

Ewa WIĘCEK-JANKA¹, Mikołaj GRZYB²

DIGITAL COMPETENCIES AND KNOWLEDGE MANAGEMENT IN RAILWAY OPERATORS: A GLOBAL BIBLIOMETRIC STUDY (1975-2025) AND IMPLICATIONS FOR SECURITY POLICY DEVELOPMENT

DOI: 10.21008/j.0239-9415.2026.093.09

Digital competencies have become one of the central research areas in contemporary management studies, and constitute the foundation for knowledge management, adaptive capabilities, and organisational resilience, particularly in high-risk and high-responsibility sectors. Their importance has increased significantly alongside the digitalisation of organisational processes and the rapid development of technologies supporting operational safety and continuity.

The aim of this article is to identify, analyse, and visualise global research trends related to digital competencies between 1975 and 2025, as well as to determine the implications of these studies for the development of safety policies and competency frameworks among railway operators.

The study employed bibliometric and scientometric analysis based on the Scopus database, using the PRISMA selection procedure and VOSviewer software for keyword co-occurrence analysis and scientific network mapping.

The results indicate an exponential growth in publications, with social sciences and computer science dominating the field, while management studies remain comparatively underrepresented.

Keywords: bibliometrics, Scopus, knowledge management, VOSviewer, scientometrics, organisation security, digital competencies

¹ Poznan University of Technology, Faculty of Engineering Management. ORCID: 0000-0002-5596-307X.

² Poznan University of Technology, Faculty of Engineering Management. ORCID: 0009-0005-3995-6581.



1. INTRODUCTION

Digital competency is now a cross-cutting concept, rooted in social sciences, computer science, and management, and in the public policy dimension. It has been structured by the European DigComp framework, which defines areas and levels of proficiency and offers examples of applications to support the design of development interventions (Carretero Gómez, Vuorikari, Punie, 2017). At the same time, the management debate has seen the consolidation of the evidence-based/evidence-informed management approach, which advocates basing organisational decisions on the best available evidence from research, organisational data, and expert knowledge (Rousseau, 2006).

In this approach, bibliometric auditing serves not only a descriptive but also a strategic function: it allows us to recognise the structure of the field (topics, schools, co-authorship networks), identify gaps, and map development trajectories, thus providing a foundation for rational competency policies (Donthu et al. 2021). Technically speaking, contemporary science mapping uses tools such as VOSviewer, which implement the visualisation of similarities (VOS) method and enable the construction of maps of keyword co-occurrence, co-citations, and co-authorship in a transparent and replicable manner (Van Eck, Waltman, 2010). The importance of such structured knowledge is growing in high-risk organisations, where operational safety depends on both technology and the competency of personnel and organisation practices that foster resilience (Weick, Sutcliffe, 2015). In the railway sector, whose safety management systems require continuous adaptation to digitalisation and cyber threats, a synthetic overview and visualisation of the global output on digital competencies (1975-2025) is therefore an essential step in designing safety policies and competency development programmes coordinated with SMS objectives (Liu et al., 2023).

This article maps the global structure of research on digital competencies (1975-2025) in order to identify the gap that constrains competency-based security policies for railway operators. The research problem is whether the mature digital-competency literature provides an operationalisable knowledge base for safety and security management in railway operators. Three research questions are posed: (RQ1) What are the growth dynamics, disciplinary structure and geography of this research? (RQ2) To what extent is it linked with operational railway personnel and railway cybersecurity? (RQ3) What implications follow for knowledge management and security policy? We test the hypothesis (H1) that the digital-competency and the railway cybersecurity streams, although both mature, develop in parallel, and that their intersection with frontline railway roles remains structurally under-represented.

2. LITERATURE REVIEW

Three streams of research frame this study. First, digital competency as a policy and analytical construct: DigComp structures it into areas and proficiency levels (Carretero Gómez et al., 2017; Vuorikari et al., 2022), and conceptual work positions it as a boundary concept spanning education, work and technology (Ilomäki et al., 2016; Van Laar et al., 2017); workplace-oriented syntheses are more recent (Alhloul, Kiss, 2022; Huu, 2023).

Second, railway cybersecurity: reviews and surveys map security standards and the safety–security interface in signalling (López-Aguilar et al., 2022; Soderi, Masti, Lun, 2023), while technical studies document vulnerabilities in ERTMS/GSM-R and CBTC communications (Lopez et al., 2018; Bu, Wu, 2019; Soderi et al., 2023).

Third, human factors, safety management and knowledge management in railways: HFACS studies attribute many incidents to skill-based errors and organisational preconditions (Guo et al., 2025; Bhuiyan et al., 2023), automation reshapes operator roles (Dadashi et al., 2014), safety-climate instruments supply the measurement layer of SMS (van Nunen et al., 2022; Lampe et al., 2021), and knowledge management appears as a strategic capability of railway enterprises, including ontology-based capture of tacit maintenance expertise (Dykan et al., 2019; Retbi et al., 2023). Only Thron et al. (2024) explicitly bridges competence, training and cyber risk for signalling staff.

