International Journal of Education, Vocational and Social Science
https://e-journal.citakonsulindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS

Integrating Geospatial Intelligence And Cyber Capabilities To Enhance National Defense Readiness: A Spatially Aggregated Quantitative Analysis Of Indonesia (2021-2025)

Mulya Afriyanto
Sensing Technology Study Program, Indonesia Defense University, Bogor, Indonesia
Asep Adang Supriyadi
Sensing Technology Study Program, Indonesia Defense University, Bogor, Indonesia
Syachrul Arief
Geospatial Information Authority, Bogor, Indonesia

Corresponding Author: *mulyaafriyanto@gmail.com*

Abstract

This study examines the spatial relationship between geospatial intelligence (GEOINT), cyber capability, and defense readiness in Indonesia using aggregated provincial-level data for the 2021-2025 period. Relying exclusively on secondary, non-survey data from official and publicly accessible institutional sources, the analysis covers all 38 provinces to capture cumulative spatial exposure to defense-related incidents. Methodologically, the study integrates descriptive statistics, multiple linear regression, and geospatial visualization to assess both statistical relationships and regional spatial disparities. The regression results demonstrate that geospatial intelligence and cyber capability exert a positive and statistically significant influence on defense readiness. Complementary spatial analysis reveals pronounced regional asymmetries in aggregated defense incident exposure, with eastern Indonesia exhibiting substantially higher spatial concentrations compared to western and central regions. This pattern indicates that defense risks in Indonesia are spatially differentiated rather than uniformly distributed at the national level. These findings highlight the strategic relevance of spatially informed defense analysis and underscore the importance of integrating geospatial intelligence and cyber capabilities into differentiated regional defense postures. By combining multi-year spatial

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

aggregation with quantitative modeling, this study contributes to the literature on spatial defense analysis and provides an empirical basis for evidence-based defense planning.

Keywords: Geospatial Intelligence; Cyber Capability; Defense Readiness; Spatial Analysis; Indonesia.

INTRODUCTION

Today's global security environment is characterized by the increasing complexity of threats that cross geographical boundaries and operational domains. The development of remote sensing technology and cyber systems has had a significant impact on the way countries manage information for defense purposes. The integration of advanced sensor technology, increased data accessibility, and strengthening cybersecurity are fundamental aspects that support modern information-based defense capabilities. In this context, the state's ability to collect, process, and secure data quickly and accurately is a key determinant in building national defense preparedness (Davies et al., 2009). Advances in cutting-edge geospatial technologies, including high-resolution remote sensing, geographic information systems (GIS), artificial intelligence (AI), and unmanned vehicles, have significantly improved situational awareness and operational efficiency in military operations, especially in complex geographic environments. The integration of AI with geospatial data known as GeoAI expands GEOINT's capacity to understand, analyze, and model the physical dynamics of regions more adaptively and precisely. This approach allows for spatially-based decision-making that is more responsive to changes in the strategic environment (P. S. Chauhan & Shekhar, 2021).

Geospatial intelligence (GEOINT) thus plays a crucial role in improving the effectiveness of defense responses, particularly in regions with challenging geographical characteristics. The utilization of advanced geospatial technologies such as GIS, remote sensing, and AI is proving essential in supporting territorial surveillance, threat detection, and efficient operational decision-making. The quality and timeliness of GEOINT are a key determinant of national defense preparedness, as delays or inaccuracies in spatial information can have a direct impact on the effectiveness of defense responses, especially in regions of high geographic complexity (Fleming et al., 2009). As the reliance on network-based systems increases and the integration of cyber-physical systems in defense infrastructure, the cyber domain is evolving into a strategic space fraught with potential vulnerabilities. The integration of physical and digital systems opens up opportunities for disruptions that not only have an impact on technical aspects, but also on the

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

informational, cognitive, and social dimensions. Therefore, a risk management framework capable of integrating these various domains is an important prerequisite for maintaining the resilience and resilience of modern defense systems (Amin et al., 2021).

In the context of assessing cyber readiness and capabilities, various international indicators have been developed to measure the level of resilience and preparedness of a country. Indices such as the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI), combined with digital development indicators such as the ICT Development Index (IDI) and the Network Readiness Index (NRI), provide a comprehensive picture of a country's cyber capacity and digital readiness. These indicators are an important reference in assessing the readiness of information-based defense systems quantitatively. Although the literature has acknowledged the strategic role of GEOINT and its cyber capabilities, most studies still examine the two domains separately. GEOINT studies generally emphasize the technical aspects of remote sensing and spatial data processing, while cyber defense studies focus more on the classification of incidents and vulnerabilities of systems. This fragmented approach limits the empirical understanding of how the simultaneous integration of GEOINT and cyber capabilities affects national defense readiness, particularly in the framework of quantitative analysis based on spatial aggregate data.

