Journal of Geographic Information System, 2025, 17(1), 45-65
https://www.scirp.org/journal/jgis
ISSN Online: 2151-1969
ISSN Print: 2151-1950

Exploring Cyber Threat Intelligence into Land Administration Systems for Enhanced Cyber Resilience

Pierre-François Blin[1], Trias Aditya[1*], Purnama Budi Santosa[1], Christophe Claramunt[2]

[1]Department of Geodetic Engineering, Universitas Gadjah Mada, Yogyakarta, Indonesia
[2]Naval Academy Research Institute, Lanvéoc, France
Email: *triasaditya@ugm.ac.id

How to cite this paper: Blin, P.-F., Aditya, T., Santosa, P.B. and Claramunt, C. (2025) Exploring Cyber Threat Intelligence into Land Administration Systems for Enhanced Cyber Resilience. *Journal of Geographic Information System*, **17**, 45-65.
https://doi.org/10.4236/jgis.2025.171003

Received: October 29, 2024
Accepted: December 24, 2024
Published: February 12, 2025

Abstract

The current global cybersecurity landscape, characterized by the increasing scale and sophistication of cyberattacks, underscores the importance of integrating Cyber Threat Intelligence (CTI) into Land Administration Systems (LAS). LAS services involve requests and responses concerning public and private cadastral data, including credentials of parties, ownership, and spatial parcels. This study explores the integration of CTI in LAS to enhance cyber resilience, focusing on the unique vulnerabilities of LAS, such as sensitive data management and interconnection with other critical systems related to spatial data uses and changes. The approach employs a case study of a typical country-specific LAS to analyse structured vulnerabilities and their attributes to determine the degree of vulnerability of LAS through a quantitative inductive approach. The analysis results indicate significant improvements in identifying and mitigating potential threats through CTI integration, thus enhancing cyber resilience. These findings are crucial for policymakers and practitioners to develop robust cybersecurity strategies for LAS.

Keywords

Cyber Threat Intelligence, Common Vulnerabilities and Exposures, Geodata, Land Administration Systems, Risk Assessment, Spatial Cadastral Data

1. Introduction

The current global cybersecurity landscape, characterised by the increasing scale and sophistication of cyberattacks, underscores the importance of integrating Cyber Threat Intelligence (CTI) for proactive and reactive cybersecurity (**Figure 1**) into Land Administration Systems (LAS). Cyberattacks targeting critical infra-

structures, including LAS [1] [2], are increasing, underscoring the urgency of integrating Cyber Threat Intelligence (CTI) into these systems to enhance their cyber resilience [3]-[5]. Although LAS are essential for land management, they are recognized as vulnerable by organizations such as FIG and UN-GGIM. However, there is a lack of specific research on their protection through CTI, highlighting the need for greater focus in this area [6]-[8].

To support LAS functions, a land information system supported by reliable spatial data management is essential. As other spatial data management systems, a land information system comprehends spatial and non-spatial data that includes administrative and legal information on land parcels could also be vulnerable to cyberattacks. A typical land information system implemented in many countries manages critical information, such as property titles, land transactions, and personal information of property owners, making them highly valuable targets for cybercriminals. LASs often integrated with other government and financial systems. Such an integration is not intended to create vulnerabilities but may have the opposite effect creating more vulnerabilities. Many users, including users of government agencies, notaries, and citizens, access LAS, which increases the risk of compromission through stolen credentials or unauthorised access. In addition, many LAS are in the early stages of digital transformation and continue to use outdated technologies that lack the latest security updates. Integration with other systems, multiple access points, reliance on legacy technologies, and the complexity of LAS makes them particularly vulnerable to cyber threats. These factors collectively contribute to the increased risk of data breaches, fraud, and operational disruption. Identifying these specific vulnerabilities underscores the need for robust CTI measures [9] to protect LAS from cyber threats and to ensure the integrity and availability of critical land data. Integrating CTI can bolster the proactive defence mechanisms of LAS, which are critical infrastructures often targeted by cybercriminals [10]. However, the integration of CTI is challenging. The vast volume of source information (opensource or paid) and the difficulty in independently determining relevant cyber threats highlight the need for frameworks capable of effectively analysing and filtering the CTI [11]. The importance of this integration is further emphasised by the increasing digitisation of land administration systems, making them vulnerable to sophisticated cyber threats. This study aimed to explore the integration of CTI into LAS, focusing on the unique vulnerabilities of these systems and providing recommendations for enhancing their cyber resilience.

The short-term objective of this study is to explore specific vulnerabilities within a country-specific LAS and propose actionable measures to enhance their cyber resilience using CTI. The typical cases of a country-specific LAS implementation are the use of a mapping server and geospatial content management. The popular mapping servers are ArcGIS Server and GeoServer. Meanwhile, geospatial content management, such as GeoNode, is more effective than the mapping server. GeoNode manages and visualizes multiple geospatial data sources by em-

ploying several open-source components under a user-friendly interface. By focusing on the structured vulnerabilities associated with geospatial technologies like ArcGIS Server, GeoServer, and GeoNode, this paper seeks to address gaps in existing cybersecurity practices for LAS.

This work builds on previous research and represents the continuation of efforts to strengthen the cybersecurity of LAS in Indonesia [12]. The long-term objectives of this research include improving the cyber resilience of LAS by contributing an interoperable CTI approach between LAS, both digitalised and in the process of digitalization. Internationally, this research aims to provide a technical solution to United Nations initiative to address evolving threats and maintain LAS security [1], supported operationally by the *Office International du Cadastre et du Régime Foncier* (OICRF) and the International Federation of Surveyors (FIG) commissions. Nationally, the results can influence LAS governance to strengthen CTI teams to support their Security Operations Centers (SOC) and Computer Security Incident Response Team (CSIRT) [13]. Developing geomatic CTI within a ISAC geomatics [14], encompassing relevant agency institutions and private companies in a country, is crucial for supporting the country's development [15] [16]. This approach aims to create a collaborative framework that enhances the sharing of threat intelligence and improves the overall security practices within the LAS ecosystem. Achieving these long-term objectives will significantly contribute to the cybersecurity landscape of LAS, ensuring the protection and integrity of land data and supporting the development of secure and resilient land administration systems both nationally and internationally. We explore the cyber resilience of LAS by developing an interoperable CTI framework applicable to LAS at various stages of digitalization. In Indonesia, where this study is focused, the research aims to strengthen the governance of LAS by enhancing the capabilities of CTI teams to support SOC and CSIRT. This approach will establish a collaborative framework for sharing threat intelligence and improving overall security practices within LAS [14]-[19].

2. Context and Background

Recent incidents have demonstrated the susceptibility of LAS to cyberattacks, highlighting the importance of integrating CTI [8]. In 2020, the Spanish land registry was targeted by a ransomware attack that disrupted operations for several days. Similarly, in 2021, the Department of Lands and Surveys of Cyprus was a victim of a cyberattack. Additionally, Estonia integrated blockchain into the land registry after several attacks, and Finland enhanced security measures following the risks identified by the Geospatial Research Institute. These examples illustrate the real-world impact of cyberattacks on LAS, resulting in significant operational disruptions and a need for enhanced security measures. The adoption of technologies such as blockchain in Estonia and improved security protocols in Finland reflects proactive steps taken to mitigate such risks. Learning from these incidents is essential for understanding the potential threats to LAS and the importance of

integrating the CTI to enhance resilience against cyber threats.