3. MATERIALS AND METHODS

The analysis was based on Scopus, considered one of the most comprehensive sources for indexing peer-reviewed literature (including CSAB selection, description of content coverage, and document types), and which promotes the reproducibility and comparability of results (Elsevier, 2022, 2025). A search was performed in the title/abstract/keyword fields for a family of phrases reflecting the scope of the concept: digital competency(s), digital skill(s), and ICT skill(s), with the following restrictions: English language, document type: article, publication stage: final, years: 1975-2025. The rationale for descriptor selection (taking into account singular and plural forms) and filter parameters can be found in the search specification (tab. 1), which constituted the starting point for the further data cleaning and aggregation steps.

Table 1. Systematic review of the search criteria for publications on digital competency

Search type	Title, abstract, keywords
Keywords	“Digital competency” or “Digital competency” or “Digital skill” or “Digital skills” or “ICT skill” or “ICT skills”
Document type	Article
Publication stage	Final
Year of publication	1975-2025
Language	English
Database	Scopus

Source: own study.

The record selection procedure was carried out according to the PRISMA 2020 guidelines: identification, deduplication, screening, evaluation of all records and inclusion in the analysis; the results were reported in the form of a flow chart indicating the number of records and the reasons for exclusion (Page et al., 2021; PRISMA, 2021). In practice, this meant removing duplicates between exports, excluding publications that did not meet the type/stage criteria, and recoding ambiguous labels (tab. 2).

Table 2. PRISMA procedure

PRISMA phase	Step/filter	Inclusion criterion	Remaining after step (n)	Excluded at step (criterion, n)	Cumulative N (after step)
Identification	Query in Scopus	All publications returned by the query	10,429	–	10,429
Filtering	Year of publication	1975-2025	10,423	Other years than 1975-2025: 6	10,423
Filtering	Document type	Article	6,556	Other than article: 3,867	6,556
Filtering	Language	English	5,446	Other than English: 1,110	5,446
Filtering	Publication stage	Final	5,228	Under review (in-press/under review): 218	5,228

PRISMA phase	Step/filter	Inclusion criterion	Remaining after step (n)	Excluded at step (criterion, n)	Cumulative N (after step)
Accepted	Records included in the analysis	Meeting all of the above criteria	5,228	–	5,228

Source: own study based on Scopus; export from [20 September 2025]; filters as in column.

The bibliographic section applies methodological recommendations for management research: explicit rules for source selection, decisions on measures and normalisation, reporting of thresholds, and transparency of analytical steps (Donthu et al., 2021; Zupic, Čater, 2015). The data were exported in CSV/RIS formats and loaded into VOSviewer using the Visualization of Similarities (VOS) method. Co-occurrence networks (level: author keywords/keywords-plus), co-authorship networks (authors, countries, organisations), and, where appropriate, co-citation networks were constructed. Normalisation was performed using the “association strength” measure, and in cases of excessive network complexity, occurrence thresholds were applied (e.g. ≥ 4 for cybersecurity–railway analyses to increase map readability), which was noted in the parameter documentation (Van Eck, Waltman, 2010).

In addition, summaries of trends (annual frequency, distribution of fields, and geography of publications) were prepared, along with methodological comments on language restrictions and document types.

4. RESULTS

In the period under study, we observe a classic “hockey stick” graph: after isolated mentions until 2002, there is a first significant jump in 2003 (15 publications), a moderate increase until 2012 (59), and then a rapid acceleration: 2018 (137) and 2020 (381), culminating in 2024 (1003). Preliminary data for 2025 (681) should be treated as incomplete (publications are currently being indexed). This dynamic reflects, on the one hand, the cumulative effect of work on definitions and measurement of digital competencies (after 2010), and, on the other, the “demand shock” associated with the acceleration of the digital transformation and the spread of remote working around 2020, which visibly increased the number of articles indexed in Scopus. It is worth noting that after 2018, the annual increase in publications is clearly non-linear, suggesting both an expansion of the author base and a diversification of topics (e.g., e-health, remote education, skills in the workplace).