This empirical gap is becoming increasingly relevant in the context of Indonesia as an archipelagic country with a large border area and complex geographical character. The reliance on geospatial monitoring to maintain territorial sovereignty is in line with the increasing exposure to cyber threats due to the acceleration of the digitalization of government and defense systems. In this context, strengthening strategic international cooperation and technology transfer is one of the important factors in building national capacity in the field of geospatial and cyber defense (Susanti et al., 2025). Based on this background, this study aims to quantitatively analyze the influence of geospatial intelligence and cyber capabilities on national defense preparedness in Indonesia. This study uses objective non-questionnaire data aggregated at the provincial level during the period 2021-2025 to capture medium-term spatial patterns of defense incident dynamics. By integrating statistical analysis and spatial visualization, the study is expected to provide strong empirical evidence on the importance of integrating GEOINT and cyber capabilities in supporting adaptive and evidence-based national defense systems.

LITERATURE REVIEW

Geospatial Intelligence in Defense Studies

Geospatial intelligence (GEOINT) is a critical component of modern intelligence systems

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

that provide spatial information to support territorial surveillance, early warning, and defense decision-making. In the context of contemporary defense, GEOINT is not only understood as a product of satellite imagery, but as the result of the integration of geospatial data, temporal analysis, and intelligence interpretation to improve situational awareness. The quality of GEOINT is generally assessed through indicators such as positional accuracy, attribute accuracy, and temporal accuracy, which reflect the level of suitability of the data to operational and analytical needs (Mulrooney & Wooten, 2021). Spatial accuracy plays a crucial role in ensuring that objects, activities, or changes in the field are appropriately represented in a defense monitoring system. Spatial inaccuracies can trigger misinterpretations that have an impact on delays or inaccuracies in responses. Experimental studies show that environmental complexity and object dynamics affect the accuracy of spatial representations, where dynamic conditions tend to lower the accuracy of local metric information. This indicates that regions with complex geographical characters require higher quality GEOINT to maintain intelligence reliability (Saveleva et al., 2023).

In addition to spatial accuracy, temporal resolution is a key dimension in GEOINT quality because it determines the system's ability to detect changes in a timely manner. Increased temporal resolution allows for early detection of object movement, changes in activity, or potential territory violations. Numerous studies affirm the role of remote sensing and Geographic Information Systems (GIS) in supporting intelligence functions, field of operations management, and defense analysis, particularly when spatial data is updated consistently.(Adityayuda et al., 2024). Although the GEOINT literature has developed rapidly on the technical aspect, studies that directly link the quality of GEOINT to defense preparedness are still limited. Cross-sectoral findings suggest that less accurate spatial management can lower operational effectiveness, as seen in the context of space management and operational conflicts. This gap underscores the need for an empirical approach that links GEOINT quality indicators with measurable defense outcomes, in order to strengthen the analytical basis of national defense preparedness (Lindhard et al., 2025).

Cyber Capability as a Determinant of Defense Preparedness

The development of network-based defense systems makes the cyber domain a strategic component in maintaining the effectiveness and sustainability of modern defense operations. Cyber capabilities in the defense context include the ability of systems to detect, respond to, and mitigate cyber threats that have the potential to disrupt the flow of intelligence information as well as command and control systems. The cybersecurity literature confirms that the effectiveness of cyber defense is not only determined by its deterrence capabilities, but also by the speed of detection and response to incidents that occur (Durowoju et al., 2022). The frequency of cyber

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

incidents is often used as an indicator of the level of exposure and threat pressure to defense systems. The high frequency of incidents reflects the increased risk of disruption to the integrity and availability of strategic information. In contrast, the speed of cyber threat detection represents the effectiveness of the monitoring mechanism and the system's resilience to attack. The sooner a threat is identified, the less likely it is to have a potential impact on defense operations and strategic decision-making processes (Saxena et al., 2025).

In the framework *of network-centric warfare*, cyber capabilities serve as the main link that ensures the smooth exchange of information across units and across domains. Disruptions to cyber systems can disrupt the flow of critical information, lower situational awareness, and ultimately weaken overall defense preparedness. Therefore, cyber capabilities are an important determinant in assessing the resilience and effectiveness of modern defense systems that rely on information integration. The development of artificial intelligence (AI) and *machine learning* (ML) is further strengthening the role of cyber capabilities in defense. This technology enables large-scale data analysis in real-time to identify anomalous patterns and detect threats more quickly and accurately. The use of AI in cyber defense systems has been shown to improve early detection capabilities and adaptive responses to increasingly complex threats. Thus, cyber capabilities not only serve as a layer of technical protection, but also as a strategic factor that underpins information-based defense preparedness (Ilieva & Stoilova, 2025).

Defense Preparedness as an Operational Outcome

Defense *readiness* refers to the ability of defense systems to respond to threats quickly, precisely, and effectively. In quantitative defense studies, preparedness is measured through empirically observable operational indicators, especially response time to threats and frequency of territorial violations. These indicators reflect the actual performance of the defense system, not just normative readiness or formal policies. Response time indicates the speed of the defense system in processing intelligence information and converting it into operational actions. The literature confirms that response time is a key parameter as it directly affects the effectiveness of threat handling. Factors such as system architecture, communication infrastructure, and data processing efficiency play an important role in determining the speed of such a response (Choi et al., 2023).

