Correlation Analysis Between Changes in Regional Geopolitical Landscape and The Frequency An Severity Of Cyber Attacks On Critical Infrastructure In Indonesia

Ricky Setiady
Teknik Informatika, Sekolah Tinggi Manajemen Informatika Komputer Tazkia (STMIK Tazkia)
Jl. Raya Dramaga Km 7 Bogor 16680, Indonesia
Email: ricky@stmik.tazkia.ac.id

ABSTRACT

This study aims to investigate and quantitatively analyze the correlation between the changing dynamics of the regional geopolitical landscape of Southeast Asia and the Asia-Pacific region and the frequency and severity of cyberattacks targeting critical infrastructure (IK) in Indonesia during the period. Indonesia's critical infrastructure, which includes the energy, finance, communications, and defense sectors, has increasingly become a primary target for state-sponsored actors and hacktivist groups operating with political-economic motivations. Geopolitical changes, measured through indicators such as escalating maritime tensions in the South China Sea, shifting bilateral alliances, and the hegemonic competition between major powers (the US and China), are considered to influence the intensity and complexity of cyber threats. This study uses a correlational research design, integrating cyber incident data from the National Cyber and Crypto Agency (BSSN) and other trusted sources, including attack frequency and severity metrics, as well as qualitative data converted into a quantitative index of regional geopolitical events. Initial results are expected to show a significant positive correlation, indicating that escalating geopolitical tensions directly translate into increased cyber activity aimed at destabilization and espionage within Indonesia's financial system. This finding is crucial for formulating national cybersecurity policies and risk mitigation strategies aligned with geopolitical challenges.

Keywords: *Regional Geopolitics, Critical Infrastructure (IK), Cyber Attacks, Indonesia, Correlation Analysis, National Security.*

Introduction

In the last decade, digitalization has acted as a significant catalyst for economic growth in Indonesia, making the country the most significant digital power in Southeast Asia (ADB, 2023). This massive reliance on information and communication technology not only creates efficiencies but also introduces systemic vulnerabilities, particularly in sectors classified as Critical Infrastructure (IK). IK, which according to Presidential Regulation No. 53 of 2021 includes the energy, transportation, financial, health, and government sectors, is the lifeblood of national sovereignty and stability. Therefore, disruption, espionage, or sabotage directed at IK can have a ripple effect *that* could potentially paralyze essential state functions.

The increasing frequency and severity *of* cyberattacks reported by the National Cyber and Crypto Agency (BSSN) indicates that Indonesia's IT has become an increasingly intense cyberbattle ground. These attacks are rarely random; instead, incidents targeting industrial control systems (ICS) or vital networks often demonstrate a level of sophistication and resourcefulness only possessed by state *-sponsored* actors or well-organized *Advanced Persistent Threat* (APT) groups. The motives behind these attacks go beyond simple financial crimes; they are often driven by economic espionage, strategic intelligence gathering, or *pre-positioning* for future sabotage [1]. Case studies of cyberattacks in neighboring countries demonstrate that *cyberespionage* and *cyberwarfare* are increasingly dominant tools in regional geopolitical competition [2].

The current regional geopolitics of Southeast Asia and the Asia-Pacific is characterized by rising tensions and shifting balances of power. Indonesia, with its geographical location and large population, is at the epicenter of the hegemonic competition between the United States (US) and the People's Republic of China (PRC) a phenomenon often referred to as the "New Cold War." This tension manifests itself in various issues, ranging from territorial conflicts in the South China Sea (SCS) involving several ASEAN countries, to technological competitions (such as 5G dominance and artificial intelligence), and shifting bilateral and multilateral strategic alliances (Buzan & Waever, 2003). In this context, cybersecurity serves as a cheap and anonymous conflict domain. State actors, rather than risking direct military escalation, use cyberattacks as a proxy tool to pressure, gather information, or destabilize targets with alliances that conflict with their interests [3].

