

Remote Sensing Big Data Analysis to Enhance Strategic Intelligence Capability in National Security

Hanny Maula Yasien^{1,a,*}, I Gusti Ngurah Bagus Sucitra^{1,b}, Moch. Djatmiko^{2,c}

¹National Intelligence College, Bogor, Indonesia

²Bhayangkara University, Jakarta, Indonesia

^ahannymaulayasien@gmail.com; ^bignsucitra@gmail.com; ^cdjtmiko@ubharajaya.ac.id

*Corresponding author

Article Info

Received: 16-June-2026

Revised: 06-Sept-2026

Accepted: 07-Sept-2026

Keywords

Artificial Intelligence; Big Data Analytics; Cybersecurity; Geospatial Intelligence; National Security; Remote Sensing; Strategic Intelligence

Abstract

The increasing complexity of national security threats in the digital era requires intelligence systems capable of conducting rapid, precise, and predictive analysis. This paper examines how remote sensing big data analysis can enhance strategic intelligence capability in national security by integrating satellite imagery, geospatial data, artificial intelligence, machine learning, deep learning, and cybersecurity mechanisms. Using a qualitative literature review approach, this study analyzes secondary sources from peer-reviewed journals, cybersecurity studies, government-related reports, and technology documents relevant to remote sensing and big data analytics. The findings show that remote sensing big data strengthens strategic intelligence by improving situational awareness, supporting early warning, detecting military and environmental changes, monitoring critical infrastructure, and enabling faster strategic decision-making. However, the effectiveness of this technology depends on data security, system reliability, inter-agency coordination, and the integration of cybersecurity mechanisms such as intrusion detection systems, federated learning, blockchain, and secure data governance. Therefore, remote sensing big data should be developed as an integrated intelligence ecosystem that combines advanced geospatial analytics, real-time data processing, cyber resilience, and institutional coordination to support national security.

1. Introduction

The evolution of national security challenges in the digital era demands intelligence systems capable of rapid, precise, and predictive analysis. As threats become increasingly complex, ranging from environmental degradation and illicit trafficking to geopolitical tensions, modern strategic intelligence must rely on robust data systems. Remote sensing and big data analytics represent critical instruments in this transformation, as remote sensing provides high-resolution geospatial data, while big data analytics enables large-scale information processing and pattern recognition. According to Feng et al. (2022), data quality and availability are critical for the use of big data in remote sensing, particularly to improve threat analysis and predictive modeling. Data obtained from satellite imagery can support intelligence purposes such as monitoring vulnerable areas, detecting military movements, and identifying potential threats to critical infrastructure.

As these technologies evolve, the main challenges lie in providing relevant insights quickly, processing the growing volume of data, and ensuring data security. Systems using advanced technologies, including Charge Frequency Control (CFC) in energy systems, are increasingly vulnerable to cyberattacks that may compromise the integrity and availability of data used in decision-making, as demonstrated by Mohan et al. (2020). Cyberattacks on communication and control infrastructure can lead to data manipulation that

threatens operational security, including in remote sensing-based systems. Therefore, the development of cyberattack defense and detection mechanisms is crucial to ensure that data generated and analyzed remains accurate and reliable for strategic decision-making. Despite its many benefits, the use of big data in remote sensing faces major challenges, with data security remaining a critical component in strategic decision-making (Gheyas & Abdallah, 2016).

The use of big data in remote sensing analysis enables faster and more accurate threat detection, including military movements, environmental changes affecting national stability, and potential threats to critical infrastructure. However, data generated by satellites and sensors remains vulnerable to manipulation and cyberattacks, which can undermine its credibility and effectiveness in strategic intelligence (Feng et al., 2022). While the sophistication of big data can improve threat detection, cybersecurity threats that access or alter strategic data pose a significant risk to national security (Elali & Rachid, 2023). Therefore, data security risk mitigation must become a top priority to ensure that remote sensing and big data analytics can be used safely and efficiently. The processing of large and diverse geospatial data also requires advanced computing systems, such as big data analytics, to support national security monitoring and response (Jia et al., 2023).

