МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

AI-DRIVEN CYBERSECURITY IN CRITICAL INFRASTRUCTURE: A BIBLIOMETRIC ANALYSIS (2015–2025)

Evgeniya Nikolova[1], Todor Slavov[2]
[1]Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria
[2]Faculty of Computer Science and Engineering, Burgas Free University, Burgas, Bulgaria
e-mails: [1]enikolova@bfu.bg, [2]tslavov@bfu.bg

This paper presents a bibliometric analysis of 1,862 research documents (2015–2025) focused on the application of Artificial Intelligence (AI) for Critical Infrastructure (CI) cybersecurity. Data from Scopus and Web of Science were processed using the Bibliometrix R-package. The study quantifies publication dynamics and maps thematic and sector-specific patterns in AI methods applied to OT/ICS/SCADA cybersecurity after 2020. Sector-specific analysis reveals distinct technological profiles: the Energy sector *remains anchored in SCADA security and False Data Injection detection; the Transport sector shows a shift toward Federated Learning for connected mobility; and the Water sector highlights a niche but growing focus on Explainable AI (XAI) and IoT. These findings map the transition from general infrastructure protection to domain-specific AI countermeasures.*

Keywords: Artificial intelligence; critical infrastructure; OT/ICS/SCADA; cybersecurity; anomaly detection; federated learning; false data injection; bibliometric analysis.

КИБЕРСИГУРНОСТ В КРИТИЧНАТА ИНФРАСТРУКТУРА: БИБЛИОМЕТРИЧЕН АНАЛИЗ (2015–2025)

Евгения Николова[1], Тодор Славов[2]
[1]Институт по математика и информатика, Българска академия на науките, София,
[2]Център по информатика и технически науки, Бургаски свободен университет
e-mails: [1]enikolova@bfu.bg, [2]tslavov@bfu.bg

Тази статия представя библиометричен анализ на 1862 научни публикации (2015–2025), свързани с прилагането на изкуствен интелект (ИИ) на критичната инфраструктура. Данните представляват библиографски записи и метаданни (заглавия,

https://doi.org/10.55630/mem.2026.55.126-133
2020 Mathematics Subject Classification: 68M25, 68T01.

резюмета, ключови думи, година, източник/списание или конференция и др.), извлечени от базите Scopus и Web of Science и обработени с помощта на R-пакета Bibliometrix. Изследването установява значително увеличение на научната продукция след 2020 г. Секторният анализ разкрива различни технологични профили: енергийният сектор остава фокусиран върху SCADA сигурността и откриване на инжектиране на фалшиви данни; транспортният сектор показва преминаване към федерирано обучение за свързана мобилност; водният сектор фокус върху обясним ИИ (XAI) и IoT. Тези резултати картографират прехода от обща защита на инфраструктурата към специфични за областта ИИ решения.

Ключови думи: Изкуствен интелект; критична инфраструктура; OT/ICS/SCADA; откриване на аномалии; федерирано обучение; инжектиране на фалшиви данни; тренд анализ.

1. INTRODUCTION

Critical infrastructure (CI) refers to systems and assets whose disruption would have a significant impact on societal safety, economic stability, and essential services. Core examples include energy systems, transportation networks, and water utilities. The digital transformation of these sectors has increased connectivity and automation [4], but it has also expanded the exposure of operational technology (OT) environments such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA). Compared to conventional IT, OT/ICS/SCADA systems are constrained by legacy protocols, long equipment lifecycles, strict availability requirements, and safety-critical operating conditions. Consequently, cyber incidents in CI can propagate beyond data loss to physical disruption and public safety impacts.

In parallel, artificial intelligence (AI) techniques, most notably machine learning (ML) and deep learning (DL), have become central to contemporary cyber defense research. AI-based approaches are widely explored for intrusion detection, anomaly detection, malware/threat identification [1], and resilience-oriented monitoring. However, CI cybersecurity literature is highly heterogeneous. AI methods are applied across different domains (e.g., power grids, connected mobility, water distribution), evaluated under different assumptions, and described using partially overlapping terminology. This fragmentation makes it difficult to identify which research directions are stabilizing, which are declining, and which are emerging— especially because trends differ substantially across CI sectors.

