating continuous index values into policy-relevant exposure classes, facilitating comparative risk assessments across provinces. The similarity between the equal-weighted CWEI and PCA CWEI rankings indicates that the observed spatial patterns of exposure are robust to alternative weighting assumptions.

3.3 Characteristics of CWEI Value Distribution

Analysis of the distribution characteristics of CWEI values across provinces provides in-depth quantitative insights into national cyber vulnerability patterns. Visualizations using the Histogram of CWEI Distribution across Provinces in Figure 3 and the Contribution of CWEI Indicators in Figure 4 reinforce and enrich the spatial findings outlined previously.

The distribution histogram in Figure 3 clearly shows that the distribution of CWEI values follows an abnormal (non-symmetric) pattern with positive skewness (leaning to the right). The vast majority of provinces (as seen from the tall bars of the histogram) are concentrated in the low to medium CWEI range (around 0.1-0.3). Meanwhile, only a small number of provinces have very high CWEI values (approaching 0.5-0.7),

Table 3. Descriptive Statistics (Normalized Values)

Indicator	N	Mean	Std. Dev	Min	Max	Skewness	Kurtosis
Energy	38	0.099	0.200	0	1	2.95	9.267
Transportation	38	0.201	0.248	0	1	2.04	3.054
Telecommunication	38	0.143	0.221	0	1	2.545	5.94
Government	38	0.097	0.173	0	1	4.067	18.178
Internet Penetration	38	0.571	0.266	0	1	-0.349	-0.764
Night-Time Light (NTL)	38	0.046	0.161	0	1	5.697	31.28
Urbanization Rate	38	0.139	0.229	0	1	2.104	3.887

indicated by the long tail on the right side of the histogram. This distribution pattern empirically proves the extreme concentration of cyber warfare risk in a handful of regions that hold a nationally strategic role, which in this context are the centers of government, economy, and digital infrastructure.

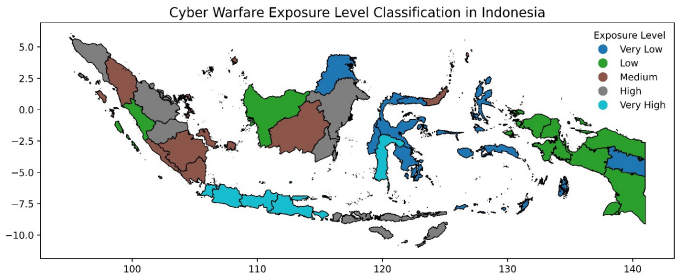

Figure 7. CWEI Level Classification Map in Indonesia

Figure 4 reveals the dominant factors driving high CWEI scores in specific provinces. This bar graph shows the average relative contribution of each index indicator. It can be seen that Internet Penetration and NTL indicators, as proxies for economic activity and urbanization, provide the highest contributions to the overall CWEI score. This is followed by critical infrastructure indicators such as Telecommunications, Energy, and Transportation. This finding is consistent with the logic that the highest exposure arises from the combination of massive digital connectivity, with high internet access, and the concentration of socio-economic-infrastructure activities.

The combination of uneven distribution patterns in Figure 3 and identified key contributors in Figure 4 has crucial policy implications. These characteristics emphasize that efforts to enhance national cyber resilience will be ineffective if implemented uniformly. Instead, a differential, risk-based approach is needed that prioritizes resources and interventions in provinces with high CWEI scores. These provinces, which are the epicentres of national activity, are prime potential targets in cyber conflict scenarios, both for disruptive attacks on vital infrastructure (energy, transportation, telecommunications) and for information and destabilization operations. This distribution and contributor analysis not only validates the CWEI construct from a statistical perspective but also transforms spatial data into actionable strategic information. The GEOINT approach through CWEI provides a clear solution for allocating cyber defense capabilities more intelligently, efficiently, and effectively, with a focus on protecting critical national assets concentrated in areas of highest exposure.