According to Guo et al. (2022), the large and continuously growing volume of data is a major challenge in remote sensing data processing, making systems such as Spark GeoPySpark important for handling geospatial data in a parallel and distributed manner. Change detection using satellite imagery also benefits from deep learning and transformation-based models, including the Bitemporal Image Transformer (BIT), which Jia et al. (2023) describe as useful for identifying land-use changes and supporting early warning of ecological risks. In the national security context, this technology can track changes in sensitive areas such as borders and strategic infrastructure with high accuracy. Bukhari et al. (2024) emphasize the importance of Intrusion Detection Systems (IDS) and federated training models to prevent threats to sensor networks while protecting data privacy. In addition, Wang et al. (2022), Chebbi et al. (2021), and Ma et al. (2023) show that big data analytics, deep learning, CNNs, and combined data acquisition methods can accelerate satellite image analysis, improve prediction accuracy, and strengthen strategic intelligence decision-making.

2. Literature Review

2.1. Definition of Remote Sensing Big Data and Strategic Intelligence

Remote sensing big data refers to the integration of satellite imagery, sensor-based geospatial information, and large-scale data analytics to collect, process, and interpret information about objects, areas, or phenomena without direct physical access. In national security, remote sensing provides strategic geospatial data for monitoring military movements, land-use changes, environmental degradation, vulnerable areas, and potential threats to critical infrastructure (Feng et al., 2022). Big data analytics enables large and complex remote sensing datasets to be processed rapidly, allowing intelligence systems to identify patterns, detect anomalies, and support predictive modeling. According to Feng et al. (2022), data quality and availability are critical in remote sensing big data because intelligence analysis depends on accurate, timely, and reliable information. Strategic intelligence can therefore be understood as the systematic use of data, analysis, and prediction to support national security decision-making, in which remote sensing big data strengthens situational awareness, early warning, and threat assessment capabilities.

2.2. Remote Sensing Big Data in Enhancing National Security Intelligence Capability

Remote sensing big data enhances national security intelligence capability by enabling faster and more accurate detection of threats, including military movements, environmental changes, natural disasters, illicit activities, and risks to strategic infrastructure. Wang et al. (2022) explain that big data analytics in remote sensing allows large volumes of satellite imagery to be processed for monitoring changes on the earth's surface that may affect national security. The use of artificial intelligence, machine learning, and deep learning further improves this capability, as Chebbi et al. (2021) state that convolutional neural networks are effective for classifying remote sensing images, detecting objects, and recognizing

patterns in large-scale geospatial datasets. Jia et al. (2023) also highlight that Bitemporal Image Transformer can support change detection and early warning in sensitive areas such as borders, natural reserves, and strategic infrastructure. However, the effectiveness of remote sensing big data depends on secure and reliable systems, because cyberattacks, data manipulation, and unauthorized access can undermine the integrity of intelligence analysis and strategic decision-making (Mohan et al., 2020; Gheyas & Abdallah, 2016).

3. Method

This paper employs a qualitative literature review approach to examine how remote sensing big data analytics can enhance strategic intelligence capability in national security. Data were collected from secondary sources, including peer-reviewed journals, government reports, cybersecurity studies, and technology-related documents relevant to remote sensing, big data analytics, artificial intelligence, and cybersecurity. The analysis was conducted thematically by categorizing the findings into several key domains, namely geospatial intelligence, predictive modeling, AI and deep learning applications, cybersecurity integration, and inter-agency coordination. This method enables the study to synthesize existing knowledge and identify the opportunities, challenges, and strategic relevance of remote sensing big data in supporting threat detection, early warning, and national security decision-making.

4. Results and Discussion

4.1. Remote Sensing Big Data as a Foundation of Strategic Intelligence

Remote sensing big data has become an important foundation for strategic intelligence because it enables the collection and analysis of large-scale geospatial information needed for national security decision-making. Through satellite imagery, aerial sensors, and unmanned systems, intelligence agencies can monitor military movements, border areas, land-use changes, environmental degradation, and potential threats to critical infrastructure. According to Tamiminia et al. (2020), platforms such as Google Earth Engine provide the ability to process geo-big data in real time, allowing decision-makers to obtain critical information more efficiently. This capability is essential because modern threats are increasingly dispersed, dynamic, and difficult to detect through conventional intelligence methods alone. Therefore, remote sensing big data strengthens strategic intelligence by improving situational awareness and expanding the scope of intelligence collection.