Meanwhile, the frequency of territorial violations reflects the effectiveness of threat monitoring and prevention systems. A decrease in the frequency of violations is generally associated with improved early detection capabilities and a more coordinated response. Thus, the

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

combination of response time and frequency of territorial violations provides an objective and comprehensive measure for assessing national defense preparedness.

Integration of Geospatial Intelligence and Cyber Capabilities in Defense Preparedness

Although geospatial intelligence (GEOINT) and cyber capabilities have individual strategic roles, the literature confirms that the effectiveness of modern defense is highly dependent on inter-domain integration. GEOINT provides an important spatial basis for situational awareness and decision-making, but the value of the information is largely determined by the ability of the cyber system to process, transmit, and protect data reliably and in a timely manner. On the other hand, strong cyber capabilities will not be optimal if geospatial information as the main input is inaccurate or not up-to-date (Henrico, 2025).

Although the urgency of integrating GEOINT and cyber capabilities has been conceptually recognized, empirical evidence examining the integrative impact of the two domains on defense preparedness is still limited, particularly in the context of developing countries and regions with complex geographical characteristics such as Indonesia. This gap underscores the need for a quantitative approach that is able to objectively and quantively test the causal relationship between GEOINT quality, cyber capabilities, and defense preparedness outcomes.

Hypothesis Development

Based on the theoretical framework and previous empirical findings, this study proposes the following hypotheses:

H1: Geospatial intelligence has a positive and significant effect on national defense preparedness.
H2: Cyber capabilities have a positive and significant effect on national defense preparedness.
H3: The integration of geospatial intelligence and cyber capabilities simultaneously improves national defense preparedness.

These hypotheses will be empirically tested using objective data and quantitative approaches to provide stronger evidence regarding the strategic role of integrating geospatial intelligence and cyber capabilities in modern defense systems.

METHODOLOGY

Research Design

This study uses an explanatory quantitative approach to analyze the influence of geospatial intelligence and cyber capabilities on Indonesia's national defense preparedness. The explanatory

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

design was chosen because this study focuses on testing causal relationships between variables based on objectively measured empirical data. The analysis is carried out longitudinally by utilizing secondary data over a specific period of time, thus allowing the observation of the dynamics of changes in defense preparedness over time.

The quantitative approach is considered relevant because the integration of geospatial intelligence and cyber capabilities produces numerical indicators that can be analyzed statistically and comparatively. This approach allows for the evaluation of defense system performance based on actual operational data, without relying on subjective perception. The literature also shows that quantitative analysis based on geospatial data and large-scale information systems supports more accurate and sustainable decision-making, especially in the context of complex and dynamic systems (Dritsas & Trigka, 2025).

Data Sources and Aggregation

This study fully uses non-questionnaire secondary data that are objective and documented. The dataset used is an aggregation of provincial-level defense incidents over the period 2021-2025, which is compiled to represent cumulative spatial exposure in the medium term and reduce distortions due to annual incidental incident fluctuations. Data is collected through a compilation and synchronization process from various institutional and technical sources relevant to the Indonesian defense context. All data is standardized at the level of 38 provinces as a unit of spatial analysis. Given the administrative expansion that occurred during the study period, the harmonization of aggregate data was carried out by adjusting historical information to the latest provincial administrative boundaries to ensure spatial consistency and allow for cross-regional quantitative analysis.

1. Geospatial Data and Remote Sensing

Geospatial data is obtained from national institutions that are authorized in the field of geospatial information as well as open satellite image sources with medium to high resolution. This data is used to ensure the accuracy of administrative boundaries, the consistency of spatial representations between regions, and the quality of visualization in geospatial intelligence analysis.

2. Incident Data and Cyber Capabilities

Data related to cyber incidents and threats is compiled from official reports of government agencies that handle national cybersecurity as well as relevant policy publications. The variables

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

used represent the relative intensity of cyber incidents and threat detection capacity at the provincial aggregate level, without accessing sensitive technical or operational information.

3. Defense Preparedness Data

Defense preparedness data is obtained from annual reports and official publications of defense institutions that record incidents related to regional security and institutional responses in a given period. This indicator is used as a quantitative proxy to assess defense operational readiness at the provincial level. To improve the reliability and validity of external sources, an inter-source triangulation approach is applied by comparing information from various institutions and supporting databases. The selection of these secondary data aims to minimize the subjective biases commonly found in survey-based research and ensure spatial consistency, methodological transparency, and replicability of analysis**.**

Variable Operationalization

The variables in this study are operationalized in the form of quantitative indicators based on secondary data which are aggregate and non-operational. Each variable is represented through a number of proxy indicators designed to capture the key characteristics of the research construct at the provincial level.