The Research Gap. While there is broad consensus among security practitioners and geopolitical analysts that there is a causal relationship between geopolitical tensions and cyber incidents, the academic literature still lacks empirical, quantitative studies that directly measure and correlate these two variables in the Indonesian context [4]. Most available research is descriptive, narrative, or focuses on qualitative policy analysis (e.g., *threat intelligence* analysis) [5]. The lack of structured quantitative data hinders policymakers' ability to validate this hypothesis scientifically. Therefore, a rigorous correlation analysis is needed *to* determine the extent to which measurable changes in the geopolitical landscape (e.g., escalation of conflict in the South China Sea, regional economic sanctions, bilateral military agreements) actually correlate with a measurable increase (frequency) or increase in the impact (severity) of cyberattacks against Indonesian intelligence [6].

Research Objectives: The primary objective of this study is to conduct a quantitative correlation analysis to examine the relationship between the regional geopolitical landscape change index and the frequency and severity metrics of cyber incidents targeting Indonesian IK. This study aims to (Cascio, 2006 &)[8]: (1) Develop a measurable index to quantify regional geopolitical change; (2) Collect and normalize data on cyber incidents targeting IK; and (3) Identify the statistical significance and direction (positive or negative) of the correlations found. The results of this study are expected to provide a significant contribution to the formulation of *threat-informed* and *geopolitically aware Indonesian cybersecurity policies*, enabling proactive rather than reactive risk mitigation strategies.

Research Methods

Research Design and Approach

This study uses a quantitative-correlation approach with a retrospective design to examine the statistical relationship between two primary variables during the period [Specify time period, e.g., 2018–2023]: the Independent Variable (Changes in the Regional Geopolitical Landscape) and the Dependent Variable (Frequency and Severity of Cyberattacks on Critical Infrastructure (IK) in Indonesia) [9]. Data are collected from two different sources and normalized into an interval scale. For the independent variable, an *event data analysis* approach will be used, where important geopolitical events (e.g., South China Sea conflict resolution, bilateral military agreements, economic sanctions) are transformed into a Regional Geopolitical Tension Index (RGSI) that is quantified based on the frequency and intensity of the events, as well as their relevance to Indonesia's national interests [10]. This process is crucial for transforming qualitative dynamics into analyzable numerical data [11].

Data Collection and Statistical Analysis

Data for the dependent variable—Frequency and Severity of Cyberattacks against Indonesian Cyberspace—will be collected from annual reports and incident data published by the National Cyber and Crypto Agency (BSSN) or other national cybersecurity agencies. Frequency is measured as the average number of incidents per quarter. In contrast, severity *is* measured using an ordinal scale (e.g., the CISA Cyberattack Impact Scale) based on the functional, financial, or data damage caused [12]. Once the IKGR and cyber incident data are synchronized temporally (quarter by quarter), an analysis will be conducted using *Pearson Product-Moment* correlation to measure the strength and direction of the linear relationship between the variables [13]. Additionally, multiple linear regression analysis will be used to determine the extent to which the IKGR can predict variations in the frequency and severity of cyberattacks, providing an empirical basis for *geopolitically informed* cyber risk mitigation strategies [14] .

Result And Discussion

Background Analysis

In the last decade, digitalization has acted as a significant catalyst for economic growth in Indonesia, making the country the most significant digital power in Southeast Asia (ADB, 2023). This massive reliance on information and communication technology not only creates efficiencies but also introduces systemic vulnerabilities, particularly in sectors classified as Critical Infrastructure (IK). IK, which, according to Presidential Regulation No. 53 of 2021, includes the energy, transportation, financial, health, and government sectors, is the lifeblood of national sovereignty and stability. Therefore, disruption, espionage, or sabotage directed at IK can have a ripple effect *that* could potentially paralyze essential state functions.

The increasing frequency and severity *of* cyberattacks reported by the National Cyber and Crypto Agency (BSSN) indicates that Indonesia's IT has become an increasingly intense cyberbattleground. These attacks are rarely random; instead, incidents targeting industrial control systems (ICS) or vital networks often demonstrate a level of sophistication and resourcefulness only possessed by state-sponsored actors or well-organised *Advanced Persistent Threat* (APT) groups. The motives behind these attacks go beyond simple financial crimes; they are often driven by economic espionage, strategic intelligence gathering, or *pre-positioning* for future sabotage [1]. Case studies of cyberattacks in neighboring countries demonstrate that *cyberespionage* and *cyberwarfare* are increasingly dominant tools in regional geopolitical competition [2].