The use of remote sensing also supports the identification of environmental and social changes that may affect national stability. For example, satellite-based observation can be used to detect deforestation, urban expansion, water pollution, forest fires, and extreme weather conditions that may trigger food insecurity, migration, or social unrest. Gammans et al. (2025) show that weather and geospatial data from satellites can be used to predict the impact of extreme weather on crop yields, which is closely related to food security and international trade stability. Similarly, Das (2025) highlight the use of geospatial techniques to assess surface water quality, which is relevant for monitoring natural resources and preventing environmental risks. In this context, remote sensing is not only a technical monitoring tool but also a strategic instrument for anticipating non-military threats to national security.

4.2. AI, Machine Learning, and Predictive Threat Detection

The integration of artificial intelligence, machine learning, and deep learning significantly enhances the analytical value of remote sensing big data. These technologies enable intelligence systems to process large satellite datasets, classify images, detect objects, identify anomalies, and recognize patterns that may indicate emerging threats. Chebbi et al. (2021) explain that deep learning and convolutional neural networks are effective techniques for classifying remote sensing images and detecting patterns within large-scale geospatial data. In strategic intelligence, this capability is important because early indicators of threats are often subtle, gradual, and difficult to identify manually. By using AI-supported analysis, intelligence agencies can produce faster, more accurate, and more predictive assessments.

Predictive threat detection can also be strengthened through change detection models and advanced geospatial computing. Jia et al. (2023) describe the use of Bitemporal Image Transformer to identify land-

use changes, particularly in natural reserves and sensitive areas. In national security, this method can be applied to monitor borders, strategic infrastructure, military facilities, protected forests, mining areas, and disaster-prone zones. Guo et al. (2022) further emphasize that systems such as Spark GeoPySpark can process large-scale remote sensing data in a parallel and distributed manner, making geospatial analysis faster and more efficient. These developments show that AI and big data analytics enable intelligence agencies not only to observe current conditions but also to predict possible threat developments.

4.3. Application in National Security and Strategic Decision-Making

Remote sensing big data has practical applications in various domains of national security, including border monitoring, military surveillance, disaster response, environmental security, and protection of critical infrastructure. According to Wang et al. (2022), big data analytics in remote sensing enables the processing of very large satellite image datasets to monitor changes on the earth's surface, such as troop movements or land-use changes that may threaten national security. This capability allows intelligence agencies to detect suspicious activity, assess vulnerable areas, and provide early warning to policymakers. Remote sensing can also support the monitoring of illegal activities, including smuggling routes, illegal mining, illegal logging, and unauthorized movements in border areas. As a result, remote sensing big data improves both the speed and accuracy of strategic decision-making.

The use of unmanned aerial vehicles and hyperspectral imagery further expands the operational value of remote sensing in national security. Partheepan et al. (2023) show that UAVs equipped with remote sensing technology can support early detection of forest fires and enable more effective disaster response. Kwan et al. (2018) emphasize the relevance of hyperspectral imagery for detecting unauthorized movements and environmental changes in border areas. Chierici et al. (2022) also demonstrate that UAV-based detection systems can provide real-time data in hazardous environments, including areas exposed to radiological threats. These examples show that remote sensing big data can support strategic intelligence by providing timely, accurate, and actionable information for national security operations.

4.4. Cybersecurity, Data Integrity, and System Reliability

Despite its strategic benefits, remote sensing big data also creates serious cybersecurity and data integrity challenges. Data collected from satellites, sensors, UAVs, and geospatial platforms is highly sensitive because it may contain information related to military activities, border conditions, critical infrastructure, and national resources. Mohan et al. (2020) explain that cyberattacks on communication and control infrastructure can compromise the integrity and availability of data used in decision-making. If remote sensing data is manipulated, disrupted, or accessed by unauthorized actors, the credibility of intelligence analysis can be undermined. Therefore, data security must become a core requirement in the development of remote sensing-based strategic intelligence systems.

Several cybersecurity mechanisms are needed to protect remote sensing big data from cyber threats. Bukhari et al. (2024) emphasize the importance of Intrusion Detection Systems and federated learning models to detect threats in sensor networks while maintaining data privacy. Federated learning is particularly relevant because it enables model training across decentralized sensor nodes without directly transferring sensitive data. Albakri et al. (2023) also highlight the potential of blockchain in ensuring that data collected from remote sensing platforms remains secure and cannot be altered. By integrating cybersecurity, intrusion detection, federated learning, and blockchain, intelligence systems can improve data reliability and maintain the integrity of strategic decision-making.