Recent surveys (2022–2024) on AI for cybersecurity often adopt a narrative approach or focus predominantly on a single CI domain (most often smart grids/energy), while treating critical infrastructure as a monolithic application area. In addition, many reviews do not provide transparent, reproducible merged corpus across major bibliographic databases. The present study provides mapping and comparing sector-stratified thematic structures for OT/ICS/SCADA security in Energy, Transport, and Water, revealing distinct technological trajectories rather than a single "CI cybersecurity" trend. Unlike prior single-sector reviews, our results explicitly quantify and visualize cross-sector divergence (e.g., federated learning visibility in Transport versus XAI signals in Water), which is not observable when CI is analyzed as one aggregate corpus.

The paper is organized into three main structural sections: introduction, methodology, and results and discussion. The methodological section presents the PRISMA-oriented

research design, the data sources used, the study objectives, and the applied bibliometric analytical approaches. In the Results and Discussion section, the publications are systematized and analyzed through sector-specific thematic mapping, accompanied by a critical discussion of the methodological robustness and limitations of the approach used.

2. METHODOLOGY

This study applies a PRISMA-guided systematic search and transparent dataset accounting, combined with bibliometric mapping and keyword-based thematic analysis, to identify research patterns in AI-driven cybersecurity for critical infrastructure (CI), with a focus on OT/ICS/SCADA contexts, over 2015–2025. PRISMA 2020 guidelines were used to ensure transparent reporting of identification, screening, and inclusion [3].

The study aims to analyze publications in the field of AI-based cybersecurity for critical infrastructure by examining publication dynamics, the formation of thematic clusters, the evolution of emerging and maturing topics, and sectoral differences in accordance with the protection needs of three sectors: energy, transport, and water.

Two bibliographic databases were used: Scopus and Web of Science Core Collection. Queries were constructed using three semantic blocks: (1) AI methods, (2) CI/OT/ICS/SCADA domains, and (3) security objectives (e.g., intrusion/anomaly/threat detection). Searches were restricted to 2015–2025, English language, and peer-reviewed journal articles and conference/proceedings papers. Exclusion terms were used to reduce off-scope retrieval. Full database queries (Scopus TITLE-ABS-KEY and WoS TS) are provided in the online repository (Data availability).

Records were retrieved from Scopus (n = 1,774) and Web of Science Core Collection (n = 971) for the period 2015–2025 (total n = 2,745) and imported into R for merging and deduplication using bibliometrix [2] via the Biblioshiny interface. Automated deduplication was performed primarily by DOI, supported by title-based matching, resulting in a final unique corpus of n = 1,862 documents (duplicates removed = 883). Because objective of the study is bibliometric mapping and thematic trend analysis, eligibility was assessed at the metadata level (titles/abstracts/keywords) and no formal full-text eligibility stage was conducted. Although the merged corpus contains a small number of 2026-indexed records (n = 4), all analyses in this paper were restricted to publications from 2015–2025. Due to database indexing conventions (e.g., early access/online-first records), a very small number of records tagged as 2026 may appear in the metadata exports; however, the study's interpretation and reported trends focus on the 2015–2025 window and are not affected materially by this negligible fraction.

Bibliometric mapping and thematic analysis were conducted in R using bibliometrix/biblioshiny [2]. Conceptual structure was derived via co-word analysis, operationalized as keyword co-occurrence networks and thematic maps. To reduce noise from heterogeneous indexing, thematic mapping was performed primarily using **Author Keywords**.

For sector-oriented analysis, the merged corpus was stratified into **Energy (N=716), Transport (N=1131), and Water (N=233)** using rule-based **multi-label** tagging applied to a concatenated metadata field (Title + Abstract + Author Keywords; TI + AB + DE). Boolean sector flags were generated using domain-specific dictionaries (e.g., grid/power/SCADA for Energy; rail/traffic/vehicle/V2X for Transport; water/wastewater/treatment for Water), allowing overlaps across sectors when multiple keyword sets matched a record.

A supplementary thematic evolution analysis (cut-point 2020) was conducted for the Energy sub-corpus using **All Keywords** to increase term coverage; outputs (tables/figures) are provided in the online repository (Data availability). Borderline inclusion and tagging cases were discussed with a second researcher to ensure consistent application of criteria.