The landscape of global cybersecurity, characterised by the increasing scale and sophistication of cyberattacks, underscores the need to integrate CTI into LAS. For instance, the IBM X-Force Threat Intelligence Index report from February 2024 states that nearly 74% of observed attacks targeted critical infrastructures [17]. Additionally, BlackBerry reported that 60% of detected attacks targeted sectors defined as critical infrastructures by various cybersecurity agencies, including networks, energy, finance, healthcare, government, agriculture, and defence [18]. The Critical Infrastructure ISAC also reported that 25% of cyberattacks in Australia targeted critical infrastructures [19]. These statistics highlight the vulnerability of critical infrastructures, including LAS, to cyberattacks. The high percentage of attacks targeting these sectors indicates significant risk and potential impact on essential services and data integrity. Understanding this context is crucial for justifying the need to integrate CTI [20] into LAS, as it directly affects the security and resilience of land administration systems. The vast volume of source information (open-source or paid) and the difficulty in independently determining relevant cyber threats highlight the need for frameworks capable of effectively analysing and filtering CTI [20]. On an international scale, this research aligns with the United Nations Economic Commission for Europe's (UNECE) initiative to address evolving cyber threats and support LAS security globally [2]. However, the immediate impact is intended for local implementation, with international applications considered as a long-term goal. This should be highly considered as all types of attacks, whether they come from local or even international malicious acts, insofar as cyberattacks are increasingly becoming a problem that goes beyond borders.

3. Modelling Approach

Based on the contextual importance and the vulnerabilities in spatial data management that includes land Administration Systems, the research provides a summary related to the interaction between the prevention strategy and response strategy approaches in cyber resilience (proactive vs reactive cyber resilience) in **Figure 1**. **Figure 1** situates Cyber Threat Intelligence (CTI) within the broader framework of cyber resilience, showing how it contributes to both proactive and reactive cybersecurity strategies in LAS. In the proactive phase, CTI enriches risk assessment by providing timely information on emerging threats. In the reactive phase, CTI is strengthened by the Incident Response, which feeds back into the Crisis Management phase, improving long-term resilience.

The figure is based on Disaster Risk Management framework [21] from IFRC (Source: www.ifrc.org). The use of colour adds clarity and makes the distinctions between phases more visually apparent. However, if necessary, the figure can be rendered in black and white without losing its effectiveness. This paper focuses on CTI's cyber threat hunting in the context of proactive cybersecurity. In a proactive cybersecurity approach, response to previous incidents or attacks (e.g., the mani-

pulation of data and privileges throughout the system) can be accommodated as the CTI also feeds the incident response and supports crisis management, which is done during the Risk Assessment phase of Cyber Risk Management (see **Figure 1**). Hence, both proactive and reactive cybersecurity are useful even if we favour one of them in the approach.

The combined use of proactive and reactive strategies is essential for LAS. Like most organizations, proactive cybersecurity in LAS is more cost-effective than responding to incidents after they occur. This balance is necessary to protect critical infrastructure.

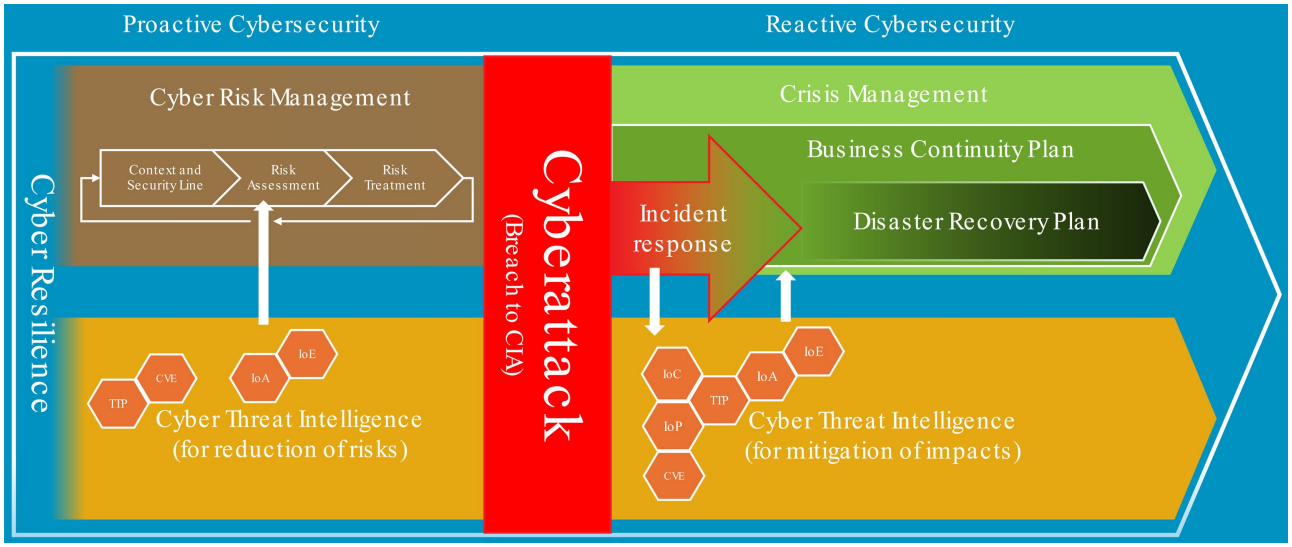

Figure 1. Cyber resilience and the role of CTI for preventive and responsive handling in cyber resilience in spatial data management that include LAS.

The methodology (**Figure 2**) used is a quantitative inductive exploratory approach. This approach explores the vulnerabilities of LAS. For example, we monitored Common Vulnerabilities and Exposures (CVE) [22] and their attributes Common Vulnerability Scoring System (CVSS) [23] and Exploit Prediction Scoring System (EPSS) [24] related to geomatics tools from a precedent cyber risk management EBIOS RM workshop in Indonesian LAS [12]. This mixed exploratory research design captures a comprehensive range of vulnerabilities structured. This includes an analysis of technical and non-technical threats and provides an overview of potential risks. This methodology is suitable for studying CTI in the context of LAS in Indonesia because it draws on best practices from CTI leaders as well as recent research articles in CTI. This contextualises the results into a practical and applicable framework for LAS [24]. We employ an exploratory inductive and quantitative approach, focusing on analysing selected vulnerabilities in LAS through quantitative attributes such as the Common Vulnerability Scoring System (CVSS) and the Exploit Prediction Scoring System (EPSS). These metrics are openly accessible and widely recognized for evaluating the severity and exploitability of vulnerabilities. The method follows a conventional approach, but

the scope of the study is original as it specifically targets vulnerabilities within the Indonesian LAS [25] based on previous research conducted on Land Data and Information Centre (PUSDATIN). The sample for this study is derived from the results of a precedent work [12]. This continuity ensures coherence and builds on established findings. This approach is particularly well-suited to the context of LAS for several reasons.