Documents by year

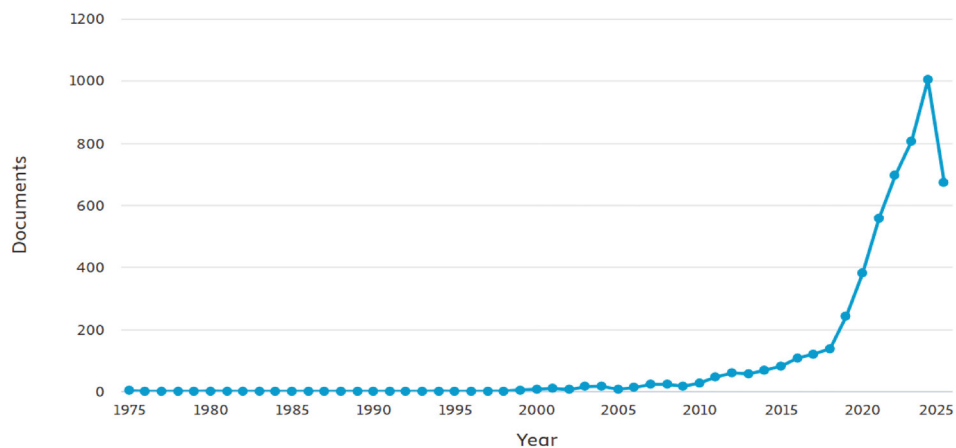


Fig. 1. “Number of articles 1975-2025” (Scopus [20 September 2025])

The distribution of fields confirms the multidisciplinary nature of the topic. Social sciences have the largest share (38.7%), reflecting the dominance of educational, inclusive, and social aspects of technology use. Computer science (14.9%) accounts for the technical component, i.e., infrastructure, software, and AI, which determine the content and directions of the competency description. Business and management (6.8%) contribute an organisational perspective (digitisation strategies, change management, productivity), and psychology (5.2%) contributes cognitive and social perspectives (motivation, workload, adaptation). Engineering (4.9%) concerns aspects such as ergonomics and the design of solutions supporting the practical use of digital tools, while art and humanities (4.6%) testify to the growing role of digital humanities and new forms of expression. Medicine (4.4%) and health sciences (2.4%) focus on e-health and telemedicine. The “other” category (11.6%) brings together a number of complementary areas (including energy and mathematics), highlighting the breadth of applications.

Table 3. Share of publications by field (Scopus, 1975-2025; article; final; English language)

No.	Subject area	Share in results (%)
1	Social Sciences	38.7
2	Computer Science	14.9
3	Business, Management & Accounting	6.8
4	Psychology	5.2
5	Engineering	4.9

No.	Subject area	Share in results (%)
6	Arts and Humanities	4.6
7	Medicine	4.4
8	Environmental Science	3.4
9	Economics, Econometrics, and Finance	3.3
10	Health Professions	2.4
11	Other	11.6

Source: based on Scopus data [20 September 2025].

Interpretatively, the dominance of social sciences in our study confirms that “digital competencies” are conceptualised in the literature primarily from the perspective of the user and the social context (education, inclusiveness, learning) and only secondarily as related to technology and operational practices. This direction is consistent with the research trend that places digital competencies within the boundaries of pedagogy and educational policy and describes them as a “boundary concept” that brings together many fields but is rarely anchored in specific work tasks (Ilomäki et al., 2016). Even where labour market requirements are emphasised, approaches tend to focus on horizontal skills (e.g., communication, collaboration, problem solving) rather than on operational safety indicators in high-risk environments (van Laar et al., 2017). From the perspective of organisation safety policies, we therefore have a wealth of evidence on behaviour, learning, and inclusiveness that can be linked to the frameworks of safety management systems (SMS) and high-reliability organisations (HRO), which emphasise resilience, anticipation, and monitoring (Weick, Sutcliffe, 2015; Hollnagel, 2014).

At the same time, this structure of literature reveals a cognitive gap: there is a lack of sectoral operationalisation of digital competencies related to work artefacts and security KPIs, e.g., in railways: working with HMI/ERTMS, operational cyber hygiene, data literacy in dispatching. Reviews of bibliometric methods warn that without narrowing the vocabulary to sectoral descriptors and the role of “front-line” analysis, they will systematically lean towards the most numerous trends, i.e., educational ones (Zupic, Čater, 2015; Donthu et al., 2021).

Within the railway literature this disconnection is explicit: security reviews and technical studies stay at the architecture and protocol layer (López-Aguilar et al., 2022; Lopez et al., 2018; Bu, Wu, 2019), while competence-related evidence appears as error taxonomies or safety climate (Guo et al., 2025; Lampe et al., 2021).

The consequence is a lack of bridges between the mature “digital competencies” trend and the development of SMS in critical sectors, including rail transport, where systemic approaches to safety are being developed but rarely linked to the measurement of staff competencies (Liu et al., 2023; Reason, 1997). Therefore, research is

needed that: (1) translates DigComp domains into measurable, job-specific safety indicators; (2) embed them in the HRO/Safety-II paradigm; (3) test their relationship with hard operational outcomes (near misses, response time, procedural compliance) in high-risk organisations. An analysis of the country of origin of the publications shows a strong concentration in Western Europe and Anglo-Saxon countries. Spain is the leader (873 publications), which can be linked to extensive digital skills development programmes, EU policies, and active educational consortiums. The United Kingdom (368) and the US (269); followed by Italy (222), China (219), and Germany (203). Indonesia, Norway, Malaysia, and Australia, among other countries, fall within the range of 166-182, suggesting a growing diffusion of the topic beyond traditional publishing centres (tab. 4).