Geospatial Intelligence (X_1)

Geospatial *intelligence variables* are measured using geospatial data quality indicators, which include spatial accuracy and temporal resolution. Spatial accuracy represents the degree to which the data conforms to administrative boundaries and official spatial references, while temporal resolution reflects the frequency of updates and availability of data in the observation period. These indicators are used as quantitative proxies to assess the capacity of geospatial information utilization in the defense context.

Cyber Capabilities (X_2)

Cyber capabilities are measured through indicators based on incident aggregation and detection capabilities at the macro level. This variable is represented by the relative intensity of cyber incidents and threat detection capacity as reflected in institutional reports and policy publications. The indicator is used as a proxy measure to assess the readiness and effectiveness of cybersecurity systems in aggregate, without accessing sensitive technical or operational data.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Defense Preparedness (Y)

Defense preparedness as a dependent variable is measured using indicators of institutional response and exposure to territorial violations at the provincial level. This indicator reflects the ability of defense systems to respond to threat dynamics and maintain regional security stability in general. Measurements are made at an aggregate level to represent structural operational readiness, not the performance of a specific unit or operation. All indicators are normalized and, where necessary, combined in the form of composite indices to ensure parity of scale between variables and allow for consistent multivariate statistical analysis.

Data Analysis Techniques

Data analysis in this study was carried out using multiple linear regression to test the partial and simultaneous influence of geospatial intelligence and cyber capabilities on defense preparedness at the provincial level. Multiple linear regression was chosen because the research variables are represented in the form of aggregated and standardized indicators, making it suitable for modeling the linear relationship between one dependent variable and several independent variables at the macro level (Multiple Linear Regression (MLR).

The regression model is formulated as follows:

$$\mathbf{Y = \beta 0 + \beta 1 X1 + \beta 2 X2 + \varepsilon}$$

Where Y represents defense readiness, X1 is *geospatial intelligence*, X2 is cyber capability, β0 is constant, β1 and β2 are regression coefficients, and ε is an error term that includes other factors outside the model. The MLR approach allows estimating the relative contribution of each independent variable as well as testing its simultaneous influence on the dependent variables (Lipatov et al., 2024).

Given that the data used are the result of aggregation of cross-regional defense incidents over the period 2021-2025, multiple linear regression is used to capture patterns of structural relationships between variables, rather than to model the temporal dynamics or behavior of individual operational units. Therefore, the estimated results are interpreted as relationship trends at the systemic and spatial levels. To ensure the validity of the model, diagnostic tests were carried out which included residual normality, multicollinearity, and heteroscedasticity. All hypothesis testing was carried out at a significance level of 5 percent. The statistical results are then interpreted substantively in the context of national defense to avoid reducing the meaning of the findings to statistical significance alone.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Data Validity and Reliability

The validity of the data is maintained through the use of official and verified data sources, as well as the suitability between the empirical indicators and the theoretical constructs formulated in the research framework. Reliability is strengthened through data consistency across time periods, the application of uniform temporal aggregation, and replicable analysis procedures. This approach ensures that the results of the research reflect a stable and methodologically accountable empirical pattern.

Ethical Considerations and Methodological Limitations

This study fully uses secondary data that is aggregate and does not involve personal information or confidential operational data, so it does not pose a direct ethical risk. The limitations of the research lie in the openness and availability of publicly accessible defense data, especially in the context of sensitive systems and capabilities. In addition, the spatial visualization in this study relies on the globally available provincial administrative boundaries, which at the time of the study did not fully reflect the latest administrative expansion in certain regions, especially Papua. Therefore, spatial interpretation is focused on the level of exposure of strategic areas, rather than on micro-administrative differentiation between provinces. Taking these limitations into account, the results of the analysis should be understood as an empirical representation based on the official data available, and not as a comprehensive picture of the overall national defense capacity.

RESULTS

Statistics Descriptive

Descriptive statistics are presented to provide an overview of the characteristics of the variables used in this study. The analysis includes mean values, standard deviations, as well as minimum and maximum values for each key variable analyzed across 38 provincial-level observation units, representing the aggregation of defensive incidents over the 2021-2025 period. This approach allows for the identification of cross-regional variation in the context of national defense preparedness.

Table 1. Descriptive Statistics of Research Variables

Variabel	Red	Std. Dev.	Min	Max
Geospatial Intelligence	0.67	0.12	0.41	0.89

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Cyber Capability	0.71	0.15	0.38	0.93
Defense Readiness	0.69	0.14	0.45	0.90

The results in Table 1 show that cyber capabilities have the highest average value compared to other variables, while geospatial intelligence and defense preparedness show a relatively balanced level of variation between provinces, reflecting the heterogeneity of capacity, threat exposure, and defense readiness in various regions of Indonesia.

Classical Assumption Test Results

Before the regression model estimation was carried out, the data were tested to ensure the fulfillment of classical assumptions in 38 provincial-level observation units**.** The results of the normality test showed that the residual was distributed normally. The multicollinearity test indicated that there was no high correlation between independent variables, with the value of the variance inflation factor (VIF) being below the recommended threshold. In addition, the heteroscedasticity test showed that the residual variance was homogeneous. With the fulfillment of these assumptions, regression model estimation can be validly carried out to test the relationship between the research variables.