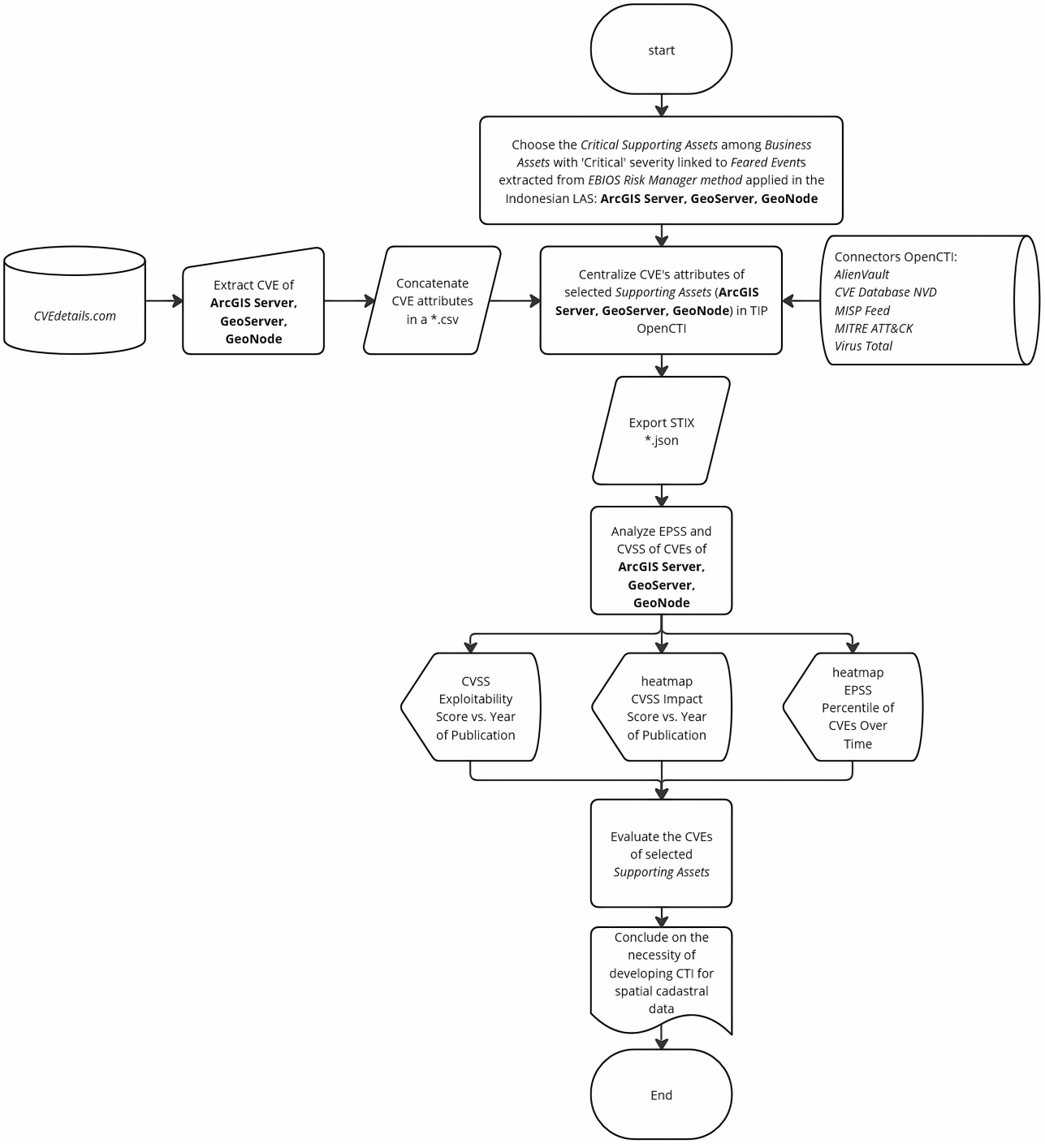

Figure 2. Research method CTI for spatial cadastral data.

1) Continuity with previous research: It builds on the analysis of the PUSDATIN of the Indonesian LAS, ensuring consistency with prior results.

2) Simplicity and Cost-Effectiveness: By relying on publicly available data (CVE details), the method is both cost-efficient and easily replicable.

3) Reproducibility: The approach is designed to be easily replicated across other LAS, making it a useful tool for future research in different contexts.

Figure 2 provides a detailed overview of the study's methodology, breaking down each stage of the analysis process. It is essential to understand the methodological approach, as it visually outlines the steps involved in the exploratory study. The inclusion of this figure was requested by the co-directors to ensure clarity and transparency in the research methodology. Therefore, its presence is crucial for readers to follow the logic of the study. Figure 2 presents the exploratory methodology used in this study. It shows how the selected vulnerabilities were identified, analysed, and mitigated. Together, these elements provide a comprehensive view of both the assets under investigation and the steps taken to assess their vulnerabilities.

The three geomatics LAS tools that were analysed using CTI, are identified in previous research, are considered *Critical Supporting Assets* for the Indonesian LAS. The *Critical Supporting Assets* among *Business Assets* with "Critical" severity linked to *Feared Event*s extracted from *EBIOS Risk Manager method* applied in the Indonesian LAS: ArcGIS Server, GeoServer, GeoNode. The country's LAS encompasses cadastral spatial data mapping and management as well as thematic information systems related to land and natural resource boundaries, provided by ministries other than Agrarian Affairs and Spatial Planning, such as Public Works, Natural Resources, and Forest & Environment. ArcGIS Server, developed by ESRI, is a proprietary platform designed for the creation, management, and distribution of spatial data services, with a particular focus on advanced geospatial analysis and web-based mapping solutions. GeoServer, an open-source counterpart, is widely utilized for publishing geospatial data and is highly valued for its compliance with OGC (Open Geospatial Consortium) standards, ensuring interoperability across diverse systems. GeoNode, which integrates both GeoServer and GeoNetwork, extends these capabilities by offering a comprehensive open-source framework that supports not only geospatial data management but also cataloguing and metadata services, thus facilitating collaborative data sharing. While all three tools are employed for geospatial data management and web services, they differ substantially in their underlying technical architecture, data handling capabilities, and security models. This comparison is essential for identifying system-specific vulnerabilities in Land Administration Systems (LAS). Their role in supporting spatial cadastral data makes them particularly relevant to this study, as vulnerabilities in these tools could have significant impacts on land transaction data integrity.

Specific data analysis techniques are employed to interpret the gathered CTI data. Quantitative data were analysed using descriptive visualisation. The heatmap graph [26] allows for a clear visualisation [27] [28] of the CVE attributes

of our sample, making it easier to identify the criticality of the supporting assets studied. Statistical representation provides a rigorous analysis of quantitative data. Employing these techniques ensures that the analysis is thorough and multidimensional, thus providing a solid foundation for the study's conclusions and recommendations. This study applies descriptive analysis techniques using heat maps to visualize the vulnerabilities of the selected LAS tools. These analyses, inspired by recent works of Trias Aditya, allow for a clear representation of the severity and exploitability of vulnerabilities using metrics such as the CVSS and EPSS scores.

The visual representations (heatmaps) serve two main purposes.

1) Highlighting Vulnerabilities: They explicitly demonstrate the degree of vulnerability in the LAS geomatics tools, which directly impacts Spatial Cadastral Data.

2) Tracking Temporal Changes: The heatmaps also show how the vulnerabilities evolve over time, helping stakeholders monitor the risks and adjust their defences accordingly.

The study uses diverse and reliable sources of structured vulnerabilities data to ensure comprehensive coverage of CTI relevant to LAS. The data sources (**Table 1**) are OpenCTI connectors to CVE database NVD, MISP feed, MITRE ATT&CK, and VirusTotal. The structured vulnerabilities data include also an export. CSV (**Figure 2**) from CVEdetails.com integrates into OpenCTI manually. These sources are recognized in the field of cybersecurity for their reliability and comprehensiveness. By integrating multiple data feeds and enrichment sources, this study can aggregate a wide array of CTI, enhancing the robustness of the analysis. Using reliable and diverse data sources strengthens the validity of the research findings and ensures that the study covers all relevant aspects of CTI for LAS. The data collected for this study were drawn from three key metrics.