Table 4. Query on “digital competency”

No.	Country	Number of publications (n)	Position of classification	Summary comment (based on description)
1	Spain	873	1	Strong national and regional strategy; extensive use of EU funding; dense networks of academic cooperation.
2	United Kingdom	368	2	Long tradition of research into digital literacy/skills; university-government-business consortia; emphasis on education and public administration.
3	United States	269	3	Interdisciplinarity (social–IT–economic); business applications, innovation, labour market.
4	Italy	222	4	Digital education, combating exclusion, impact on regional development.
5	China	219	5	Mass digitisation, e-learning, AI, digital transformation of the public sector.
6	Germany	203	6	Industry 4.0, automation, technical education; stable growth in research.
7	Indonesia	182	7	Development of skills to level the playing field between urban and rural areas.
8	Norway	181	8	Strong emphasis on education and a knowledge-based economy.
9	Malaysia	178	9	Digital skills as a lever for modernisation and attracting technological investment.
10	Australia	166	10	Integration of digital competencies in education and the economic system.

Source: based on Scopus data [20 September 2025].

The geographical distribution of the achievements, which shows a clear concentration in selected countries (including Spain, the United Kingdom, and the United States), has direct operational consequences for the formation of research partnerships. In terms of scientometrics, leading countries and their institutions act as network hubs which, thanks to their high intermediary centrality and dense co-authorship ties, accelerate the diffusion of knowledge, standardisation of practices, and effectiveness of fundraising (Katz, Martin, 1997; Wagner, Leydesdorff, 2005). Our publication geography results therefore suggest prioritising consortia with centres that combine educational agendas here: the DigComp framework, research on digital literacy/skills with implementations in administration and the private sector. It is in these ecosystems that it is easiest to translate results into policies and programmes (Carretero Gómez, Vuorikari, Punie, 2017).

At the same time, the relatively lower participation of some countries does not necessarily indicate a lack of scientific activity but may result from language and indexing bias. Comparative studies show that the coverage of bibliographic databases varies both geographically and by field; for example, Scopus better records social and applied sciences than Web of Science, which may impact the visibility of the achievements of non-English-speaking countries (Mongeon, Paul-Hus, 2016). Furthermore, the language barrier systematically reduces the detectability and use of results published outside English, even if they are highly useful for practice (Amano, González-Varo, Sutherland, 2016). For this reason, subsequent stages of reviews should include: (a) checking for language bias (e.g., including multilingual abstracts and searches in local languages); (b) including grey literature, which often contains key evidence in the areas of public policy and implementation (Haddaway et al., 2015; Paez, 2017). Supplementing with government reports, standards, and industry documents not only reduces the effect of selection, but also enhances the decision-making utility of the results (evidence-informed management) in high-risk sectors.

5. DISCUSSION

The bibliometric analysis confirms the dominance of socio-educational and IT approaches in research on digital competencies, with a relatively smaller, though growing, contribution from business and management (38.7% vs. 14.9% vs. 6.8% share). This thematic structure is consistent with the direction of the DigComp framework, which emphasises the use of technology by citizens and employees, e.g., learning, collaboration, security, problem solving, and in the latest update, expands the catalogue of examples to include the areas of AI and digital security (Carretero Gómez, Vuorikari, Punie, 2017; Vuorikari et al., 2022). As a result, the “focus” of the literature remains on the user and the educational process, while the “organisational” and “operational” components, e.g., measuring competencies in line work, integration with security KPIs, are less prominent.

From the perspective of management review methodology, such an asymmetrical distribution of fields is not surprising: bibliometrics, unless narrowed down lexically to sector descriptors, “leans” towards the most numerous represented trends (Zupic, Čater, 2015; Donthu et al., 2021). Our results confirm this rule and reinforce the argument for sectoral segmentation (rail) and the expansion of the dictionary to include frontline roles, e.g., dispatcher, train driver, signalling technician, and safety descriptors (SMS, HRO, cyber maturity). This clarification facilitates translation between the strands of “digital competencies” and “system security”, which is crucial for practice.