4.5. Challenges and Future Direction

The implementation of remote sensing big data for strategic intelligence still faces several challenges, including data volume, processing speed, data integration, spatial-temporal limitations, cybersecurity risks, and inter-agency coordination. Su et al. (2022) note that limitations in spatial resolution and temporal coverage remain a challenge in monitoring large-scale ecological disturbances and recovery. In addition, the integration of data from multiple sources, such as satellites, UAVs, field sensors, open-source geospatial platforms, and government databases, requires strong computing infrastructure and standardized data governance. Technologies such as cloud computing, Apache Hadoop, Apache Spark, and GeoPySpark can help address these challenges by improving the efficiency of large-scale geospatial data processing.

However, technology alone is insufficient without strong institutional coordination and secure information-sharing mechanisms.

Future development should focus on strengthening AI-driven geospatial intelligence, real-time data processing, cybersecurity resilience, and inter-agency integration. The emergence of quantum computing and hybrid quantum-classical models, as discussed by Fan et al. (2023), may accelerate remote sensing image classification and improve predictive analysis. Meanwhile, platforms such as OpenStreetMap can support government mapping and strategic infrastructure monitoring, as highlighted by Sarretta et al. (2023). For national security purposes, the future of remote sensing big data depends on the ability to combine advanced analytics, secure systems, and coordinated intelligence workflows. Therefore, remote sensing big data should be developed as an integrated strategic intelligence ecosystem that supports early warning, threat detection, crisis response, and long-term national security planning.

5. Conclusion

Remote sensing big data analysis is a strategic instrument for enhancing intelligence capability in national security because it enables the collection, processing, and interpretation of large-scale geospatial information in a faster, broader, and more predictive manner. Through satellite imagery, UAVs, aerial sensors, and geospatial platforms, intelligence agencies can monitor border areas, military movements, land-use changes, environmental degradation, natural disasters, and potential threats to critical infrastructure. The integration of big data analytics, artificial intelligence, machine learning, deep learning, and advanced geospatial computing further improves the ability to classify satellite images, detect changes, identify anomalies, and generate early warning. Therefore, remote sensing big data does not merely function as a technical monitoring tool, but also as a foundation for strategic intelligence, situational awareness, predictive threat detection, crisis response, and national security decision-making.

However, the effectiveness of remote sensing big data depends heavily on cybersecurity, data integrity, system reliability, and inter-agency coordination. Data collected from satellites, sensors, UAVs, and geospatial platforms is vulnerable to cyberattacks, manipulation, unauthorized access, and disruption, which may undermine the credibility of intelligence analysis and strategic decision-making. For this reason, cybersecurity mechanisms such as Intrusion Detection Systems, federated learning, blockchain, secure data governance, and protected information-sharing systems must be integrated into remote sensing-based intelligence systems. Future development should focus on building an integrated intelligence ecosystem that combines AI-driven geospatial intelligence, real-time data processing, secure digital infrastructure, human analytical capacity, and coordinated institutional workflows. Thus, the success of remote sensing big data analysis in national security depends not only on technological sophistication, but also on resilience, governance, and institutional integration.

References

- Albakri, A., Alabdullah, B., & Alhayan, F. (2023). Blockchain-assisted machine learning with hybrid metaheuristics-empowered cyber attack detection and classification model. *Sustainability*, 15(18), 13887. <https://doi.org/10.3390/su151813887>
- Bukhari, S. M. S., Zafar, M. H., Houran, M. A., Moosavi, S. K. R., Mansoor, M., Muaaz, M., & Sanfilippo, F. (2024). Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. *Ad Hoc Networks*, 155, 103407. <https://doi.org/10.1016/j.adhoc.2024.103407>
- Chebbi, I., Mellouli, N., Farah, I. R., & Lamolle, M. (2021). Big remote sensing image classification based on deep learning extraction features and distributed Spark frameworks. *Big Data and Cognitive Computing*, 5(2), 21. <https://doi.org/10.3390/bdcc5020021>
- Chierici, A., Malizia, A., Di Giovanni, D., Ciolini, R., & D'Errico, F. (2022). A high-performance gamma spectrometer for unmanned systems based on off-the-shelf components. *Sensors*, 22(3), 1078. <https://doi.org/10.3390/s22031078>
- Das, A. (2025). Surface water quality evaluation of Mahanadi and its tributary Katha Jodi River, Cuttack District, Odisha, using WQI, PLSR, SRI, and geospatial techniques. *Applied Water Science*, 15(2). <https://doi.org/10.1007/s13201-024-02357-2>