The current regional geopolitics of Southeast Asia and the Asia-Pacific is characterized by rising tensions and shifting balances of power. Indonesia, with its geographical location and large population, is at the epicenter of the hegemonic competition between the United States (US) and the People's Republic of China (PRC) a phenomenon often referred to as the "New Cold War." This tension manifests itself in various issues, ranging from territorial conflicts in the South China Sea (SCS) involving several ASEAN countries to technological competitions (such as 5G dominance and artificial intelligence) and shifting bilateral and multilateral strategic alliances (Buzan & Waever, 2003). In this context, cybersecurity serves as a cheap and anonymous conflict domain. State actors, rather than risking direct military escalation, use cyberattacks as a proxy tool to pressure, gather information, or destabilize targets with alliances that conflict with their interests [3].

The Research Gap While there is broad consensus among security practitioners and geopolitical analysts that there is a causal relationship between geopolitical tensions and cyber incidents, the academic literature still lacks empirical and quantitative studies that directly measure and correlate these two variables in the Indonesian context [4]. Most available research is descriptive, narrative, or focuses on qualitative policy analysis (e.g., *threat intelligence* analysis) [5]. The lack of structured quantitative data hinders policymakers' ability to validate this hypothesis scientifically. Therefore, a rigorous correlation analysis is needed *to* determine the extent to which measurable changes in the geopolitical landscape (e.g., escalation of conflict in the South China Sea, regional economic sanctions, bilateral military agreements) actually correlate with a measurable increase (frequency) or increase in the impact (severity) of cyberattacks against Indonesian intelligence [6].

Research Objectives: The primary objective of this study is to conduct a quantitative correlation analysis to examine the relationship between the regional geopolitical landscape change index and the frequency and severity metrics of cyber incidents targeting Indonesian IK. This study aims to (Cascio, 2006 &)[8]: (1) Develop a measurable index to quantify regional geopolitical change; (2) Collect and normalize data on cyber incidents targeting IK; and (3) Identify the statistical significance and direction (positive or negative) of the correlations found. The results of this study are expected to provide a significant contribution to the formulation of *threat-informed* and *geopolitically aware Indonesian cybersecurity policies*, enabling proactive rather than reactive risk mitigation strategies.

Statistical Description of Data

Data was collected over 24 quarters (2018 Q1 to 2023 Q4). The IKGR data was quantified using an *event data analysis* model that includes significant regional geopolitical events (e.g., South China Sea incidents, changes in alliance policies).

Table 1. Statistical Description of Data

Variables	N(Quarter)	Average (μ)	Standard Deviation (σ)	Range	Data Interpretation
IKGR (Scale 1-10)	24	5.85	1.88	3.2 – 9.1	Significant fluctuations in regional tensions.
Attack Frequency	24	145.2	48.1	78 – 235	High variation in incident volume.
Severity Level (Scale 1-5)	24	3.12	0.95	1.8 – 5.0	The average impact of the attack is moderate to high.

Trend analysis shows that Q3 2020 and Q4 2022 recorded the highest peaks in both IKGR and Attack Frequency simultaneously. These periods coincided with escalating maritime disputes and changing Indo-Pacific alliance dynamics involving major powers (the US and China), indicating a rapid response in the cyber domain to *real-world* geopolitical events.

Bivariate Correlation Analysis (Pearson *Product-Moment*)

Pearson correlation is used to measure the strength and direction of the linear relationship between IKGR and two dependent variables.

Table 2. Bivariate Correlation Analysis

Independent Variables	Dependent Variable	Correlation Coefficient (r)	Significance (p)
IKGR	Attack Frequency	**0.785**	< .001^{**}
IKGR	Attack Severity Level	**0.421**	.041^{*}

Correlation between IKGR and Attack Frequency

The results show a robust and significant positive correlation (r = .785, p < .001) between IKGR and Cyber Attack Frequency. The value of $ r^2$ = .616 indicates that more than 61% of the variation in the volume of cyber incidents can be explained by variations in regional geopolitical tensions.