In the railway literature, we observe the dynamic development of two mature but separate streams: (1) cybersecurity of systems such as CPS, control, communication, standards, human factors, and automation. Systematic reviews and surveys diagnose the maturation of this area–safety–security relations, standardisation and signalling protection – while noting that the management and personnel perspective appears less frequently (López-Aguilar et al., 2022; Soderi, Masti, Lun, 2023; Lopez et al., 2018; Bu, Wu, 2019). (2) Human factors, competence and safety management of operational personnel: error taxonomies, automation and safety climate (Guo et al., 2025; Bhuiyan et al., 2023; Dadashi et al., 2014; Lampe et al., 2021). At their interface, digital competency is rarely a measurable construct; Thron et al. (2024) is the notable exception, deriving training needs and ‘digital resilience’ requirements for signalling staff. These observations are consistent with our “zero-hit” result for the combined filter: digital competency $\wedge$ operational personnel $\wedge$ cybersecurity $\wedge$ railway.

The diagnosed gap is systemic rather than incidental. From a safety management perspective, the implications are twofold. First, the evidence-based management agenda requires the collection of research from different streams (Rousseau, 2006). In practice, this means designing a competency mapping process in line with the European Digital Competency Framework for Citizens (DigComp) for specific artefacts and safety procedures applicable to railway operations.

Regarding competencies, the reference source is the domains and proficiency levels described in the newer versions of DigComp, including information and data literacy, communication and collaboration, digital content creation, security, problem solving, and an emphasis on AI and data literacy (Vuorikari, Kluzer, Carretero, 2022). As regards operational practices, mapping should include the operation of ETCS/ERTMS (European Train Control System / European Railway Traffic Management System) systems, including working with traffic procedures and cab screens; cyber hygiene practices at front-line workstations (password management, updates, phishing recognition, proper use of media and access); and interaction with HMI (Human–Machine Interface) interfaces in the cab and at stations. The next step is to incorporate these dimensions into the Safety Management System (SMS) metrics so that the results of digital competency evaluation feed into established indicators such as procedural compliance, frequency and nature of near misses, response times, reporting rates and organisation learning (Liu, Wang, Gao, 2023).

At the same time, in line with the paradigms of High Reliability Organizations (HROs) and the Safety-II concept, the focus should shift to the positive capabilities of the system: resilience, anticipation, monitoring, and responding/learning. It is these capabilities that digital competencies can strengthen in the daily work of line teams: better data proficiency promotes early detection of deviations, conscious cyber hygiene practices limit attack vectors, and more efficient work with HMI reduces cognitive load and the risk of operational errors (Weick, Sutcliffe, 2015; Hollnagel, 2017). The path is defined as follows:

DigComp → ETCS-ERTMS/HMI artefacts/procedures → KPIs in SMS → Safety-II/HRO potentials, creates a coherent management framework linking competency learning with operational safety (Weick, Sutcliffe, 2015; Hollnagel, 2014). Our data, with a predominance of social sciences and computer science, and a moderate contribution from management, suggest that the conceptual resources for such a translation exist but require the connection of previously separate networks of authors and institutions.

The geography of the output (Spain, UK, and the US as leaders) and the “hockey stick” growth trend after 2018 are consistent with the broader context: European digital competency programmes and research funding (Spain), mature publishing ecosystems (UK, USA) and increased demand for training and standards during the accelerated digitisation after 2020, including data security and remote working. This background legitimises the building of bridges between consortia in the field of education/competencies (strong in EU countries) and cyber-rail centres (strong in China and Scandinavia), which, as reviews show, focus on the technical layer and protection standards (e.g., EN/IEC) with less exposure to HR and safety culture issues.

Consequently, we propose sectoral segmentation of subsequent analyses: (A) a corpus of digital competencies filtered by a dictionary of frontline roles and railway terminology; (B) a cyber-railway corpus filtered by organisation descriptors (e.g., safety culture, SMS, training, human factors). The subcorpora defined in this way can then be linked using co-word and co-citation analysis, according to methodological recommendations for management (Zupic, Čater, 2015; Donthu et al., 2021). The goal is to obtain “bridges” between topics and authors and a list of candidates for common metrics (e.g., digital HMI proficiency, operational cyber hygiene, operational data literacy) compatible with SMS/HRO. This will shift the field from the currently dominant socio-educational and IT approach to an integrated organisation perspective demanded by operational security practice.

6. IMPLICATIONS FOR MANAGEMENT AND FURTHER RESEARCH

The results of bibliometrics and scientometrics suggest three directions for “horizontal” actions and several sectoral steps. First, it is necessary to create industry-specific keyword dictionaries. Our study shows the dominance of socio-educational and

IT approaches, along with weaker visibility of managerial and operational perspectives. The taxonomy of descriptors combining DigComp (e.g., “safety & security”, “problem solving” extended to include AI) with SMS/HRO and railway terminology (e.g. ETCS/ERTMS, HMI, ICS/SCADA) and with the terms safety culture and cyber maturity (Zupic, Čater, 2015; Donthu et al., 2021; Vuorikari et al., 2022). The dictionary constructed in this way should be published and maintained as a “living document” so that it can be used in articles, grants, and data repositories.