- Elali, F. R., & Rachid, L. N. (2023). AI-generated research paper fabrication and plagiarism in the scientific community. *Patterns*, 4(3), 100706. <https://doi.org/10.1016/j.patter.2023.100706>
- Fan, F., Shi, Y., Guggemos, T., & Zhu, X. X. (2023). Hybrid quantum-classical convolutional neural network model for image classification. *IEEE Transactions on Neural Networks and Learning Systems*, 35(12). <https://doi.org/10.1109/TNNLS.2023.3312170>
- Feng, Q., Chen, B., Li, G., Yao, X., Gao, B., & Zhang, L. (2022). A review for sample datasets of remote sensing imagery. *National Remote Sensing Bulletin*, 26(4), 589–605. <https://doi.org/10.11834/jrs.20221162>
- Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics*, 1(6). <https://doi.org/10.1186/s41044-016-0006-0>
- Guo, J., Huang, C., & Hou, J. (2022). A scalable computing resources system for remote sensing big data processing using GeoPySpark based on Spark on K8s. *Remote Sensing*, 14(3), 521. <https://doi.org/10.3390/rs14030521>
- Jia, B., Cheng, Z., Wang, C., Zhao, J., & An, N. (2023). CA-BIT: A change detection method of land use in natural reserves. *Agronomy*, 13(3), 635. <https://doi.org/10.3390/agronomy13030635>
- Kwan, C. (2018). Remote sensing performance enhancement in hyperspectral images. *Sensors*, 18(11), 3598. <https://doi.org/10.3390/s18113598>
- Ma, X., Liu, H., & Peng, Z. (2023). Assimilating a blended dataset of satellite-based estimations and in situ observations to improve WRF-Chem PM2.5 prediction. *Atmospheric Environment*, 319, 120284. <https://doi.org/10.1016/j.atmosenv.2023.120284>
- Mohan, A., Meskin, N., & Mehrjerdi, H. (2020). A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems. *Energies*, 13(15), 3860. <https://doi.org/10.3390/en13153860>
- Nes, K., Schaefer, A., Gammans, M., & Scheitrum, D. P. (2025). Extreme weather events, climate expectations, and agricultural export dynamics. *American Journal of Agricultural Economics*, 107(3), 826–845. <https://doi.org/10.1111/ajae.12505>
- Partheepan, S., Sanati, F., & Hassan, J. (2023). Autonomous unmanned aerial vehicles in bushfire management: Challenges and opportunities. *Drones*, 7(1), 47. <https://doi.org/10.3390/drones7010047>
- Sarretta, A., Napolitano, M., & Minghini, M. (2023). OpenStreetMap as an input source for producing governmental datasets: The case of the Italian Military Geographic Institute. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, XLVIII-4/W7-2023, 193–200. <https://doi.org/10.5194/isprs-archives-xlvi-4-w7-2023-193-2023>
- Su, X., Shen, Y., Zhou, W., Liu, Y., Cheng, H., & Liu, G. (2022). Mapping forest disturbance and recovery for ecological security improvement on the Qinghai-Tibet Plateau: A case study from Three Parallel Rivers Region. *Global Ecology and Conservation*, 33, e01983. <https://doi.org/10.1016/j.gecco.2021.e01983>
- Tamiminia, H., Salehi, B., Mahdianpari, M., Quackenbush, L. J., Adeli, S., & Brisco, B. (2020). Google Earth Engine for geo-big data applications: A meta-analysis and systematic review. *ISPRS Journal of Photogrammetry and Remote Sensing*, 164, 152–170. <https://doi.org/10.1016/j.isprsjprs.2020.04.001>
- Wang, Y., Guo, E., Kang, Y., & Ma, H. (2022). Assessment of land desertification and its drivers on the Mongolian plateau using intensity analysis and the geographical detector technique. *Remote Sensing*, 14(24), 6365. <https://doi.org/10.3390/rs14246365>