1) EPSS Percentile

2) CVSS Impact Score

3) CVSS Exploitability Score

A total of 54 CVEs were analysed, all sourced from CVEdetails.com, an open-access database that aggregates information on known vulnerabilities. For each of the three geomatics LAS tools selected, these metrics were used to assess the severity and exploitability of vulnerabilities. The volume of data allows for a robust analysis of the potential risks to the Indonesian LAS.

The sample for this study was carefully selected to represent the LAS in Indonesia. The sample was derived from the conclusions of a previous risk analysis workshop focusing on maintaining the integrity of SPATIAL cadastral data during parcel subdivision of freehold land. Following the signing of a confidentiality policy with the Indonesian LAS, we cannot disclose the entirety of this document from which our sample is extracted. By basing the sample selection on previous risk analysis findings, the study ensures that the chosen sample is relevant and representative of the key vulnerabilities in LAS. A well-selected sample enhances

Table 1. Sources of data.

Data name sources	Description	References
AlienVault	Imports threat data from the Alien Labs Open Threat Exchange (OTX) platform.	https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/alienvault
CVE database (NVD)	Retrieves vulnerability information from the National Vulnerability Database, maintained by the NIST (National Institute of Standards and Technology)	https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/cve
MISP feed	Integrates threat data from MISP (Malware Information Sharing Platform) feeds to enrich OpenCTI.	https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/misp-feed
MITRE ATT&CK	Retrieves information on tactics, techniques, and procedures (TTPs) from the MITRE ATT&CK database.	https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/mitre
VirusTotal	Enriches existing objects in OpenCTI with information from VirusTotal.	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/virustotal
CVEdetails.com	Provides detailed vulnerability data from the CVEdetails website, integrated into OpenCTI.	https://www.cvedetails.com/

the applicability of the research findings to the broader context of LAS in Indonesia, by using typical software use to disseminate polygon areas represented land use and land allocation boundaries, making the recommendations more actionable. The choice of the OpenCTI Community Edition as the main tool for managing vulnerability data was motivated by several factors.

1) Cost-Effectiveness: OpenCTI is a free and open-source platform, making it an ideal choice for organizations seeking to manage cybersecurity data without incurring additional costs.

2) Leadership in TIP Solutions: OpenCTI is recognized as a leading Threat Intelligence Platform (TIP), providing advanced capabilities for centralizing, and managing dispersed vulnerability data.

The decision to use this tool was based on the need to streamline and centralize vulnerability management in a manner that is both efficient and scalable.

Rigorous processes are implemented to validate the results of the study [29]. The validation process involves using OpenCTI Community Edition to manage and operationalize cyber threat intelligence knowledge and observables, ensuring reliability and validity through trusted sources following the NATO Admiralty system standards. The NATO Admiralty system provides a structured framework for assessing the reliability of sources and the credibility of information [30]. Using OpenCTI's capabilities for managing and validating CTI ensures that the findings are based on high-quality data. Validating the results through established frameworks and reliable tools ensures that the study's conclusions are robust and trustworthy, enhancing their value for policymakers and practitioners.

This study leverages advanced tools and technologies to collect and analyse CTI data. The technological tools used include the OpenCTI Community Edition Threat Information Platform and its connectors to CVE databases and CVE enrichment sources. OpenCTI provides a centralized platform for collecting, correlating, and analysing CTI data, thereby facilitating a comprehensive understanding of the threat landscape. The use of multiple connectors enhances the richness of the data. Utilizing advanced tools like OpenCTI ensures that the study benefits from state-of-the-art capabilities in CTI analysis, making the findings more relevant and actionable. The selection of specific systems for comparison was based on the fact that Land Administration Systems (LAS) are classified as critical infrastructures, similar to sectors like finance and transportation, where Cyber Threat Intelligence (CTI) is already widely implemented. Given the importance of LAS in managing national land assets, the application of CTI to these systems is a logical step to enhance their cybersecurity posture. The comparative analysis underscores the potential benefits of implementing CTI in LAS, drawing parallels with other critical infrastructures where similar strategies have already been successfully deployed. The methodology is compared with existing CTI practices to highlight its strengths and limitations [29]. The CTI of LAS and, more broadly, of geomatics lags behind other sensitive infrastructures. Our methodological approach is inspired by other domains such as the financial and transportation sectors [31], by following the CTI lifecycle [32]. Drawing inspiration from more advanced CTI practices in other sectors allows for the adoption of best practices and innovative techniques. This comparison also helps identify gaps and areas for improvement in the CTI practices for LAS. Comparing the methodology with existing practices ensures that the study adopts proven strategies and highlights areas where LAS CTI practices can be enhanced, contributing to the overall improvement of cybersecurity in this field.

4. Result and Analysis

Our analysis of the country-specific LAS revealed significant vulnerabilities in geospatial tools such as ArcGIS Server, GeoServer, and GeoNode, which are critical for managing cadastral data. These weaknesses expose the systems to potential unauthorized access and data manipulation, threatening the integrity of land administration processes.

The structured vulnerabilities (**Table 2**) identified include specific Common Vulnerabilities and Exposures (CVE) such as CVE-2024-25699 and CVE-2024-25693 for ArcGIS. These CVEs are organised in defined formats, such as CSV, JSON, XML, and STIX [33], and can be easily analysed and processed using security tools. They allow for automated vulnerability management processes and easy integration with vulnerability management systems.

Conversely, unstructured vulnerabilities (**Table 2**) include data not organised in specific formats, often found in free text, such as emails, PDF reports, blog articles, and forums. For example, despite its popularity, the shapefile format

Table 2. Structured vulnerability data and unstructured vulnerability data [34]-[36].

Criteria	Structured vulnerability data	Unstructured vulnerability data
Description	Data organized in a defined format and easily interpretable by machines.	Data not organized in a specific format, often in free text.
Format	CSV, JSON, XML, STIX (Structured Threat Information Expression), BPMN (Business Process Model and Notation).	Emails, PDF reports, blog articles, forums, social networks.
Indicators	CVE (Common Vulnerabilities and Exposures), CPE (Common Platform Enumeration), CVSS (Common Vulnerability Scoring System), EPSS (Exploit Prediction Scoring System).	Discussions on forums, blog posts, tweets, internal notes, articles.
Advantages	(1) Easy to analyse automatically and process with security tools.	(1) Often contains rich contextual information and narrative details.
	(2) Easy integration with vulnerability management systems.	(2) Allows capturing qualitative information and specific insights.
Disadvantages	(1) May lack context or important narrative details.	(1) Difficult to analyse automatically without advanced natural language processing (NLP) techniques.
	(2) Requires regular normalization and updates.	(2) May contain noisy or irrelevant information.
Uses	(1) Automation of vulnerability management processes.	(1) Collection of qualitative information for in-depth analysis.
	(2) Reporting and tracking of vulnerabilities.	(2) Identification of emerging trends and contextual threats.
Analysis tools	(1) TIP (Threat Intelligence Platform) like OpenCTI and MISP.	(1) Natural language processing (NLP) tools, sentiment analysis, search engines.
	(2) Integration of TAXII (Trusted Automated eXchange of Indicator Information) for sharing STIX data.	(2) Use of CTI platforms like OpenCTI and Feedly to aggregate and analyse unstructured data.
Scenario examples	(1) Automatic updating of vulnerability databases.	(1) Monitoring forums and social networks to detect discussions on specific vulnerabilities.
	(2) Use of TTP to identify attacker behaviours.	(2) Follow cybersecurity news and trends.
Maintenance requirements	Must be regularly updated to include new vulnerabilities automatically.	Requires constant monitoring to extract relevant information.
Interoperability	Highly interoperable with security systems and other databases via STIX and TAXII.	Less interoperable, often requires specialized tools for analysis.
Orchestration and automation	Can be integrated into SOAR (Security Orchestration, Automation, and Response) platforms for automated vulnerability management, with generally high integration.	Can feed SOAR (Security Orchestration, Automation, and Response) for automated responses based on contextual analysis, but often requires more complex configuration and integration with automation tools (Zapier, Make, IFTTT).

presents risks because it consists of multiple files, some of which may go unnoticed if they are malicious. File formats incompatible with ArcGIS, such as FlatGeobuf, require converters, such as ogr2ogr, to open doors for malicious activities. Vulnerabilities in QGIS include Python macros embedded in project files, which can execute malicious code if the user accepts execution without caution.