Secondly, a standardised list of operational role descriptors in publications (e.g., train driver, dispatcher/traffic controller, signalling technician, station operator, rolling-stock maintainer) is recommended. Our “zero-hit” results for the combination of four areas (digital competencies $\wedge$ operational personnel $\wedge$ cybersecurity $\wedge$ railways) indicate that the lack of a standard for naming roles weakens the sensitivity of queries and hinders the integration of literature streams. In practice, we recommend preparing a “map of synonyms” (EN/PL and other languages), the inclusion of descriptors in keywords and abstracts, and their control versions in repositories (ORCID/CRediT for author roles and “role keywords” for operational roles). The summary and illustrations of the gaps in our study can serve as a model for such standardisation.

Thirdly, data and metadata reporting should be required to facilitate the replication of bibliometric analyses: full query specifications (fields, restrictions, export date), .csv/.ris files, software versions, normalisation metrics and thresholds (e.g., a threshold of ≥ 4 occurrences for co-words, justified by the complexity of the network in the cyber-rail network), as well as PRISMA diagrams. These recommendations are consistent with the methodological guidelines for management reviews and systematic reviews (Donthu et al., 2021; Page et al., 2021), and in the area of science mapping, with VOSviewer practice (Van Eck, Waltman, 2010).

Finally, considering the geography of achievements and co-authorship networks, it is worth initiating cross-regional consortia: centres with strong achievements in competencies (Spain, UK) with cyber-rail teams (China, Sweden, Singapore), with an explicitly agreed dictionary and metadata package. This focus will increase the visibility of work at the intersection of “competency–security–operations” and reduce the linguistic/indexing bias indicated in our data.

7. LIMITATIONS

This study is subject to several limitations that should be considered when interpreting the findings.

First, the analysis relies on a single bibliographic database (Scopus). Although Scopus offers broad multidisciplinary coverage and high-quality metadata, database-specific indexing policies may bias the visibility of certain regions, journals, and disciplines. Future work should triangulate the results with complementary sources (e.g., Web of Science, Dimensions, Crossref) to test the robustness of trends and network structures.

Second, the search was restricted to English-language, final-stage journal articles. While this improves comparability and metadata quality, it underrepresents non-English research outputs, conference proceedings, and grey literature (e.g., standards, governmental and industry reports) that can be particularly relevant for security policy in regulated, high-risk sectors.

Third, keyword ambiguity and synonymy (e.g., digital competency/competence, digital skills, ICT skills) may affect both sensitivity and specificity of retrieval, even after cleaning procedures. Furthermore, operational role descriptors in railways are not standardised in metadata, which can hinder sector-specific mapping.

Fourth, the results of network analyses are sensitive to parameter choices (normalisation and occurrence thresholds). The adopted settings were selected to improve map readability, but they may attenuate niche topics with high practical relevance.

Finally, recent-year counts (especially for 2025) should be treated as provisional due to indexing delays.

The analysis is based on a single bibliographic source (Scopus). Scopus was chosen as the most representative source for bibliometric analyses because it combines a broad and balanced coverage of disciplines with high-quality metadata and a transparent selection policy. First, inter-database comparisons show that Scopus indexes more titles than Web of Science in many areas, especially in the social sciences and applied fields, thus better reflecting multidisciplinary topics such as “digital competencies”, where scientific publications are scattered (Mongeon, Paul-Hus, 2016). This broader coverage also results in greater completeness of the citations, approximately 20% more than WoS in cross-sectional studies, which stabilises impact estimates and citation networks, important for co-occurrence and co-authorship maps (Falagas et al., 2008; Kulkarni et al., 2009). Second, Scopus content is curated by an independent Content Selection & Advisory Board (CSAB), and the publicly available Content Coverage Guide describes the selection criteria and activities of local councils (including for non-English-speaking countries); this transparency of selection and standardisation of metadata increases the reliability and replicability of analyses (Elsevier, 2022). Third, in large-scale comparisons, Scopus performs well against WoS, Dimensions, and Crossref in terms of record completeness and citation link quality, which is critical for the quality of network models (Visser, Van Eck, Waltman, 2021; Harzing, Alakangas, 2016).