3. RESULTS AND DISCUSSION

Our work focuses on three CI sectors (Energy, Transport, Water) selected due to data availability and relevance to OT/ICS/SCADA security; other CI sectors were left for future work.

3.1. Sector-Specific AI Strategies

Table 1. Summary of Sector-Specific Bibliometric Profiles (2015–2025)

Sector	Sub-corpus size N	High-frequency themes	Distinctive/emerging
Energy	716	FDI; SCADA	Increased attention to grid-specific adversarial models (e.g., false data injection; state estimation)
Transport	1131	SCADA/ICS security; anomaly detection; intrusion detection; cybersecurity	Federated learning (privacy/privacy-preserving mobility)
Water	233	Anomaly detection; industrial control systems; intrusion detection; ML/DL	Niche growth toward explainable AI (XAI) and IoT trust/monitoring in water distribution contexts

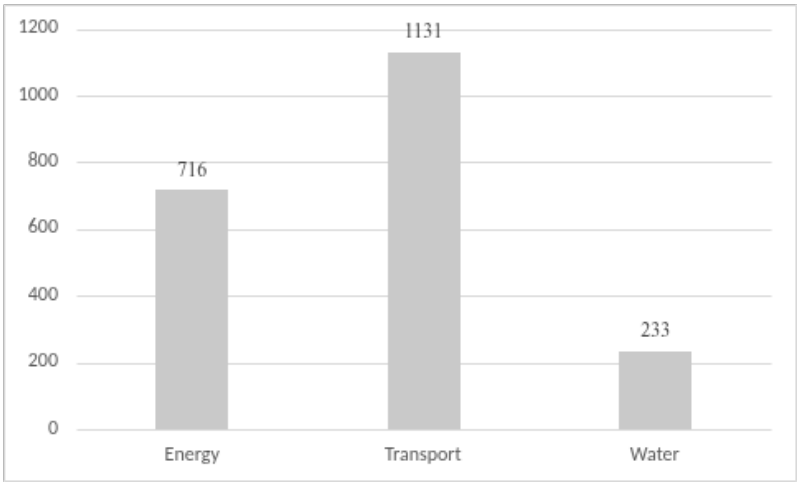

Figure 1. Sub-corpus sizes by sector

Table 2. Emerging vs. Declining/Maturing Thematic Clusters

Category	Identified Themes (Keywords)	Context / Sector Impact
Emerging / recently visible themes	Federated learning; XAI	Transport: federated learning cluster (CF = 243); Water: explainable AI cluster (CF = 26)
Maturing / baseline themes	Signature-based detection; Standard NNs/LSTMs; General **SCADA** terms	Recurrent across sector maps; foundational vocabulary

	Energy	**Transport**	**Water**
Emerging themes	—	Federated Learning	XAI (+ IoT signal)
Maturing / baseline themes	SCADA / Anomaly Detection / Intrusion Detection	SCADA / ICS Security / Anomaly Detection	Anomaly Detection / ICS / ML

Figure 2. Summary matrix of sector association of emerging vs baseline themes

Our work focuses on three CI sectors (Energy, Transport, Water) selected due to data availability and relevance to OT/ICS/SCADA security; other CI sectors were left for future work. The analysis was conducted separately for Energy (N=716), Transport (N=1,131), and Water (N=233), emphasizing the distinctive thematic patterns and, where applicable, their temporal evolution within each sector. Tables 1 and 2 collectively summarize the sector-specific bibliometric profiles for 2015–2025, detailing sub-corpus sizes, high-frequency keywords, distinctive and emerging topics across Energy, Transport, and Water, and categorizing thematic clusters into emerging versus maturing trends with their sectoral context and impact. Sub-corpus sizes are visualized in Figure 1, while sector association of emerging versus baseline themes is summarized in Figure 2.

Detailed time-slice outputs (Energy evolution split at 2020) are available in the online repository (Data availability).

3.1.1. Energy Sector The Energy sub-corpus (N=716) is dominated by OT/ICS/SCADA-oriented security and AI-based detection (Fig. 3). In the thematic map, machine learning co-occurs strongly with SCADA, anomaly detection, and industrial control systems, indicating a shared baseline for monitoring and detection, while additional clusters (cybersecurity, intrusion detection, deep learning) reflect the consolidation of AI-based protection methods in OT environments. A supplementary thematic evolution analysis (split at 2020) suggests a shift from broader CI themes toward more specialized network-security topics, including links from power-system protection to state estimation and false-data-injection attack detection; outputs are available in the online repository (Data availability). Overall, Energy-sector research remains SCADA-centered, with increasing emphasis on grid-specific attack models.