Analysing the CVE databases and incident reports for ArcGIS Server, GeoServer, and GeoNode is relevant, but it is very partial, as it does not cover the threat landscape covered by unstructured vulnerabilities. In our sample of 54 CVEs from ArcGIS Server, GeoServer, and GeoNode, ranging from 2009-09-14 to 2024-08-08, I have preferred only to represent the Percentile EPSS (**Figure 3**) after 2021, considering that those before 2021 are likely to be greatly corrected by the LAS.

Knowing that the EPSS Percentile [37] represents the relative rank of the EPSS score in relation to all evaluated vulnerabilities, (for example, an EPSS percentile of 95% means that the vulnerability is more likely to be exploited than 95% of the other vulnerabilities assessed), one can interpret the moderately exploitable CVEs for ArcGIS Server and GeoNode. In contrast, GeoServer's CVEs are extremes percentiles. Warning, CVE-2024-36401, the latest recently released, has EPSS Score and EPSS Percentile close to the maximum with CVSS3 of 9.8 is highly critical.

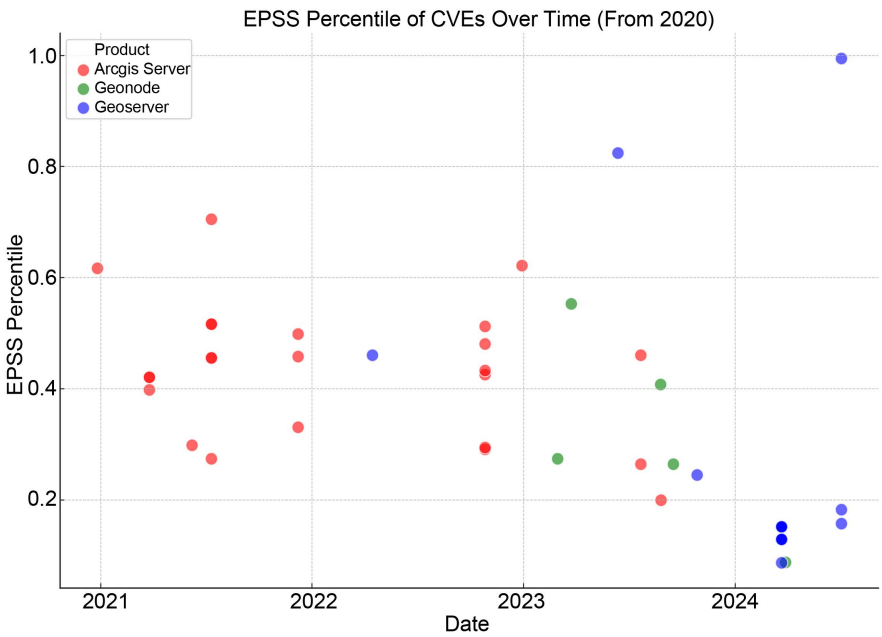

Figure 3. EPSS percentile of CVEs over time (From 2020).

The structured vulnerabilities in our sample have significant impacts, although the majority have CVSS (Common Vulnerability Scoring System) [38], which is less than 4 (**Table 3**).

Knowing that the CVSS Impact Score evaluates the potential damage of a successful exploitation, while the CVSS Exploitability Score (**Figure 4**) evaluates the

ease with which the vulnerability is exploited, we can consider that this impact is easily achievable for an attacker (Figure 5).

Table 3. CVSS ratings.

CVSS score	Severity level	Description	Example of impact	Preventive action of CISO
0.0	None	No vulnerability. The software is secure and presents no known risk.	n/a	n/a
0.1 - 3.9	Low	Minor vulnerability with limited impact. May be exploitable but has minimal and easily manageable consequences.	CVE-2023-25840: This XSS vulnerability in ArcGIS Server versions 10.8.1 to 11.1 allows a remote authenticated attacker to create a link that could potentially render an image in the victim's browser. The privileges required to execute this attack are high, limiting the threat to users with administrative rights, but it remains a serious risk in sensitive environments where these users operate.	Install the "ArcGIS Server Security 2023 Update 1 Patch," restrict access to administrative interfaces, educate users, and monitor access logs for suspicious activity.
4.0 - 6.9	Medium	Moderate vulnerability with notable impact. Requires attention and remediation but is not critical.	CVE-2021-29107: A stored XSS vulnerability in ArcGIS Server Manager versions 10.8.1 and below allows an unauthenticated attacker to inject malicious strings that can be executed by other users, potentially compromising user sessions.	Install the "ArcGIS Server Security 2021 Update 1 Patch," limit access to administrative interfaces, educate users, and monitor logs for suspicious activity.
7.0 - 8.9	High	Significant vulnerability with major impact. Can cause considerable disruptions and requires prompt intervention for remediation.	CVE-2023-51444: This vulnerability in the REST Coverage Store API of GeoServer allows an administrator with limited privileges to exploit this flaw to overwrite security files and gain full administrative privileges.	Update GeoServer to versions 2.23.4 or 2.24.1, restrict access to the REST Coverage Store API, monitor access logs, and implement strict access controls.
9.0 - 10.0	Critical	Extremely severe vulnerability with major consequences. Can lead to complete system compromise and requires immediate remediation.	CVE-2024-36401: This critical vulnerability in GeoServer allows remote code execution (RCE) by unauthenticated users via OGC requests. The attack exploits the incorrect evaluation of property names as XPath expressions, allowing the attacker to execute arbitrary code on the server. This exposes systems to complete compromise, including server control, data breaches, and service disruptions. All GeoServer deployments prior to versions 2.23.6, 2.24.4, and 2.25.2 are vulnerable.	Update GeoServer to the patched versions, apply the workaround by removing gt-complex-x.y.jar if needed, isolate vulnerable systems, and monitor logs for any exploitation attempts.