Furthermore, a conscious decision was made to limit the search to English and the document type “article” (final), which improves the comparability and quality of metadata, but underestimates grey literature (white papers, standards, government reports) and publications in other languages, which may more accurately reflect implementation practices (e.g., in regulated sectors). An additional limitation is the variability and ambiguity of keywords (e.g., dispersion between “digital skills”, “digital competency”, “ICT skills”), which affects the sensitivity and specificity of queries; despite metadata cleaning procedures, there remains a risk of attribution errors, e.g., synonyms, homonyms, and varying naming conventions for

operational roles. The results of network analyses, e.g., co-occurrence, co-authorship, are sensitive to threshold and normalisation settings; the adopted parameters improve the readability of maps, but may muffle niche threads of high practical value. Indexing delays (especially for 2025) should also be taken into account, as they mean that data from the most recent period is incomplete. Finally, assigning publications to fields in the database classification carries the risk of cross-domain categorisation errors, and aggregation at the country level does not distinguish between the intensity of cooperation between sectors. All these factors suggest that the results should be treated as a conservative estimate of the scale and structure of the research field and justify replication using multi-source queries and extended linguistic and typological criteria.

8. CONCLUSIONS

The bibliometric and scientometric analysis confirms the maturity and scale of the field of “digital competencies” and, at the same time, clearly reveals a significant research gap at the intersection of: digital competencies $\wedge$ operational/front-line personnel $\wedge$ cybersecurity $\wedge$ railways. In the combined query, no articles meeting all four criteria were identified in any of the areas, which made it impossible to construct a common map of co-occurring concepts and thus indicates a lack of a quantified, sectoral perspective combining a competency approach with digital security in the railway environment. The analysis of concept pairs confirms the existence of two developed but separate streams: digital competency $\wedge$ cybersecurity (84-87 works) and cybersecurity $\wedge$ railway (74-75 works). Only one publication deals with the combination of cybersecurity of operational personnel $\wedge$, which shows that the “people in the system” component remains marginal. We are therefore dealing with a systemic gap, not an ad hoc one, requiring the design of a purposeful research agenda.

The results should be interpreted in the context of the rapid growth of output in recent years: after isolated mentions until 2022, there is a jump in 2023 (15), culminating in 2024 (1003) with a preliminary 681 items in 2025. At the same time, the map of terms for “cyber-rail” focuses on technical topics (cyber-physical systems, network security, IoT, deep learning, reliability, vulnerability/risk management), which explains why the organisation and personnel component remains less visible in metadata and keywords.

In subsequent research steps, a detailed theme of “cybersecurity in the railway sector” will be developed in the logic of in-depth network mapping: co-occurrence of concepts and clusters, co-authorship networks, and exploration of “management interventions” in metadata. This sequence corresponds to the zero-hit diagnosis and allows us to move from the observation of a gap to an operational research framework for security and competency management policies in the railway sector.

LITERATURE

- Alhloul, A., Kiss, E. (2022). Industry 4.0 as a challenge for the skills and competencies of the labor force: A bibliometric review and a survey. *Sci*, 4(3), 34, <https://doi.org/10.3390/sci4030034>.
- Amano, T., González-Varo, J.P., Sutherland, W.J. (2016). Languages are still a major barrier to global science. *PLOS Biology*, 14(12), e2000933, <https://doi.org/10.1371/journal.pbio.2000933>.
- Bhuiyan, M.R.H., Ibtihal, S.A., Nokshi, K.N. (2023). Involvement of human and organizational factors in railway accidents: Application of the Human Factors Analysis and Classification System and Bayesian network. *Transportation Research Record*, 2677(6), 505-518, <https://doi.org/10.1177/03611981231156932>.
- Brand, A., Allen, L., Altman, M., Hlava, M., Scott, J. (2015). Beyond authorship: Attribution, contribution, collaboration, and credit. *Learned Publishing*, 28(2), 151-155, <https://doi.org/10.1087/20150211>.
- Bu, B., Wu, W. (2019). Security analysis for CBTC systems under attack–defense confrontation. *Electronics*, 8(9), 991, <https://doi.org/10.3390/electronics8090991>.
- Carretero Gómez, S., Vuorikari, R., Punie, Y. (2017). *DigComp 2.1: The Digital Competency Framework for Citizens with eight proficiency levels and examples of use*. Publications Office of the European Union.
- Childers, S. (2003). Computer literacy: Necessity or buzzword? *Library Philosophy and Practice*, 5(2), 1-10, <https://digitalcommons.unl.edu/libraryscience/97>.
- Dadashi, N., Wilson, J.R., Golightly, D., Sharples, S. (2014). A framework to support human factors of automation in railway intelligent infrastructure. *Ergonomics*, 57(3), 387-402, <https://doi.org/10.1080/00140139.2014.893026>.
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., Lim, W.M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, 133, 285-296.
- Dykan, V., Ovchynnikova, V., Dykan, V., Kalicheva, N., Korin, M. (2019). Strategic knowledge management as means of ensuring the competitiveness of railway transport enterprises. *SHS Web of Conferences*, 67, 01003, <https://doi.org/10.1051/shsconf/20196701003>.
- Elsevier (2022). *Scopus content coverage guide*. Elsevier. Retrieved from https://www.elsevier.com/_data/assets/pdf_file/0007/69451/Scopus_ContentCoverage_Guide_WEB.pdf.
- Elsevier (2025). *Scopus content: What is included*.
- Falagas, M.E., Pitsouni, E.I., Malietzis, G.A., Pappas, G. (2008). Comparison of PubMed, Scopus, Web of Science, and Google Scholar: Strengths and weaknesses. *The FASEB Journal*, 22(2), 338-342, <https://doi.org/10.1096/fj.07-9492LSF>.
- Guo, Z., Pang, H., Zhang, J., Zhang, J., Wang, J., He, C., Li, C. (2025). Using HFACS to understand human error in railway dispatcher performance: A study of proactive safety inspection records. *Ergonomics*, 68(1), 37-50, <https://doi.org/10.1080/00140139.2023.2287975>.
- Haak, L.L., Fenner, M., Paglione, L., Pentz, E., Ratner, H. (2012). ORCID: A system to uniquely identify researchers. *Learned Publishing*, 25(4), 259-264, <https://doi.org/10.1087/20120404>.