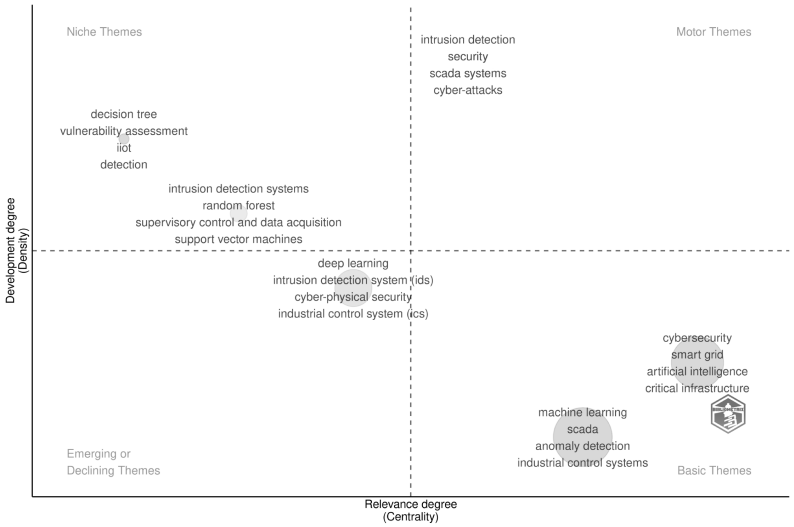

Figure 3. Thematic Map of the Energy sector

3.1.2. Transport Sector The Transport sub-corpus highlights a different thematic emphasis (Fig. 4). General security terminology remains pervasive, while the thematic map separates methodological directions: anomaly detection and intrusion detection are prominent, and federated learning emerges as a sector-differentiating theme, indicating growing attention to distributed and privacy-preserving learning aligned with connected mobility and geographically distributed data sources (ClusterFrequency: anomaly detection = 555; federated learning = 243).

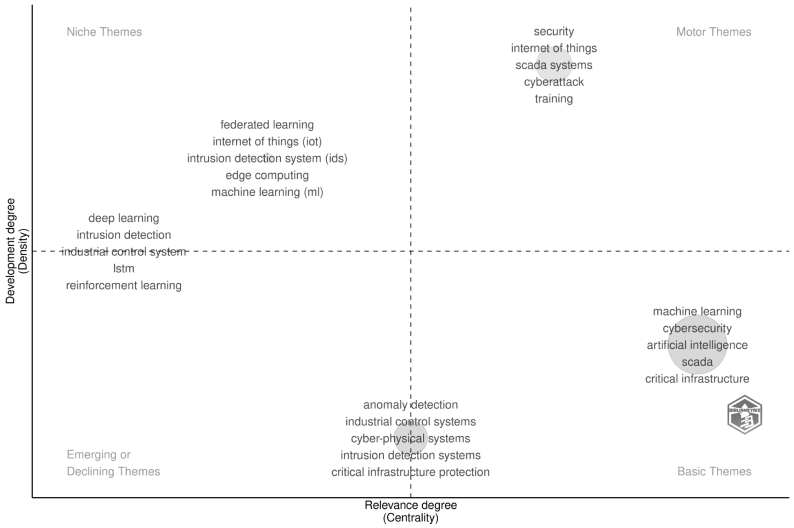

Figure 4. Thematic Map of the Transport sector

3.1.3. Water Sector The Water sub-corpus shows a compact but coherent landscape emphasis (Fig. 5), with anomaly detection and machine learning anchored around industrial control systems and water distribution contexts. Notably, the presence of an explainable AI (XAI) cluster suggests increasing emphasis on interpretability and operator trust, alongside a separate IoT-related security signal.