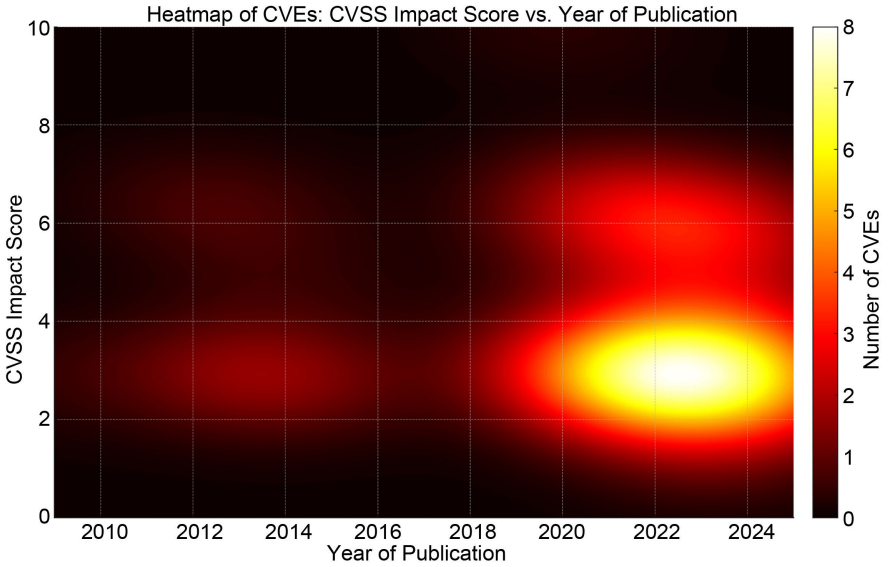

Figure 4. Heatmap of CVEs_CVSS impact score vs. year of publication.

The year of publication in **Figure 4** refers to the date when each CVE was published, ranging from 2010 to 2024. CVSS (Common Vulnerability Scoring System) Impact Scores represent the potential severity or impact of a vulnerability. Higher scores indicate more severe vulnerabilities, with a maximum value of 10. The yellow areas represent a higher number of CVEs, indicating periods where more vulnerabilities with high impact scores were published. The red areas represent a moderate number of vulnerabilities, the less frequent but still notable. The blacker areas, it can be interpreted as periods with either very few or no vulnerabilities published with significant impact scores.

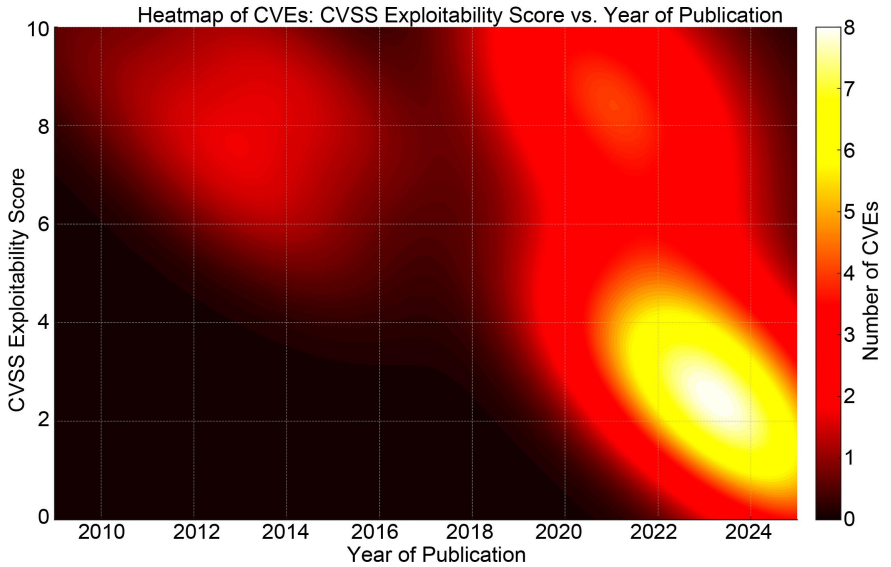

Figure 5. Heatmap of CVEs_CVSS exploitability score vs. year of publication.

The CVSS Impact Score and CVSS Exploitability Score represent distinct aspects

of vulnerability assessment within the Common Vulnerability Scoring System framework. The Impact Score quantifies the potential severity of damage that could ensue if a vulnerability were successfully exploited. Specifically, it reflects the adverse consequences on the system's confidentiality, integrity, and availability. A higher impact score signifies a vulnerability with the capacity to inflict considerable harm to the affected system or network. Conversely, the Exploitability Score evaluates the ease with which a vulnerability can be exploited by an attacker. This score incorporates factors such as the level of access required, the complexity of the attack, and the degree of user interaction necessary for exploitation. A vulnerability with a higher exploitability score is more accessible to attackers, thus posing a greater immediate threat.

The year of publication refers to the specific year in which each CVE was disclosed. This is represented along the X-axis, spanning from 2010 to 2024. CVSS Exploitability Scores quantify the relative ease with which a vulnerability can be exploited. These scores are based on various factors, such as the level of access required, the complexity of the attack, and whether user interaction is necessary for exploitation. A higher exploitability score indicates a vulnerability that is easier for attackers to exploit. The more yellow the region, the greater the concentration of CVEs with high exploitability scores published during that period. Yellow areas represent regions where vulnerabilities with similar exploitability scores are particularly prevalent for cybersecurity of spatial cadastral data. The more reddish the region, the more moderate the number of CVEs present in that particular score and time range. Red areas indicate a significant, though not as dense, presence of vulnerabilities. The blacker the region, it can be interpreted as representing periods or score ranges where few to no vulnerabilities were reported. Black regions suggest an absence or a minimal number of CVEs within that particular score range for the corresponding year.

The overall significance of the results indicates that spatial cadastral data [39] in the LAS are particularly vulnerable to cyberattacks. The diagram and graphs that represent the results could be used to provide practical implementations in developing CTI strategies managed by SOC analyst team for enabling preventive actions in LAS cyber resilience. The findings highlight the crucial need to improve LAS cybersecurity to protect this critical data. For example, from **Figure 3**, we can see that since 2002, the vulnerabilities have mainly concerned opensource products (GeoNode and GeoServer), which suggests that the cybersecurity of ESRI products has improved in the last 3 years. From **Figure 4** and **Figure 5** we can see that the number of CVEs related to these 3 products has increased exponentially from 2019, the majority focusing on the last 3 years in the CVSS Score Medium category, but with high exploitability even if the trend has been decreasing since 2023. By providing a methodology and tools for identifying and managing vulnerabilities, this research significantly contributes to the cybersecurity of LAS.

These results enrich the existing literature by proposing a method and tools to meet the needs of persistent maintenance of cadastral data (PARTY, RIGHTS,

SPATIAL) [40], specifically focusing on spatial cadastral data for this research. Collecting, organizing, and storing the vulnerabilities of LAS strengthens the cybersecurity expertise of specialized teams and increases awareness among the broader LAS workforces. Additionally, by offering detailed insights into the specific vulnerabilities of spatial cadastral data and highlighting both structured and unstructured flaws, this research helps bridge existing gaps in understanding the risks to LAS, providing a solid foundation for future studies and practical improvements.

These results may have practical implications (**Table 4**) at the 3 levels of the CTI: strategic. Operational, tactical [39].

Table 4. Practical implications.