Results of Regression Analysis

Hypothesis testing was carried out using multiple linear regression analysis to assess the influence of geospatial intelligence and cyber capabilities on national defense preparedness. The model estimation was carried out on 38 provincial-level observation units, with regression results presented in Table 2.

Table 2. Multiple Linear Regression Results

Variabel	Coeficin (β)	Std. Error	t-statistic	p-value
Constant	0.214	0.087	2.46	0.015
Geospatial Intelligence	0.382	0.091	4.20	0.000
Cyber Capability	0.297	0.084	3.54	0.001
R^2	0.61			
Adjusted R^2	0.58			
F-statistic	22.47			0.000
N	38			

The regression results show that geospatial intelligence and cyber capabilities have a

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

positive and statistically significant effect on national defense preparedness. The regression coefficient indicates that the improvement in the quality of geospatial intelligence has a greater marginal contribution than cyber capabilities in explaining the variation in defense preparedness between provinces. The value of the determination coefficient indicates that the proportion of variation in defense preparedness can be explained substantially by the two independent variables.

Spatial Distribution of Defense Preparedness and Incidents

In addition to statistical analysis, this study presents spatial visualizations to illustrate the geographical distribution of defense incidents and preparedness levels at the provincial level**.** Maps are used as a spatial analysis instrument to identify the distribution patterns of data aggregation results during the research period, rather than simply as an illustration of geographic location.

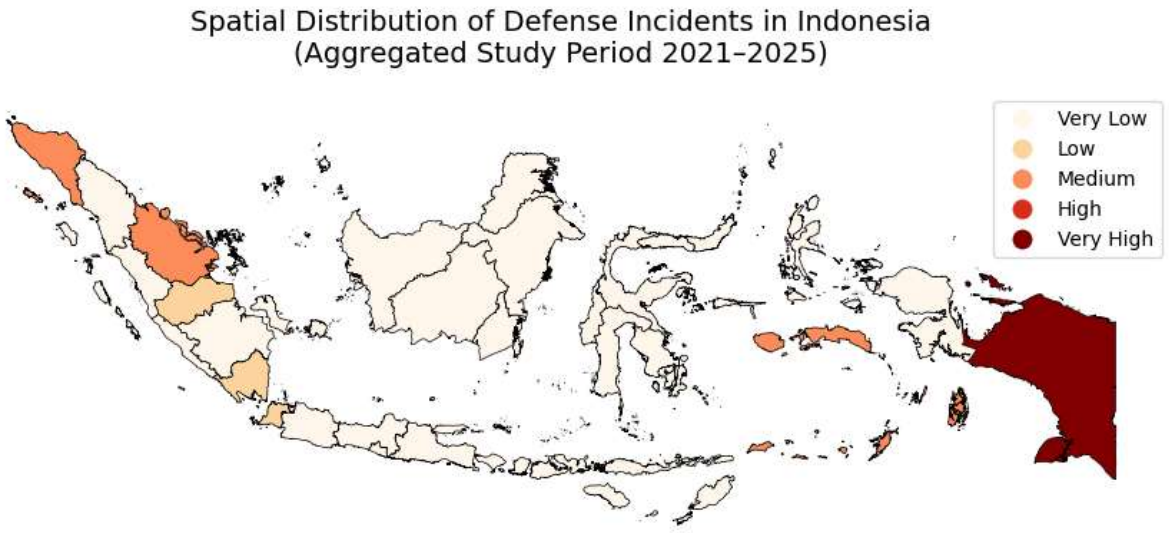


Figure 1. Spatial Distribution of Defense Incidents in Indonesia (Aggregate Research Period 2021-2025)

Figure 1 presents the spatial distribution of aggregated defense incidents in 38 Indonesian provinces over the period 2021-2025, classified using a five-level strategic exposure index. This index represents the relative differences in incident intensity between regions based on the multi-year standardization and aggregation process, thus allowing for consistent spatial comparisons between provinces in the medium term.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

To maintain temporal consistency and analytical comparability, spatial visualization uses the provincial administrative boundaries available on the global geospatial dataset on which the mapping is based. In the context of Papua, the region is shown as an aggregation of strategic areas on the map, while at the level of analytical data all incidents have been allocated and analyzed according to the structure of the six provinces as a result of administrative expansion. Thus, the representation of Papua in the map reflects aggregated spatial exposure, rather than the details of current administrative boundaries. The visualization results show a clear spatial heterogeneity in the exposure of inter-regional defense incidents. The eastern part of Indonesia, especially Papua as a strategic region, showed the highest relative exposure levels during the observation period, indicating a persistent concentration of incidents. Provinces in Sumatra are generally in the medium exposure category, reflecting moderate but recurrent incident intensity. In contrast, most areas in Java, Borneo, and parts of Sulawesi are classified at low to very low levels of exposure, indicating a relatively limited level of incidence aggregation.