Table 5 summarizes the distribution characteristics of the CWEI under the Equal-Weighted and PCA-derived weights. Both index variants exhibit positive skewness and leptokurtic behaviour, indicating that high exposure values are concentrated in a small number of provinces, while the majority exhibit relatively low to moderate levels of exposure. The PCA CWEI exhibits a higher mean and standard deviation compared to the Equal-Weighted CWEI, reflecting the greater influence of the dominant variance component captured by PCA. Despite these differences, the overall shape of the distributions remains very similar, as evidenced by nearly identical skewness and kurtosis values. This consistency suggests that the core structure of exposure is not substantially altered by the choice of weighting methodology, strengthening the stability of the composite index.

3.4 Weighting Robustness and Sensitivity Analysis

As part of the validation, robustness tests were conducted to assess the sensitivity of the CWEI to indicator weighting assumptions. A potential concern is that index results may rely too heavily on subjective assumptions in determining weights. To test this, the CWEI calculated using the equal-weighted method, where all indicators are assumed to have equal contribution, was compared with the CWEI calculated using PCA, an objective weighting method based on data variance.

The results of this comparison, visualized in Figure 5, show a nearly perfect linear relationship between the two versions of the index. The data points representing each province are tightly clustered around the trend line. The strength of this relationship is quantified by the very high coefficient of determination (R^2) of 0.997. This value indicates that 99.7% of the variation in the PCA-derived weights CWEI can be explained by the equal-weighted CWEI, and vice versa. This finding is in line with a similar study conducted by Bruno et al. (2023) using correlation analysis and PCA to test the redundancy of the composite index, and confirming the very high robustness of the CWEI model. The relative ranking and exposure classification

Table 4. Provincial CWEI and Exposure Level

Province	CWEI Equal-Weighted	CWEI PCA	Exposure Level	Ranking
DKI Jakarta	0.746	1	Very high	1
West Java	0.573	0.81	Very high	2
Central Java	0.564	0.769	Very high	3
East Java	0.494	0.686	Very high	4
Banten	0.418	0.519	Very high	5
Special Region of Yogyakarta	0.284	0.379	Very high	6
Bali	0.249	0.325	Very high	7
South Sulawesi	0.183	0.23	Very high	8
East Kalimantan	0.176	0.203	High	9
East Nusa Tenggara	0.168	0.191	High	10
Aceh	0.164	0.205	High	11
West Nusa Tenggara	0.163	0.192	High	12
Riau	0.163	0.193	High	13
Jambi	0.156	0.176	High	14
South Kalimantan	0.154	0.178	High	15
Riau Islands	0.149	0.177	Medium	16
North Sumatra	0.147	0.186	Medium	17
North Sulawesi	0.141	0.167	Medium	18
Bengkulu	0.141	0.155	Medium	19
Lampung	0.14	0.167	Medium	20
Central Kalimantan	0.139	0.156	Medium	21
Bangka Belitung Islands	0.135	0.15	Medium	22
South Sumatra	0.135	0.164	Medium	23
West Kalimantan	0.13	0.147	Low	24
West Sumatra	0.128	0.154	Low	25
West Papua	0.122	0.129	Low	26
Papua	0.109	0.125	Low	27
Central Papua	0.107	0.126	Low	28
Southwest Papua	0.093	0.097	Low	29
South Papua	0.09	0.095	Low	30
Papua Mountains	0.09	0.129	Very Low	31
Maluku	0.079	0.087	Very Low	32
North Maluku	0.073	0.073	Very Low	33
North Kalimantan	0.07	0.068	Very Low	34
Southeast Sulawesi	0.064	0.056	Very Low	35
Gorontalo	0.044	0.031	Very Low	36
Central Sulawesi	0.036	0.024	Very Low	37
West Sulawesi	0.019	0	Very Low	38

Table 5. Distribution Statistics (Index Level)

Indicator	Mean	Std. Dev	Min	Max	Skewness	Kurtosis
CWEI Equal-Weighted	0.185	0.161	0.019	0.746	2.034	3.457
CWEI PCA	0.229	0.227	0	1	2.038	3.339

between provinces remained virtually unchanged regardless of the weighting method used.