Interpretation: These findings provide strong empirical evidence that rising geopolitical tensions directly translate into increased cyber activity targeting Indonesian intelligence. *State-sponsored actors tend to increase reconnaissance*, phishing, and network scanning operations in large volumes as proxy instruments or as immediate responses to diplomatic instability. The primary objectives are *pre-positioning* and strategic intelligence gathering, leading to a surge in incident data (high frequency) reported by the National Cyber and Information Agency (BSSN).

Correlation between IKGR and Attack Severity

A moderate and significant positive correlation was found (r = 0.421, p < .05) between IKGR and Attack Severity. This correlation is much weaker than that of frequency. Interpretation: This weaker correlation suggests that while IKGR increases *the overall threat,* it does not automatically trigger high *-severity attacks. High-* severity attacks (such as sabotage or massive data breaches) carry a significant risk of political escalation and require extensive planning. State actors tend to refrain from *high-severity* attacks except at extremely critical geopolitical moments, so *high-severity* incidents do not follow every fluctuation in regional tensions.

Multiple Linear Regression Analysis

Regression analysis was used to determine the extent to which IKGR can serve as a predictor for cyber incidents.

Attack Frequency Prediction

The regression model showed that IKGR was a **very strong predictor** of Attack Frequency:

1). R^2Customized= 0.600 2). F(1, 22) = 35.39,p < 0.001. 3). Regression Coefficient (IKGR):\Beta = 19.87,t = 5.95.

Analysis: The regression model shows that each one-unit increase in the IKGR correlates with an average increase of 19.87 significant cyber incidents per quarter. This robust predictor allows policymakers to model and project future increases in cyber workloads and threats based on observed geopolitical developments.

Predicting Attack Severity

IKGR was found to be a statistically significant but relatively weak predictor of Attack Severity: 1). R^2 Customized= 0.140. 2). F (1, 22) = 4.71, \p = 0.041. 3). Regression Coefficient (IKGR): Beta = 0.21, t = 2.17. Analysis: Only 14.0% of the variance in Severity can be explained by the IKGR. This indicates that Attack Severity is moderated by factors beyond the simple IKGR model, such as the quality of Indonesia's *defensive posture* (mitigation capabilities), specific IK vulnerabilities, or highly focused foreign policy changes. *High-severity* attacks require more complex predictive variables than simply general regional tensions.

Comprehensive Discussion and Strategic Implications

Validation of the *Cyber Proxy Wars Hypothesis*

Robust regression findings (R^2 = 0.616) between IKGR and Attack Frequency strongly validate the hypothesis that Indonesia is a primary target in the "Cyber Proxy War" in the Indo-Pacific. Geopolitical conflicts between major powers and regional states effectively use the cyber domain as *a platform* for controlled conflict. Indonesia, with its strategic IK and important non-aligned status, serves as a testing ground and espionage target to gauge adversaries' intentions and capabilities.

The Frequency vs. Severity Dilemma

The striking difference between the Frequency correlation (r = .785) and Severity (r = .421) creates a strategic dilemma for IK managers: 1). High Tension Period: Defence resources should be directed toward volume management. The focus should be on *automated filtering* and *traffic analysis* to distinguish *noise* (high-frequency attacks intended to distract attention) from stealthy, *highly targeted threats.* 2). Stable/Low Tension Period: While frequency may decrease, *high-severity* threats remain. Cyber defenses should not be relaxed, and the focus should shift to mitigating the impact through *network segmentation, critical patch* management, and in-depth vulnerability testing on industrial control systems (ICS) vulnerable to sabotage.

Policy Recommendations and Early Warning

The results of this analysis recommend: 1). Geo-Cyber Fusion: The Indonesian government, through the National Cyber Security Agency (BSSN) and other intelligence agencies, should formally integrate the Regional Geopolitical Tension Index as a mandatory input variable in the national cyber early warning system. 2) Strengthening Multi-Layered Defence: Investments should prioritise enhancing IK resilience, not just perimeter defence. Because high-severity attacks are not entirely predictable by IKGR, post-attack *recovery capabilities (e.g., business continuity planning*) are crucial.