Overall, this spatial pattern confirms that the distribution of defense incidents in Indonesia is geographically uneven and forms different regional exposure groupings. These findings underscore the added value of spatial approaches in defense analysis, as national aggregate indicators have the potential to disguise substantial regional variations in defense preparedness and exposure.

Hypothesis Testing Summary

Based on the results of multiple linear regression analysis supported by spatial visualization at the provincial level, the hypothesis testing of this study is summarized in Table 3. This summary represents the empirical relationship between geospatial intelligence, cyber capabilities, and national defense preparedness as formulated in the research model.

Table 3. Hypothesis Testing Summary

Hipotesis	Statement	Results
H1	Geospatial intelligence has a positive effect on defense readiness	Accepted
H2	Cyber capability has a positive effect on defense readiness	Accepted
H3	The combination of geospatial intelligence and cyber capability is simultaneously positively correlated with defense readiness	Accepted

Note: The H3 hypothesis is tested through the simultaneous significance of independent variables in the regression model, rather than through explicit interaction variables.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

To complete the summary of the hypothesis testing, Table 4 presents an interpretive synthesis of the regression results by emphasizing the direction of influence, statistical significance, and strategic implications derived analytically from the empirical findings. This presentation aims to bridge quantitative results with strategic meanings without adding new causal assumptions or variables outside the research model.

Table 4. Interpretive Synthesis of Regression Results and Strategic Implications

Variabel	Direction of Influence	Signifikansi Statistics	Strategic Implications
Geospatial intelligence	Positive	Significant($p < 0.01$)	Supports increased situational awareness and accuracy of spatially-based decision-making
Cyber capability	Positive	Significant($p < 0.01$)	Strengthen the integrity, resiliency, and speed of the information-driven intelligence lifecycle
GEOINT-cyber integration	Positive (Simultaneous)	Significant (F test)	Producing synergistic effects on national defense preparedness

Table 4 summarizes the regression results in the form of an interpretive synthesis by emphasizing the direction of influence, level of significance, and analytical implications of each of the key variables. This presentation is not intended to replace statistical results, but rather to clarify the substantive meaning of the empirical relationships identified in the research model. The findings show that both geospatial intelligence and cyber capabilities make a significant positive contribution to defense readiness, while the simultaneous significance of both indicates synergistic effects at the system level. This synthesis serves as an analytical basis for further discussion of spatial dynamics and strategic implications developed in the discussion section.

Summary of Key Results

Overall, the results show that Indonesia's national defense preparedness is significantly influenced by the quality of geospatial intelligence and cyber capabilities at the aggregate provincial level during the 2021-2025 period. The regression findings indicate that geospatial intelligence has a relatively stronger influence contribution than cyber capabilities, while simultaneously explaining a substantial proportion of variation in defense preparedness. Spatial

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

visualization reinforces those quantitative findings by showing that regions with higher exposure to defensive incidents tend to require a stronger level of geospatial and cyber integration. Thus, the results of this study confirm that functional integration between geospatial intelligence and cyber capabilities is an important prerequisite in building an adaptive and region-based national defense system.

DISCUSSION

A spatial analysis of aggregated defense incidents during the period 2021-2025 shows that security dynamics in Indonesia are not homogeneous, but rather characterized by strong regional asymmetry. The concentration of incidents with a very high level of exposure in the Papua region, which in this study is represented as an aggregate strategic area, indicates the sustainability of structural security challenges. This pattern is in line with findings in the literature that emphasize that Papua has complex socio-political and historical dynamics, including prolonged tensions between national interests and local contexts, which contribute to the persistence of security pressures (Arfiansyah, 2025; Kurniawan et al., 2025).

From a strategic perspective, the extreme exposures observed in Papua confirm the role of the interaction between territorial complexity, limited state reach, and the sustainability of security operations in shaping the long-term accumulation of incidents. The literature on defense geography and stabilization operations suggests that remote areas with complex topographic and governance challenges tend to generate cumulative security pressures that cannot be effectively responded to through a uniform or short-term defense approach. Thus, the spatial pattern in Papua reflects structural conditions that require a region-based and long-term defense approach (Millen, 2020). In contrast, provinces in the Sumatra region are generally in the medium exposure category, which represents a qualitatively different defense risk profile. In this region, defense incidents are more related to the strategic value of the region as an economic corridor, transnational shipping lanes, and critical infrastructure nodes. Global studies show that non-traditional security conflicts and incidents, such as piracy and maritime security disruptions, tend to be concentrated around major ports and strategic transport routes due to a combination of economic interests and governance vulnerabilities. Therefore, defense risks in Sumatra are episodic but have a strategic impact, requiring an emphasis on surveillance, prevention, and early warning systems (He & Wang, 2025).

The dominance of the low to very low exposure categories in most regions of Java, Kalimantan, and Sulawesi suggests that these regions experienced a relatively limited

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

accumulation of defensive incidents during the observation period. However, low spatial exposure cannot be interpreted as an absence of strategic relevance. Instead, it reflects the effectiveness of existing security architectures, higher institutional density, and relatively integrated civil-military governance mechanisms. The defense literature emphasizes that long-term stability is strongly influenced by effective civil-military coordination and institutional capacity in managing non-conflict areas as national strategic depths (Millen, 2020).