Analysis of Table 6 reveals the underlying structure of the data. The first principal component (PC1), which captures the largest variance in the dataset, shows the loadings for each indicator. Based on absolute loadings, the indicators Transportation (0.4943) and Urbanization Level (0.4742) contributed the most, followed by Telecommunication (0.4319) and In-

Table 6. PCA Loading

Indicator	PC1 Loading	Absolute Loading	Relative Contribution (%)
Transportation	0.4943	0.4943	19.2989
Urbanization Rate	0.4742	0.4742	18.5146
Telecommunication	0.4319	0.4319	16.8616
Internet Penetration	0.3599	0.3599	14.0515
Energy	0.2833	0.2833	11.0603
Government	0.2744	0.2744	10.7151
Night-Time Light (NTL)	0.2433	0.2433	9.4979

Table 7. Robustness Test (Equal-Weighted vs PCA)

Metric	Value
Pearson Correlation	0.99836
P-value	0

ternet Penetration (0.3599). This loading pattern strengthens the conceptual validity of the CWEI, as the indicators that are theoretically most relevant to critical infrastructure vulnerability and the critical mass of the digital population are the ones that are statistically most determinant in shaping variations in index scores.

The consistency between the two approaches, demonstrated by the near-perfect scatterplot and the absence of significant changes in provincial rankings, conveys an important methodological message. The cyber warfare exposure patterns mapped by the CWEI are stable and robust. They are not dependent on subjective weighting choices but rather reflect the inherent spatial realities of Indonesia's digital infrastructure and socio-economic activities. This robustness test not only enhances the scientific credibility of the index but also provides operational confidence for stakeholders and policymakers to use the CWEI maps as a reliable basis for designing differentiated cyber defense strategies.

Table 7 presents the robustness assessment between the equal-weighted and PCA-derived weights CWEIs, followed by the results of the OAT sensitivity analysis in Table 8. The Pearson correlation coefficient of 0.998, with a statistically significant p-value, indicates a near-perfect linear relationship between the two index formulations, confirming that the overall ranking of provinces is highly stable across different weighting approaches. Further OAT sensitivity analysis shows that a ±10% change in the weighting of individual indicators results in only marginal changes in the composite index, with correlation values consistently exceeding 0.99. Among all indicators, Internet Penetration exhibits the largest relative influence, although its impact remains limited and does not alter the overall exposure structure. Collectively, these findings confirm that the CWEI is robust and insensitive to moderate variations in weighting assumptions, meeting a key methodological requirement for composite index construction.

3.5 Spatial Distribution of CWEI and Exposure Levels

Analysis of the spatial distribution of the CWEI in Indonesia, as visualized in Figures 6 and 7, reveals a highly structured pattern of cyber exposure that aligns with geographic, economic, and demographic realities. The CWEI map in Figure 6 shows a spectrum of exposure values from 0 to 1. This map shows a clear gradation of vulnerability, where areas with high index values (lighter colors/closer to 0.5-0.7 on the bar scale) are concentrated predominantly on the island of Java, with several points scattered across Sumatra, Kalimantan, and Sulawesi, which are centers of regional economic growth and governance.

This pattern is reinforced and qualified by the Classification Map in Figure 7, which groups provinces into five categories: Very Low, Low, Medium, High, and Very High. This classification clearly shows that provinces with Very High exposure are almost entirely located on the island of Java (such as Jakarta, West Java, East Java, and Banten) and several other administrative/commercial centers outside Java. This reflects the accumulation of risk factors such as the density of critical digital infrastructure, the intensity of digital economic transactions, the concentration of government data, and high geopolitical activity.

Provinces with Low to Very Low exposure are consistently located in areas with low population density, limited economic and government activity, and underdeveloped digital infrastructure. These areas are primarily located in eastern Indonesia, most of the small islands, and inland areas. The consistency between the CWEI map and this classification map indicates no significant spatial anomalies. The resulting pattern fully aligns with geographic-economic logic: the higher the intensity of a region's socio-economic-digital activity, the higher its exposure to potential cyberwarfare attacks. This consistency is a strong indicator that the CWEI construction is capable of validly and consistently representing spatial reality.