CTI Level	Practical implications	Specific measures to improve LAS security
Strategic	(1) Visualization for a comprehensive understanding of the breadth, height, and depth of the threat.	(1) Rigorously enforce regulatory frameworks and standards.
	(2) Managerial awareness of the LAS's degree of vulnerability.	(2) Allocate budgets to cybersecurity (awareness, training).
	(3) Assists in long-term planning and effective governance implementation.	(3) Decide iterative strategic and operational risk analyses on a recurring basis.
	(4) Necessitates clear governance.	
Operational	(1) Provides quantitative information on threats specific to land administration infrastructures for proactive management.	(1) Implement cybersecurity geomatics training programs for geoprocessing business staff.
	(2) Facilitates the implementation of operational security measures.	(2) Develop partnerships with cybersecurity entities for threat information sharing (ISAC).
	(3) Provides insights for coordinating incident response.	(3) Continuous monitoring of land administration systems to detect suspicious activities (Indicators of Attacks and Indicators of Compromise).
		(4) Implement internal Blue Teaming and Red Teaming actions (Purple teaming).
		(5) Contract external Red Teams.
Tactical	(1) Illuminates in-depth and detailed vulnerabilities of the LAS SDI.	(1) Deploy security patches on assets following the identification of vulnerabilities.
	(2) Enables quick and effective responses to immediate threats and the implementation of specific security measures.	(2) Strengthen the SOC (human recruitment, investment in CTI knowledge management tools).
	(3) Aids in immediate and informed decision-making in response to specific security incidents.	(3) Compose Blue team units.

The validation methods included using reliable data from trusted sources such as NIST, CISA, and MITRE, integrated through OpenCTI. The data were automatically collected and analysed, then clearly and dynamically represented using

the NATO Admiralty [41] standard to evaluate the reliability and credibility of the information. The reliability and validity of the data and analyses were ensured by using OpenCTI connectors to various trusted databases, ensuring that the results are based on reliable and recognized data. The analyses were conducted systematically to ensure an accurate and consistent representation of the identified vulnerabilities, which strengthens the validity of the study's conclusions.

5. Conclusions

This study has identified critical vulnerabilities in typical or country-specific Land Administration Systems (LAS) geomatics tools, underlining the need for stronger CTI knowledge to prioritize the protection of spatial cadastral data. By focusing on the integration of Cyber Threat Intelligence (CTI), this research offers a comprehensive framework for reducing risks and enhancing the cyber resilience of LAS.

The methodology presented in this study is centered on the extraction, analysis, and visualization of Common Vulnerabilities and Exposures (CVEs) related to key geospatial technologies such as ArcGIS Server, GeoServer, and GeoNode. The approach demonstrated here contributes significantly to the existing literature by providing a novel way of integrating CTI into LAS, thereby addressing a major gap in the protection of geospatial data [42].

The scientific contribution of this study lies in the development of a structured methodology for identifying and analysing LAS vulnerabilities using CVSS and EPSS metrics. By leveraging both quantitative and visual analysis, such as heatmaps and timelines, this study enables a clearer understanding of the evolving risk landscape for LAS. These visual tools provide an intuitive means to assess vulnerability trends over time, but more importantly, they facilitate the identification of vulnerabilities with the highest potential impact on critical land administration processes.

On a practical level, the findings of this research have several implications.

1) Strategic Implications: The need for stronger enforcement of security frameworks and the integration of continuous monitoring for identifying emerging vulnerabilities in LAS.

2) Operational Implications: The importance of specialized training programs to ensure that LAS operators are equipped to handle evolving cybersecurity threats.

3) Tactical Implications: The study emphasizes the necessity for real-time threat intelligence and information sharing among LAS through platforms such as ISAC-LAS, or even an ISAC-GEOMATICS dedicated to the spatial data management sector, which can facilitate coordinated responses to shared vulnerabilities. In order to develop strategies to predict more patches for additional issues and to respond quicky before attackers exploit vulnerabilities, owners of LASs could be benefiting from knowledge management investment. The application of CTI for the cadastral sector can be improved by condensing knowledge management on

vulnerabilities and their fixes in order to anticipate attacks and share this knowledge between LAS.

The study's limitations include technical constraints related to the deployment of a fully functional Threat Intelligence Platform (TIP), as well as logistical challenges and cultural reluctance to share critical information between LAS, which may have limited the ability to conduct comprehensive vulnerability scanning. Moreover, the analysis of unstructured vulnerabilities remains incomplete due to the absence of threat hunting techniques and text-based processing methodologies.

Future research should address these limitations by focusing on:

1) Fostering collaboration between the SOCs of different LAS through interconnected TIPs to ensure the exchange of common vulnerabilities.

2) Developing Cyber Threat Hunting capabilities to complement CTI of LAS efforts by proactively identifying unstructured vulnerabilities across various levels of the internet. This will allow for the discovery of a wider range of threats, thereby enhancing the security posture of LAS.

In conclusion, this study highlights the pivotal role of CTI in the proactive protection of LAS against cyber threats. The findings not only provide a solid methodological foundation for integrating CTI into LAS but also present a roadmap for future advancements in LAS and geomatics cybersecurity. By adopting the recommendations of this research, LAS can significantly improve its resilience to cyber threats, ensuring the integrity and security of critical cadastral data. Continuous improvement and enhanced collaboration between LAS and cybersecurity platforms will be key to sustaining these efforts in the future.

Acknowledgements

We thank CVEdetails.com and OpenCTI for providing free access to their data sources. We are also grateful to UGM for funding the PhD and covering the article submission fees.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] United Nations (2022) United Nations Economic Commission for Europe Scenario Study on Future Land Administration in the UNECE Region.

[2] FAO, UNECE, FIG, Bennett, R., Stöcker, C. and Asiama, K. (2022) Digital Transformation and Land Administration. FAO, UNECE (United Nations Economic Commission for Europe).

[3] Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H. and Almuhaideb, A.M. (2023) A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, **23**, Article 7273. https://doi.org/10.3390/s23167273

[4] Sahrom Abu, M., Rahayu Selamat, S., Ariffin, A. and Yusof, R. (2018) Cyber Threat

Intelligence—Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, **10**, 371-379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

[5] Salvi, A., Spagnoletti, P. and Noori, N.S. (2022) Cyber-Resilience of Critical Cyber Infrastructures: Integrating Digital Twins in the Electric Power Ecosystem. *Computers & Security*, **112**, Article ID: 102507. https://doi.org/10.1016/j.cose.2021.102507

[6] Samtani, S., Zhao, Z. and Krishnan, R. (2023) Secure Knowledge Management and Cybersecurity in the Era of Artificial Intelligence. *Information Systems Frontiers*, **25**, 425-429. https://doi.org/10.1007/s10796-023-10372-y

[7] Berady, A., Tong, V.V.T., Guette, G. and Jaume, M. (2021) Caractérisation Tactique d'un Attaquant Évoluant Dans Un Réseau Compromis. *Journée thématique du GT SSLR*. https://gtsslr21-reseau.sciencesconf.org/353075

[8] Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M. and Foo, E. (2024) Current Approaches and Future Directions for Cyber Threat Intelligence Sharing: A Survey. *Journal of Information Security and Applications*, **83**, Article ID: 103786. https://doi.org/10.1016/j.jisa.2024.103786

[9] Aljuhami, A.M. and Bamasoud, D.M. (2021) Cyber Threat Intelligence in Risk Management. *International Journal of Advanced Computer Science and Applications*, **12**, 156-164. https://doi.org/10.14569/ijacsa.2021.0121018

[10] Saxena, R. and Gayathri, E. (2022) Cyber Threat Intelligence Challenges: Leveraging Blockchain Intelligence with Possible Solution. *Materials Today: Proceedings*, **51**, 682-689. https://doi.org/10.1016/j.matpr.2021.06.204

[11] Li, J. (2018) Cyber Security Meets Artificial Intelligence: A Survey. *Frontiers of Information Technology & Electronic Engineering*, **19**, 1462-1474. https://doi.org/10.1631/fitee.1800573

[12] Blin, P., Aditya, T., Santosa, P.B. and Claramunt, C. (2023) A Methodological Approach Towards Cyber Risk Management in Land Administrations Systems. *Land*, **13**, Article 19. https://doi.org/10.3390/land13010019

[13] Skytterholm, A.N. and Jaatun, M.G. (2023) Exploring the Need for a CERT for the Norwegian Construction Sector. In: Onwubiko, C., *et al*., Eds., *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*, Springer, 57-73.