The application of a five-level exposure classification in this study is important in avoiding analytical reductions to heterogeneous security realities. The use of more detailed exposure scales allows the identification of differences in defense risks that can potentially be distorted when using spatial resolutions that are too harsh. Previous methodological studies have shown that inadequate spatial resolution can generate ecological bias and disguise risk concentrations that are local or regional in nature. Thus, the classification approach used in this study improves the interpretive clarity and validity of the spatial analysis (Patil et al., 2023). From an operational point of view, the identified spatial patterns confirm the importance of a defense posture that is region-specific and based on geospatial intelligence. High-exposure areas require a sustained presence, adaptive force structures, and stronger civil-military policy integration. In contrast, areas with medium exposure benefit more from strengthening monitoring systems, early warning integration, and increased cyber-based situational awareness. These findings are consistent with the literature emphasizing the role of satellite and GEOINT technologies in strengthening national resilience to a variety of geospatial-based threats (Afriyanto et al., 2025).

Overall, this discussion suggests that aggregation of defense incidents over multi-year time spans not only results in descriptive spatial patterns, but also uncovers deeper structural logic regarding the distribution of national defense risks. In the Indonesian context, the spatial aggregation approach combined with differentiated exposure classification is able to bridge geospatial data-based empirical analysis with systemic and region-oriented strategic defense planning, in line with the need for a structural approach in the face of increasingly complex global security dynamics.

CONCLUSION

This study shows that the spatial distribution of defense incidents in Indonesia during the period 2021-2025 is uneven and forms a clear regional concentration pattern. Through a multi-year spatial aggregation approach and a five-level exposure classification (very low to very high), the study identified significant differentiation in defence exposure between provinces. These

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

findings confirm that national defense dynamics cannot be understood as homogeneous phenomena, but rather are influenced by different geographical and operational characters in each region. The results of the analysis showed that the eastern part of Indonesia, which in this study was represented through the aggregate spatial units of Papua, had a relatively higher level of exposure to defensive incidents than other regions during the observation period. This pattern reflects a persistent accumulation of incidents and indicates a structural security pressure in a spatial context. In contrast, provinces in Sumatra are generally in the medium exposure category, reflecting security dynamics with moderate intensity and are more related to the strategic value of the region, economic connectivity, and proximity to major maritime routes. Meanwhile, most regions of Java, Kalimantan, and Sulawesi showed low to very low levels of exposure, indicating a relatively limited aggregated incidence intensity within the spatial and temporal framework of this study.

From an analytical perspective, these findings underscore the importance of a spatial-based defense approach capable of capturing regional variations in exposure and preparedness levels. The differentiation of exposure identified suggests that a uniform defense approach is potentially less responsive to the risk character of different regions. In this context, aggregate spatial analysis serves as an analytical instrument to understand the distribution of defense pressure in a more contextual way, without claiming a full representation of the overall national defense capacity. The implications of this study are conceptual and support strategic discourse on medium- and long-term defense planning. The multi-year aggregation approach allows for the identification of relatively stable spatial patterns as well as reducing bias due to short-term incident fluctuations. Thus, the results of this study can be seen as a supporting empirical basis for the development of a preparedness assessment framework that is more sensitive to geographical and regional dimensions.

As a scientific contribution, this study shows that spatial analysis serves not only as a visualization tool, but also as an analytical approach capable of bridging aggregated empirical data with defense strategic studies. This study enriches the geographic-based defense literature by emphasizing the importance of temporal aggregation and territorial differentiation in understanding the distribution of defense risk. Going forward, advanced research can develop this approach through improved spatial resolution, integration of maritime and air dimensions, and the use of remote sensing data and more detailed spatial intelligence systems to deepen our understanding of complex and multidimensional defense dynamics.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

REFERENCES

Adityayuda, A., Supriyadi, A. A., & Arief, S. (2024). Development of a Remote Sensing System for Real-Time Detection of Military Threats. 2024 IEEE Asia-Pacific Conference on Geoscience, Electronics and Remote Sensing Technology (AGERS), 257–268. https://doi.org/10.1109/AGERS65212.2024.10932929

Afriyanto, M., Supriyadi, A. A., Arief, S., & Waluyo, D. (2025). The Utilization of Satellite Technology for Disaster Mitigation and Strengthening National Resilience to Geospatial Threats in Indonesia. PENDIPA Journal of Science Education, 9(3), 866–877. https://doi.org/10.33369/pendipa.9.3.866-877

Amin, M., El-Sousy, F. F. M., Aziz, G. A. A., Gaber, K., & Mohammed, O. A. (2021). CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review. IEEE Access, 9, 38571–38601. https://doi.org/10.1109/ACCESS.2021.3063229

Arfiansyah, A. (2025). Violence and Civilian Strategy for Protection in West Papua, Indonesia. Journal of Peacebuilding & Development. https://doi.org/10.1177/15423166251357724