The spatial distribution of the CWEI strengthens the index's position as a reliable proxy within the GEOINT framework. The resulting map not only describes the current situation but also provides a critical spatial basis for strategic planning, cybersecurity resource allocation, and targeted mitigation policymaking, focusing on areas classified as High and Very High. Table 9 displays the results of the global Moran's I analysis applied to the CWEI. The observed Moran's I value

Table 8. OAT Sensitivity Analysis

Indicator	Correlation (+10%)	Correlation (-10%)
Energy	0.996	0.995
Transportation	0.998	0.996
Telecommunication	0.998	0.997
Government	0.997	0.997
Internet Penetration	0.993	0.990
Night-Time Light	0.998	0.997
Urbanization Rate	0.999	0.998

Table 9. Spatial Statistics (Moran's I)

Metric	Value
Moran's I	0.689
Expected I	-0.027
Z-score	7.072
p-value	0.000

is 0.689. This value is substantially higher than the value expected under spatial randomness, indicating strong positive spatial autocorrelation. The associated Z-scores and highly significant p-values confirm that the spatial autocorrelation of exposure is not random. Provinces with high CWEI values tend to be geographically close together, particularly in Java and parts of Sumatra, while provinces with low exposure are clustered in eastern Indonesia. This spatial dependence underscores the importance of incorporating spatial considerations in exposure assessments and policy formulation, as regional vulnerability is shaped not only by local characteristics but also by broader spatial and infrastructure interdependencies.

3.6 Synthesis and Strategic Implications

The results of this study indicate that the CWEI exhibits a highly uneven spatial distribution across Indonesia. Descriptive statistics for the indicators in Table 3 show that most of the variables comprising the CWEI, particularly energy, telecommunications, government, and nighttime light intensity, follow a right-skewed distribution with high skewness and kurtosis values. This pattern indicates a strong concentration of strategic infrastructure assets and digital activities in a small number of provinces, while the majority of other regions have relatively lower levels of exposure. This finding confirms that cyber warfare risk in Indonesia is not homogeneously distributed but rather structurally clustered. Accordingly, CWEI scores should not be interpreted as indicators of cybercrime prevalence, but as measures of structural exposure to strategic cyber warfare operations. At the provincial level in Table 4, provinces on the island of Java, particularly Jakarta, West Java, Central Java, and East Java, consistently rank in the Very High category. These results directly confirm that regions with high critical infrastructure density and high digital activity exhibit greater levels of cyberwarfare exposure. These provinces' dominant positions reflect Java's central role as the center of government, the economy, the energy network, and national telecommunications connectivity. Conversely, most provinces in Eastern Indonesia rank in the Low to Very Low categories, illustrating the gap in digital and infrastructure development between regions.

Analysis of the aggregate index distribution in Table 5 reveals a high degree of variation in the CWEI, with significant skewness and kurtosis at the index level. This indicates that national cyber warfare risk is dominated by a small number of high-risk provinces, while most other provinces contribute relatively little to the total national exposure. From a non-military defense policy perspective, this finding confirms that cyber risk mitigation strategies are ineffective if applied uniformly. Instead, a regional priority-based approach is crucial to ensuring efficient allocation of cybersecurity resources.

Model robustness tests in Table 7 show a very strong correlation between the equal-weighted index and the PCA-derived weights index (Pearson's $\alpha = 0.998$; $p < 0.001$). These results indicate that the equal-weighted approach used in constructing the CWEI is not only transparent and easily replicated, but also empirically stable and consistent with data-driven weighting methods. Thus, the indicator selection and weighting scheme in this study have strong methodological validity, making them suitable for use as a tool for policy analysis and strategic planning.