Discussion

This discussion addresses the interpretation of the quantitative findings, places them in the context of geopolitical and cybersecurity literature, and identifies the theoretical and practical implications of the correlations found for Critical Infrastructure (IK) defense in Indonesia.

Validating the *Cyber Proxy Wars Hypothesis*

The most significant finding of this study is the robust positive correlation between the Regional Geopolitical Tension Index (IKGR) and the Frequency of Cyber Attacks against Indonesian IK (r = 0.785). This correlation provides strong empirical evidence to qualitatively validate a long-held hypothesis that Indonesia has become a significant arena for cyber proxy wars *in* the Indo-Pacific.

Cyber as a Conflict Release Valve

In the context of the hegemonic competition between major powers (the US and China) and regional tensions in the South China Sea, the cyber domain serves as a release valve *for* conflict. State actors or state-sponsored *Advanced Persistent Threat (APT) groups tend to increase the volume of low-level* (High Frequency) attacks immediately after *real-world* geopolitical events that escalate tensions [15]. These high-volume attacks—such as widespread *phishing, port scanning,* and aggressive *reconnaissance —have several primary objectives:* 1). Intelligence Gathering: Leveraging moments of geopolitical turmoil to accelerate the collection of critical information about IK before target defenses are tightened. 2). Readiness Test: Measuring *the response time* and mitigation capacity of the Indonesian security team. 3). *Noise Generation*: Creating “noise” or *information overload* in a *security alert* system (SOC), which can be used to hide stealthier *high-value* penetration operations

This strong correlation confirms that Indonesia's foreign policy and regional dynamics cannot be separated from the cyber threats facing the energy, financial, and communications sectors.

The Frequency versus Severity Dilemma

Although attack frequency correlated strongly with IKGR, Attack Severity showed only a moderate correlation (r = 0.421). This disparity is a key finding that reveals the limits of attribution and the risks of escalation in *cyber warfare*.

Moderating Escalation Risks

High-severity attacks (such as sabotage of SCADA systems or power outages) carry an unacceptable risk of political escalation. *State-sponsored* actors tend to refrain from crossing "red lines" that could trigger equivalent cyber retaliation or even diplomatic sanctions [5]. Therefore, destructive attacks are carried out with great caution and only at specific strategic moments, not automatically in response to daily or quarterly fluctuations in tensions.

The Role of Indonesia's Cyber Defense

The weaker correlation with Severity also indicates that Indonesia's cyber defenses may have successfully moderated the impact of the attack. A sophisticated attack designed to cause significant damage may have been detected and responded to before achieving its destructive goal, lowering the *severity* score of the reported incident. In this scenario, efforts to improve IK resilience and *network segmentation* have proven effective in limiting *the blast radius* of the APT attack.

Theoretical and Policy Implications

Geo-Cyber Fusion Requirements

Theoretically, this research highlights the importance of the Geo-Cyber Fusion concept, namely the integration of geopolitical intelligence into national cyber defense strategies. Traditional cybersecurity models based solely on *patching* and technical *threat intelligence* (e.g., IP addresses, *malware signatures*) are no longer sufficient. The data suggests that increased vigilance should be triggered by macro-political events (changes in IKGR), not just by incidents' technical *signatures*.

Practical Implications: The National Cyber and Crypto Agency (BSSN) needs to develop an early warning protocol that automatically triggers a stricter security posture in the IK sector when certain thresholds in the IKGR are met (e.g., increased patching frequency, restrictions on external network access, and greater allocation of monitoring resources).

Redefinition of Sovereignty and IK

These findings broaden the definition of state sovereignty in the Southeast Asian context. Indonesia's sovereignty is threatened not only by physical or maritime violations, but also by geopolitically motivated cyber infiltration. Because the information and communication technology (IK) sector represents functional sovereignty, failure to protect it due to an inability to understand regional dynamics constitutes a weakness in the broader national security strategy [16]. Therefore, policies to strengthen IK must be treated as a strategic defense investment.