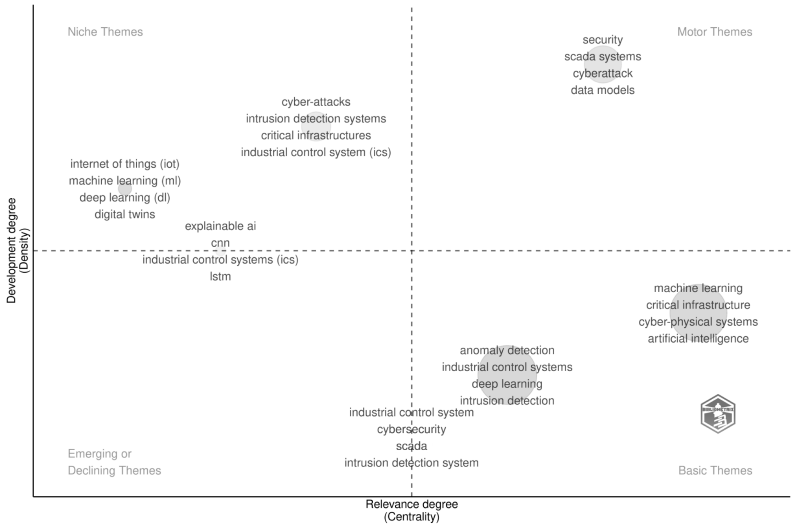

Figure 5. Thematic Map of the Water sector

3.2. Methodological robustness and limitations. To characterize the robustness of the thematic structure, **Callon centrality and density** are used, which reflect the relevance of the topic to the field and its internal cohesion, respectively. Themes with high centrality and density are interpreted as well-developed and influential, whereas low centrality/low-density themes are considered emerging or declining and should be treated cautiously. Sensitivity to preprocessing and threshold choices (e.g., keyword normalization and minimum frequency) further supports interpreting the results as high-level conceptual patterns rather than definitive taxonomies.

This study integrates PRISMA-guided dataset accounting with bibliometric science mapping in bibliometrix/biblioshiny [2], ensuring transparent retrieval, screening, merging, and deduplication, while thematic mapping characterizes the conceptual structure of the final corpus. Nevertheless, several methodological limitations should be noted. First, the reliability of co-word thematic mapping is bounded by metadata quality and database/export coverage (e.g., inconsistent or missing Author Keywords/abstracts across Scopus and Web of Science), which can affect term frequencies and cluster composition. Second, thematic structures are sensitive to analysis settings (field selection, Louvain clustering, and minimum-frequency thresholds); therefore, clusters should be interpreted as high-level, reproducible signals rather than definitive taxonomies. Third, deduplication performed primarily via DOI (supported by title-based matching when DOI is missing) may leave residual duplicates or merge near-duplicate records. Finally,

sector stratification relied on rule-based multi-label tagging over TI+AB+DE, which may introduce false positives/false negatives when sector context is implicit or expressed using non-standard vocabulary; the 2020 split is an analytic contrast point and may mask earlier or later waves of emergence.

4. CONCLUSION

Using a bibliometric dataset of 1,862 documents, this study investigates the evolution of AI-based cybersecurity across critical infrastructure sectors. While anomaly detection remains a universal baseline, AI strategies are increasingly sector-specific: the Energy sector focuses on countering physics-aware attacks (e.g., False Data Injection), the Transport sector emphasizes decentralized, privacy-preserving models (Federated Learning), and the Water sector highlights the need for Explainable AI (XAI) to ensure operator trust. Future research will focus on bridging gaps in the Water and Transport sectors through the development of interpretable AI models suitable for resource-constrained edge devices, thereby strengthening the resilience of distributed Industrial IoT and cyber-physical systems against adversarial AI threats.

Data availability. The full deduplicated dataset (n = 1,862), sector labels, and derived bibliometric tables are available at: https://github.com/tslavov-git/Bibliometric-Analysis

References

[1] Aminu, M., Akinsanya, A., Oyedokun, O., and Akinwande, O. T. (2024). A review of advanced cyber threat detection techniques in critical infrastructure: Evolution, current state, and future directions. *International Journal of Computer Applications Technology and Research*, 13(8), 74–87. https://www.irejournals.com/paper-details/1706103.

[2] Aria, M., and Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, 11(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007.

[3] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. https://doi.org/10.1136/bmj.n71.

[4] Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., and Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial internet of things. *IEEE Internet of Things Journal*, 6(4), 6822–6834. https://doi.org/10.1109/JIOT.2019.2912020.