Spatial analysis using Moran's I in Table 9 yielded a high and statistically significant positive value ($I = 0.689$; $p < 0.001$), indicating strong spatial autocorrelation of cyber warfare exposure in Indonesia. This finding indicates that cyber vulnerabilities do not emerge randomly, but rather form organized geographic patterns. This cluster pattern strengthens the argument that spatial factors, such as geographic proximity, infrastructure connectivity, and concentration of economic activity, play a significant role in shaping cyber warfare risk. From a GEOINT perspective, this study confirms that cyber warfare exposure is a spatially mappable, measurable, and predictable phenomenon. A CWEI-based approach allows for the identification of potential vulnerabilities without relying solely on historical cyber incident data, which is often incomplete, classified, or unavailable to independent researchers. A key advantage of this approach lies in its ability to integrate open and measurable indicators, such as critical infrastructure density, digital connectivity levels, and economic activity, into a

systematic analytical framework.

The strategic implications of these findings are significant for national security policy. The concentration of risk in provinces categorized as High and Very High indicates that resources for cyber protection, detection, and response cannot be distributed equitably. Instead, cybersecurity policies and investments need to be prioritized in regions that serve as centers of government, the economy, and the national digital network. Furthermore, identifying key contributors to the CWEI, such as telecommunications and energy infrastructure, provides an empirical basis for formulating more targeted and risk-based policies to protect critical sectors.

From a policy perspective, CWEI exposure classes provide a clear basis for prioritizing cybersecurity interventions. Provinces classified as Very High and High exposure require proactive protection of critical infrastructure, enhanced cyber defense readiness, and continuous threat monitoring. Medium exposure provinces should prioritize capacity building and early-warning systems, while Low exposure regions may focus on baseline cybersecurity standards and resilience planning. This exposure-based prioritization supports efficient allocation of national cybersecurity resources under budget constraints.

Although the research results demonstrate high methodological consistency, this study has a significant limitation: the lack of empirical validation using actual cyberwarfare incident data. Therefore, the CWEI in this study represents potential exposure, not the actual attack rate. Further research is recommended to integrate the limited available cyber incident data and simulated attack scenarios to validate and refine the CWEI model.

3.7 Further Research Directions

Based on the identified limitations, several priority directions for further research are proposed to improve the robustness and applicability of the CWEI. First, empirical validation using observed cyber incident data is a critical research priority. Future studies should seek collaboration with national cybersecurity authorities, military cyber defense units, and private sector stakeholders to access anonymized incident datasets. Such collaboration would enable validation of the CWEI against the frequency and impact of actual attacks, facilitate the development of predictive models for cyber threat forecasting, and support cost-effectiveness analyses of targeted cyber defense interventions.

Second, further research should expand the CWEI beyond infrastructure exposure by integrating cyber defense capacity and resilience indicators. Combining variables related to security operations centers, incident response teams, cybersecurity workforce capacity, vulnerability management practices, and recovery mechanisms would enable the development of a more comprehensive cyber risk index. A combined framework of exposure and defense capacity would improve risk classification and enhance policy relevance for national cyber defense planning.

Third, increasing spatial resolution represents an important methodological extension. While provincial-level analysis is appropriate for strategic assessments, future research should develop district-level or grid-based CWEI models to capture intra-provincial heterogeneity and support operational and tactical decision-making. Such improvements would enable more precise resource allocation and integration with local intelligence.

Fourth, temporal dynamics must be explicitly addressed through longitudinal and dynamic modeling approaches. Developing time-series-based CWEIs, combined with stochastic or agent-based models, will enable researchers to examine exposure trends, simulate cyberattack scenarios, and evaluate policy interventions under different future conditions. Finally, the CWEI framework can be extended for international comparative analysis. Applying the methodology across ASEAN or other regional contexts would enable benchmarking, identification of best practices, and formulation of regional cybersecurity cooperation strategies, thus extending the research's contribution beyond the national scale.

A further limitation relates to spatial aggregation at the provincial level, which may introduce Modifiable Areal Unit Problem (MAUP) effects. Provincial boundaries can obscure intra-provincial heterogeneity in infrastructure density and digital exposure, potentially smoothing localized hotspots. While appropriate for national strategic planning, future studies should consider higher spatial resolutions to mitigate aggregation bias.