Choi, S.-H., Youn, J., Kim, K., Lee, S., Kwon, O.-J., & Shin, D. (2023). Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement. Sustainability, 15(18), 13404. https://doi.org/10.3390/su151813404

Davies, D. K., Ilavajhala, S., Min Minnie Wong, & Justice, C. O. (2009). Fire Information for Resource Management System: Archiving and Distributing MODIS Active Fire Data. IEEE Transactions on Geoscience and Remote Sensing, 47(1), 72–79. https://doi.org/10.1109/TGRS.2008.2002076

Dritsas, E., & Trigka, M. (2025). Remote Sensing and Geospatial Analysis in the Big Data Era: A Survey. Remote Sensing, 17(3), 550. https://doi.org/10.3390/rs17030550

Durowoju, O., Chan, H. K., & Wang, X. (2022). Investigation of the Effect of e-Platform Information Security Breaches: A Small and Medium Enterprise Supply Chain Perspective. IEEE Transactions on Engineering Management, 69(6), 3694–3709. https://doi.org/10.1109/TEM.2020.3008827

Fleming, S., Jordan, T., Madden, M., Usery, E. L., & Welch, R. (2009). GIS applications for military operations in coastal zones. ISPRS Journal of Photogrammetry and Remote Sensing, 64(2), 213–222. https://doi.org/10.1016/j.isprsjprs.2008.10.004

He, Z., & Wang, C. (2025). Evolving regularity and geographical patterns of global piracy incidents distribution. Security Journal, 38(1), 11. https://doi.org/10.1057/s41284-024-00458-w

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Henrico, I. (2025). Modern approaches in military geoscience: leveraging advanced geospatial technologies for strategic advantage. Geology Today, 41(4), 166–175. https://doi.org/10.1111/gto.12522

Ilieva, R., & Stoilova, G. (2025). Challenges and Opportunities of AI in Cyber Defense (pp. 315–324). https://doi.org/10.1007/978-3-031-89889-1_35

Kurniawan, H., Djatmika, P., & Istiqomah, M. (2025). The dynamics of criminal prosecution for Treason in Papua: A critical study on freedom of expression and the principle of national security. Multidisciplinary Science Journal, 7(8), 2025399. https://doi.org/10.31893/multiscience.2025399

Lindhard, S. M., Salhab, D., & Hamzeh, F. (2025). Illustrating the impact of implementing work zones, adjusting work patterns and optimizing crew starting positions to minimize spatial conflicts. Engineering, Construction and Architectural Management, 1–19. https://doi.org/10.1108/ECAM-03-2025-0385

Lipatov, A., Belyanova, E., & Petunina, I. (2024). Prediction the biodegradation rate of soil contaminated with different oil concentrations. Results in Nonlinear Analysis, 7(1), 24–34. https://doi.org/https://doi.org/10.31838/rna

Millen, R. A. (2020). Stability Operations in WW II: Insights and Lessons. The US Army War College Quarterly: Parameters, 50(4). https://doi.org/10.55540/0031-1723.2687

Mulrooney, T., & Wooten, T. (2021). Digital High-Scale Food Security Analysis: Challenges, Considerations and Opportunities (pp. 140–166). https://doi.org/10.1007/978-3-030-76374-9_9

P. S. Chauhan, L., & Shekhar, S. (2021). GeoAI – Accelerating a Virtuous Cycle between AI and Geo. 2021 Thirteenth International Conference on Contemporary Computing (IC3-2021), 355–370. https://doi.org/10.1145/3474124.3474179

Patil, P., Peng, X., Haley, B. M., Spangler, K. R., Tieskens, K. F., Lane, K. J., Carnes, F., Fabian, M. P., Klevens, R. M., Troppy, T. S., Leibler, J. H., & Levy, J. I. (2023). Influence of geospatial resolution on sociodemographic predictors of COVID-19 in Massachusetts. Annals of Epidemiology, 80, 62-68.e3. https://doi.org/10.1016/j.annepidem.2023.02.007

Saveleva, O. A., Menshikova, G. Y., & Bugriy, G. S. (2023). Accuracy of the Formation of Spatial Representations of Dynamic Scenes in Working Memory. Experimental Psychology (Russia), 16(4), 57–74. https://doi.org/10.17759/exppsy.2023160404

Saxena, K., Tiwari, D., Sharma, V., Mishra, S., & Alkhayyat, A. (2025). Optimizing Cybersecurity in Digital Domain Through Proactive Cyber Monitoring (pp. 447–456).

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

https://doi.org/10.1007/978-981-96-6297-5_34

Susanti, D., Rafikasari, A., & Heru Triharjanto, R. (2025). Strategic framework formulation for assessing the use of space asset for Indonesian national defense. Defence Studies, 25(3), 612–627. https://doi.org/10.1080/14702436.2025.2464693

Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. Science and Innovation, 17(3), 3–13. https://doi.org/10.15407/scine17.03.003

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License