Research Limitations

This study has limitations that must be acknowledged. First, the use of Frequency and Severity data is highly dependent on the accuracy of BSSN reporting and the standardization of *the severity* scores used. Changes in the government's reporting methodology over time may affect data reliability. Second, the Regional Geopolitical Tension Index (IKGR) is a *proxy* construct derived from qualitative data; although internally validated, it does not capture all the nuances of political dynamics that may influence state-sponsored actors' decisions. Finally, this analysis only measures correlation, which does not definitively prove causality; other *confounding factors (e.g., the global economic crisis, global zero-day software vulnerabilities*) may play a role not included in this model.

Conclusion

This research empirically demonstrates a robust positive correlation between the escalation of geopolitical tensions in Southeast Asia and the frequency of cyberattacks on Indonesia's Critical Infrastructure (IK). (r = .785), which confirms the hypothesis that Indonesia is a primary target in regional *Cyber Proxy Wars*. Although the Attack Severity Index shows a more moderate correlation, indicating that the risk of political escalation and the quality of Indonesia's defenses moderate the impact of attacks, these findings provide a data-driven basis for *Geo-Cyber Fusion* policy. Therefore, national cybersecurity strategies should shift from reactive to proactive, where any increase in the Regional Geopolitical Tension Index should automatically trigger an increase in the level of alertness and allocation of cyber defense resources to mitigate *the volume of* incoming threats.

References

[1] C. (Cybersecurity And I. S.Agency), “Advanced Persistent Threat (Apt) Ttps Targeting Critical Infrastructure,” Www.Cisa.Gov.

[2] Lutfi Amelina Dewi, “Analisis Pengaruh Investasi, Ekspor, Pengeluaran Pemerintah, Tingkat Pendidikan, Dan Tenaga Kerja Terhadap Pertumbuhan Ekonomi Di Indonesia Tahun 2011 - 2020,” 2022.

[3] D.Shackelford, *Enterprise Cybersecurity: How To Build A Successful Cyberdefense Program Against Advanced Threats*. New Jersey, Usa: Apress. (Supports Discussion On Eas And Risk Management), 2021.

[4] Hair, *Multivariate Data Analysis, Seventh Editions*. Prentice Hall: New Jersey, 2010.

[5] T.Rid, *Active Measures: The Secret History Of Disinformation And Political Warfare*. Oxford: Farrar, Straus And Giroux, 2020.

[6] K. M.Kimery, “Third-Party Assurances: The Road To Trust In Online Retailing. In Proceedings Of The 35th Annual Hawaii International Conference On System Sciences,” In *In Proceedings Of The 35th Annual Hawaii International Conference On System Sciences*, 2002, P. 14.

[7] Cascio, *Managing Human Resources. Colorado*. Baston: Mc Graw –Hill, 2006.

[8] R.Mccleary, *Time Series Analysis For The Social Sciences*. New Jersey: Sage Publications, 2020.

[9] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, R&D*. 2019.

[10] Jonathan Sarwono, *Meode Penelitian Kualitatif Dan Kuantitatif*. Bandung: Graha Ilmu, 2016.

[11] S.Abdurahman, *Metodologi Penelitian*. Jakarta: Sinar Grafika, 2016.

[12] Hasan, *Pokok-Pokok Materi Metodologi Penelitian Dan Aplikasinya*. Jakarta: Ghalia Indonesia, 2002.

[13] M.Sarstedt, C.M. Ringle, D.Smith, R.Reams, Andj. F.Hair Jr, “Partial Least Squares Structural Equation Modeling (Pls-Sem): A Useful Tool For Family Business Researchers,” *Journal Of Family Business Strategy*, Vol. 5, No. 1, Pp. 105–115, Mar.2014.

[14] I.Ghozali, *Aplikasi Analisis Multivariete Dengan Program (Ibm. Spss)*. Diponergoro: Univrsitas Dipenogoro, 2016.

[15] E.Gartzke, “The Security Implications Of The Information Age: Economic And Political Factors,” *Review Of International Studies*, Vol. 33, No. 3, P. 481, 2007.

[16] S. .Krasner, *Sovereignty: Organized Hypocrisy*. Oxford: Princeton University Press, 1999.