4. CONCLUSIONS

This study developed a GEOINT-based Cyber Warfare Exposure Index (CWEI) to assess provincial-level exposure of Indonesia's strategic infrastructure to cyber warfare. Three principal findings emerge. First, exposure is highly concentrated in Java, Bali, and South Sulawesi, with nine provinces classified as High to Very High exposure (CWEI > 0.17). DKI Jakarta recorded the highest value (0.752), followed by West Java, Central Java, and East Java, reflecting the spatial concentration of critical infrastructure, digital activity, and population density. Second, a pronounced west-east disparity was identified, ten provinces in Eastern Indonesia fall into the Very Low category (CWEI < 0.2), with West Sulawesi exhibiting the lowest score (0.019), indicating that exposure strongly aligns with infrastructure intensity and regional digital development gaps. Third, the index demonstrates strong methodological robustness, as PCA-derived weights produced near-identical results to the equal-weighted model (R^2 = 0.997; Pearson r = 0.998), while a significant positive Moran's I ($p < 0.001$) confirms spatial clustering, with Jakarta, Bandung, and Surabaya forming primary hotspots. Overall, the study provides the first spatially explicit, subnational assessment of cyber warfare exposure in Indonesia and offers an empirically grounded framework to support geographically differentiated cybersecurity planning and resource prioritization.

5. ACKNOWLEDGEMENT

This study was conducted as part of an academic assignment under formal academic supervision and was fully self-funded by the author. The author gratefully acknowledges the academic guidance and scholarly feedback provided during the course of the study, as well as editorial and language assistance that contributed to improving the clarity and presentation of the manuscript. Appreciation is also extended to institutions and data providers for making relevant geospatial and statistical datasets publicly accessible. The views and conclusions expressed in this paper are solely those of the author.

REFERENCES

Abrardi, L., S. Comino, and S. Grassini (2025). The Economics of Cyber Risk: A Survey of the Literature. *Journal of Industrial and Business Economics*; 1–35

Adityayuda, A., A. A. Supriyadi, and S. Arief (2024). Development of a Remote Sensing System for Real-Time Detection of Military Threats. In *2024 IEEE Asia-Pacific Conference on Geoscience, Electronics and Remote Sensing Technology (AGERS)*. IEEE, pages 257–268

Aljohani, T. M. (2024). Cyberattacks on Energy Infrastructures as Modern War Weapons-Part I: Analysis and Motives. *IEEE Technology and Society Magazine*, **43**(2); 59–69

Alomari, M. A., M. N. Al-Andoli, M. Ghaleb, R. Thabit, G. Alkawsi, J. A. J. Alsayaydeh, and A. S. A. Gaid (2025). Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. *Energies*, **18**(1); 141

Alqararah, K. (2023). Assessing the Robustness of Composite Indicators: The Case of the Global Innovation Index. *Journal of Innovation and Entrepreneurship*, **12**(1); 61

Anggoro, F., R. E. Caraka, F. A. Prasetyo, M. Ramadhani, P. U. Gio, R.-C. Chen, and B. Pardamean (2022). Revisiting Cluster Vulnerabilities towards Information and Communication Technologies in the Eastern Island of Indonesia Using Fuzzy C Means. *Sustainability*, **14**(6); 3428

APJII Indonesia (2024). Internet Indonesia. Annual Report

Aulianisa, S. S. and I. Indirwan (2020). Lesrev (Lex Scientia Law Review). *Lex Scientia Law Review*, **4**(1); 33–48

Avtar, R., A. Kouser, A. Kumar, D. Singh, P. Misra, A. Gupta, A. P. Yunus, P. Kumar, B. A. Johnson, R. Dasgupta, N. Sahu, and A. B. Rimba (2021). Remote Sensing for International Peace and Security: Its Role and Implications. *Remote Sensing*, **13**(3); 439

Bruno, G., A. Diglio, C. Piccolo, and E. Pipicelli (2023). A Reduced Composite Indicator for Digital Divide Measurement at the Regional Level: An Application to the Digital Economy and Society Index (desi). *Technological Forecasting and Social Change*, **190**; 122461

Chang, T. C., J. H. Tang, and T. C. Chan (2025). Spatiotemporal Impact of Urban Development on Nighttime Light Intensity and Its Hotspot Distribution. *PLoS One*, **20**(6); e0325696