[14] Sholihah, I.M., Setiawan, H. and Nabila, O.G. (2021) Design and Development of Information Sharing and Analysis Center (ISAC) as an Information Sharing Platform. 2021 *Sixth International Conference on Informatics and Computing* (*ICIC*), Jakart 3-4 November 2021, 1-6. https://doi.org/10.1109/icic54025.2021.9632989

[15] Aditya Putra, F. (2022) Tata Kelola Ekosistem Berbagi Informasi Keamanan Siber pada Information Sharing and Analysis Center (ISAC) Sektor Pemerintah Daerah di Indonesia. *Info Kripto*, **16**, 23-32. https://doi.org/10.56706/ik.v16i1.39

[16] Wallis, T. and Leszczyna, R. (2022) EE-ISAC—Practical Cybersecurity Solution for the Energy Sector. *Energies*, **15**, Article 2170. https://doi.org/10.3390/en15062170

[17] (2024) IBM X-Force Threat Intelligence Index 2024 Synthèse. https://www.ibm.com/downloads/cas/XQMYXR4A

[18] Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC) (2022) Annual Cyber Threat Report 2022.

[19] Halima Ibrahim, K. (2024) Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. https://www.jucs.org/jucs_25_11/cyber_threat_intelligence_for/jucs_25_11_1478_1502_kure.pdf

[20] Khafian, N. (2023) The Role of Collaborative Governance in Indonesian Disaster Management. *Journal of Governance and Administrative Reform*, **4**, 158-175. https://doi.org/10.20473/jgar.v4i2.53367

[21] Singh, G.P., Bharti, V. and Hooda, M.K. (2022) An Analysis of Common Vulnerabilities and Exposures in View of MITRE ATT&CK. *Asian Journal of Convergence in Technology*, **8**, 15-17. https://doi.org/10.33130/ajct.2022v08i02.004

[22] Machalewski, T., Szymanek, M., Czubak, A. and Turba, T. (2024) Expressing Impact of Vulnerabilities: An Expert-Filled Dataset and Vector Changer Framework for Modelling Multistage Attacks, Based on Cve, Cvss and Cwe. *ECMS* 2024 *Proceedings*, Cracow, 4-7 June 2024, 569-578. https://doi.org/10.7148/2024-0569

[23] Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I. and Roytman, M. (2021) Exploit Prediction Scoring System (EPSS). *Digital Threats*: *Research and Practice*, **2**, 1-17. https://doi.org/10.1145/3436242

[24] Jahani Chehrehbargh, F., Rajabifard, A., Atazadeh, B. and Steudler, D. (2024) Current Challenges and Strategic Directions for Land Administration System Modernisation in Indonesia. *Journal of Spatial Science*, **69**, 1097-1129. https://doi.org/10.1080/14498596.2024.2360531

[25] Yagi, S., Tsuchikawa, K. and Tsuji, K. (2024) A Heatmap-Based Visualization Technique for Finding Operational Problems. https://discovery.researcher.life/article/a-heatmap-based-visualization-technique-for-finding-operational-problems/8c5461b514c13bd6bcff6aff0ca3c296

[26] Aditya, T. (2023) Visualizing Title Uncertainty and Quality Issues in the Digital Era of Land Administration. https://fig.net/resources/proceedings/fig_proceedings/7_2023/papers/se02/SE02_aditya_12363.pdf

[27] Sakellariou, G., Fouliras, P., Mavridis, I. and Sarigiannidis, P. (2022) A Reference Model for Cyber Threat Intelligence (CTI) Systems. *Electronics*, **11**, Article 1401. https://doi.org/10.3390/electronics11091401

[28] Wilhoit, K. and Opacki, J. (2022) Operationalizing Threat Intelligence: A Guide to Developing and Operationalizing Cyber Threat Intelligence Programs. Packt Publishing Ltd.

[29] Teichmann, F.M. and Boticiu, S.R. (2024) Cyber Threat Intelligence: Existing Benefits and Challenges for Law Firms and Businesses. *International Cybersecurity Law Review*, **5**, 491-499. https://doi.org/10.1365/s43439-024-00117-1

[30] Valdés Ríos, V., Zaidi, F., Cavalli, A.R. and Rego, A. (2024) Towards the Adoption of Automated Cyber Threat Intelligence Information Sharing with Integrated Risk Assessment. *Proceedings of the* 19*th International Conference on Availability*, *Reliability and Security*, Vienna, 30 July-2 August 2024, 1-9. https://doi.org/10.1145/3664476.3670444

[31] Hank, S.W. (2024) Transforming Unstructured Data Sources into Structured Cyber Threat Intelligence. https://medium.shawnhank.com/transforming-unstructured-data-sources-into-structured-cyber-threat-intelligence-415b23b67bc5

[32] Jo, H., Lee, Y. and Shin, S. (2022) Vulcan: Automatic Extraction and Analysis of Cyber Threat Intelligence from Unstructured Text. *Computers & Security*, **120**, Article ID: 102763. https://doi.org/10.1016/j.cose.2022.102763

[33] Jacobs, J., Romanosky, S., Adjerid, I. and Baker, W. (2020) Improving Vulnerability Remediation through Better Exploit Prediction. *Journal of Cybersecurity*, **6**, tyaa015.

https://doi.org/10.1093/cybsec/tyaa015

[34] Li, L., Huang, C. and Chen, J. (2024) Automated Discovery and Mapping Att&ck Tactics and Techniques for Unstructured Cyber Threat Intelligence. *Computers & Security*, **140**, Article ID: 103815. https://doi.org/10.1016/j.cose.2024.103815

[35] Ramsdale, A., Shiaeles, S. and Kolokotronis, N. (2020) A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. *Electronics*, **9**, Article 824. https://doi.org/10.3390/electronics9050824

[36] Jacobs, J. and Romanosky, S. (2024) Probability, Percentiles, and Binning—How to Understand and Interpret EPSS Scores. https://www.first.org/epss/articles/prob_percentile_bins

[37] Lee, J. and Kang, M. (2015) Geospatial Big Data: Challenges and Opportunities. *Big Data Research*, **2**, 74-81. https://doi.org/10.1016/j.bdr.2015.01.003

[38] Bennett, R.M., Unger, E., Lemmen, C. and Dijkstra, P. (2021) Land Administration Maintenance: A Review of the Persistent Problem and Emerging Fit-For-Purpose Solutions. *Land*, **10**, Article 509. https://doi.org/10.3390/land10050509

[39] Roccia, T. (2023) Visual Threat Intelligence: An Illustrated Guide for Threat Researchers. Independently Published.

[40] Irwin, D. and Mandel, D.R. (2019) Improving Information Evaluation for Intelligence Production. *Intelligence and National Security*, **34**, 503-525. https://doi.org/10.1080/02684527.2019.1569343

[41] Irwin, D. and Mandel, D.R. (2019) Improving Information Evaluation for Intelligence Production. *Intelligence and National Security*, **34**, 503-525. https://doi.org/10.1080/02684527.2019.1569343

[42] Blin, P.-F. (2025) Proactive Cybersecurity for Spatial Cadastral Data of Land Administration System. Ph.D. Thesis, Universitas Gadjah Mada.