Czuryk, M. (2023). Cybersecurity and Protection of Critical Infrastructure. *Studia Iuridica Lublinensia*, **32**(5); 43–52

Decancq, K. and M. A. Lugo (2013). Weights in Multidimensional Indices of Wellbeing: An Overview. *Econometric Reviews*, **32**(1); 7–34

Elvidge, C. D., K. E. Baugh, M. Zhizhin, and F.-C. Hsu (2013). Why VIIRS Data Are Superior to DMSP for Mapping Nighttime Lights. *Proceedings of the Asia-Pacific Advanced Network*, **35**(0); 62

Gasser, P. (2020). A Review on Energy Security Indices to Compare Country Performances. *Energy Policy*, **139**; 111339

Gibson, J., S. Olivia, and G. Boe-Gibson (2020). Night Lights in Economics: Sources and Uses. *Journal of Economic Surveys*, **34**(5); 955–980

Harknett, R. J. and M. Smeets (2022). Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies*, **45**(4); 534–567

Ibrahim, A., A. Arief, and S. D. Abdullah (2020). Keamanan untuk Penerapan Layanan Publik pada Sistem Pemerintahan Berbasis Elektronik (SPBE): Sebuah Kajian Pustaka Sistematis. *IJIS – Indonesian Journal on Information System*, **5**(2); 135 (in Indonesia)

Jaya, I. G. N. M., S. M. Pahlevi, A. Susenna, L. Agustina, D. Kusumasari, Y. A. A. Sukma, D. Hernikawati, A. A. Rahmi, A. A. Pravitasari, and F. Kristiani (2024). Framework for Monitoring the Spatiotemporal Distribution and Clustering of the Digital Society Index of Indonesia. *Sustainability*, **16**(24); 11258

Kartiasih, F., N. D. Nachrowi, I. D. G. K. Wisana, and D. Handayani (2023). Inequalities of Indonesia's Regional Digital Development and Its Association with Socioeconomic Characteristics: A Spatial and Multivariate Analysis. *Information Technology for Development*, **29**(2–3); 299–328

Lasaiba, M. A. (2022). Perkotaan dalam Perspektif Kemiskinan, Permukiman Kumuh dan Urban Heat Island (Suatu Telaah Literatur). *GEOFORUM*, **1**(2); 63–72 (in Indonesia)

Li, S. and J. Shan (2022). Adaptive Geometric Interval Classifier. *ISPRS International Journal of Geo-Information*, **11**(8); 430

Liu, X., M. Chen, C. Claramunt, M. Batty, M.-P. Kwan, A. M. Senousi, T. Cheng, J. Strobl, A. Cöltekin, J. Wilson, T. Bandrova, M. Konecny, P. M. Torrens, F. Zhang, L. He, J. Wang, C. Ratti, O. Kolditz, A. Klippel, S. Li, H. Lin, and G. Lü (2022). Geographic Information Science in the Era of Geospatial Big Data: A Cyberspace Perspective. *The Innovation*, **3**(5); 100279

Manullang, S. O. (2022). The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws. *Society*, **10**(2); 489–502

Marull, J., M. Farré, M. Andreu Espuña, A. Prior, V. Galletto, and J. Trullén (2023). How to Measure Large-Scale Complex Urban Network Structures Using Night-Time Light Satellite Databases: Application to European Metropolitan Regions. *Environment and Planning B: Urban Analytics and*

City Science, **50**(7); 1947–1963
Marwan, A., D. O.-C. Garduño, and F. Bonfigli (2022). Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia. *BESTUUR*, **10**(1); 22
Maulana, E. D., E. Sumarminingsih, Nurjannah, A. B. Astuti, and S. Astutik (2025). Bayesian IGARCH Modeling of Jakarta Composite Index Volatility Using Hamiltonian Monte Carlo Algorithm. *Science and Technology Indonesia*, **11**(1); 261–279
Nardo, M., M. Saisana, A. Saltelli, S. Tarantola, A. Hoffmanand, and E. Giovannini (2008). Handbook on Constructing Composite Indicators: Methodology and Userguide
OpenStreetMap (2025). Copyright and License. https://www.openstreetmap.org/copyright
Pesaresi, M., M. Schiavina, P. Politis, S. Freire, K. Krasnodębska, J. H. Uhl, A. Carioli, C. Corbane, L. Dijkstra, P. Florio, H. K. Friedrich, J. Gao, S. Leyk, L. Lu, L. Maffenini, I. Mari-Rivero, M. Melchiorri, V. Syrris, J. Van Den Hoek, and T. Kemper (2024). Advances on the Global Human Settlement Layer by Joint Assessment of Earth Observation and Population Survey Data. *International Journal of Digital Earth*, **17**(1); 1–54
Pramono, B. (2025). Strategic Adaptations for Hybrid Warfare: Enhancing Indonesian National Defence in the Digital ERA. *International Journal of Innovative Research and Scientific Studies*, **8**(6); 974–981
Reveron, D. S. and J. E. Savage (2020). Cybersecurity Convergence: Digital Human and National Security. *Orbis*, **64**(4); 555–570
Setiawan, S., A. A. Supriyadi, P. Widodo, and D. A. Navalino (2024). Aerial Photo Database Model of Indonesia's National Territory in a Geospatial Intelligence Perspective. *Journal of Applied and Natural Science*, **16**(2); 637–645
Situmorang, A. C., M. Suryanegara, D. Gunawan, and F. H. Juwono (2023). Proposal of the Indonesian Framework for Telecommunications Infrastructure Based on Network and Socioeconomic Indicators. *Informatics*, **10**(2); 44
Sommer, U., E. Matania, and N. Hassid (2023). The Rise of Companies in the Cyber Era and the Pursuant Shift in National Security. *Political Science*, **75**(2); 140–164
Starovoitov, V. V. and Y. I. Golub (2021). Data Normalization in Machine Learning. *Informatics*, **18**(3); 83–96
Suhadi, Supari, I. Iskandar, M. Irfan, and H. Akhsan (2023). Drought Assessment in Aceh and North Sumatra Using Effective Drought Index. *Science and Technology Indonesia*, **8**(2); 259–264
Venkatachary, S. K., J. Prasad, A. Alagappan, L. J. B. Andrews, R. A. Raj, and S. Duraisamy (2024). Cybersecurity and Cyber-Terrorism Challenges to Energy-Related Infrastructures – Cybersecurity Frameworks and Economics – Comprehensive Review. *International Journal of Critical Infrastructure Protection*, **45**; 100677
Wibowo, A., W. Alawiyah, and Azriadi (2024). The Importance of Personal Data Protection in Indonesia's Economic Development. *Cogent Social Sciences*, **10**(1); 2306751
Wu, R. M., Z. Zhang, W. Yan, J. Fan, J. Gou, B. Liu, E. Gide, J. Soar, B. Shen, S. Fazal-e Hasan, et al. (2022). A Comparative Analysis of the Principal Component Analysis and Entropy Weight Methods to Establish the Indexing Measurement. *PloS one*, **17**(1); e0262261
Yu, Z., H. Gao, X. Cong, N. Wu, and H. H. Song (2023). A Survey on Cyber-Physical Systems Security. *IEEE Internet of Things Journal*, **10**(24); 21670–21686
Zeddini, B., M. Maachaoui, and Y. Inedjaren (2022). Security Threats in Intelligent Transportation Systems and Their Risk Levels. *Risks*, **10**(5); 91
Zheng, M., W. Huang, G. Xu, X. Li, and L. Jiao (2023a). Spatial Gradients of Urban Land Density and Nighttime Light Intensity in 30 Global Megacities. *Humanities and Social Sciences Communications*, **10**(1); 404
Zheng, Q., K. C. Seto, Y. Zhou, S. You, and Q. Weng (2023b). Nighttime Light Remote Sensing for Urban Applications: Progress, Challenges, and Prospects. *ISPRS Journal of Photogrammetry and Remote Sensing*, **202**; 125–141