- Haddaway, N.R., Collins, A.M., Coughlin, D., Kirk, S. (2015). The role of grey literature in evidence syntheses for environmental science and policy. *Environmental Evidence*, 4(1), 1-13, <https://doi.org/10.1186/s13750-015-0043-3>.
- Harzing, A.-W., Alakangas, S. (2016). Google Scholar, Scopus, and the Web of Science: A longitudinal and cross-disciplinary comparison. *Scientometrics*, 106(2), 787-804, <https://doi.org/10.1007/s11192-015-1798-9>.
- Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Ashgate.
- Hollnagel, E. (2017). *Safety-II in practice: Developing the resilience potentials*. Routledge, <https://doi.org/10.4324/9781315201047>.
- Huu, P.T. (2023). Impact of employee digital competence on the relationship between digital autonomy and innovative work behavior: A systematic review. *Artificial Intelligence Review*, 56, 14193-14222, <https://doi.org/10.1007/s10462-023-10492-6>.
- Ilomäki, L., Paavola, S., Lakkala, M., Kantosalo, A. (2016). Digital competency – An emerging boundary concept for policy and educational research. *Education and Information Technologies*, 21(3), 655-679, <https://doi.org/10.1007/s10639-014-9346-4>.
- Katz, J.S., Martin, B.R. (1997). What is research collaboration? *Research Policy*, 26(1), 1-18, [https://doi.org/10.1016/S0048-7333\(96\)00917-1](https://doi.org/10.1016/S0048-7333(96)00917-1).
- Kulkarni, A.V., Aziz, B., Shams, I., Busse, J.W. (2009). Comparisons of citations in Web of Science, Scopus, and Google Scholar. *JAMA*, 302(10), 1092-1096, <https://doi.org/10.1001/jama.2009.1307>.
- Lampe, I., Arifin, K., Ali, M., Mahfudz, M., Samad, M., Ciyo, M.B., Khairil, M., Derahim, N., Wan Isa, W.M.Z. (2021). Organizational safety climate factor model in the urban rail transport industry through CFA analysis. *Sustainability*, 13(5), 2939, <https://doi.org/10.3390/su13052939>.
- Liu, J., Wang, Y., Deng, C., Jin, Z., Wang, G., Yang, C., Li, X. (2023). Research on safety supervision and management system of China railway based on association rule and DEMATEL. *PLOS ONE*, 18(12), e0295755.
- Lopez, I., Aguado, M., Arsuaga, I., Toledo, N. (2018). A framework for vulnerability detection in European train control railway communications. *Security and Communication Networks*, 2018, <https://doi.org/10.1155/2018/5634181>.
- López-Aguilar, P., Batista, E., Martínez-Ballesté, A., Solanas, A. (2022). Information security and privacy in railway transportation: A systematic review. *Sensors*, 22(20), 7698, <https://doi.org/10.3390/s22207698>.
- Mongeon, P., Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics*, 106(1), 213-228, <https://doi.org/10.1007/s11192-015-1765-5>.
- Nunen, K. van, Reniers, G., Ponnet, K. (2022). Measuring safety culture using an integrative approach: The development of a comprehensive conceptual framework and an applied safety culture assessment instrument. *International Journal of Environmental Research and Public Health*, 19(20), 13602, <https://doi.org/10.3390/ijerph192013602>.
- Page, M.J. et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71, <https://doi.org/10.1136/bmj.n71>.

- Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71, <https://doi.org/10.1136/bmj.n71>.
- PRISMA (2021). *PRISMA 2020 flow diagram*. Retrieved from org/prisma-2020-flow-diagram.
- Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.
- Retbi, A., Bennani, S., Ragala, Z. (2023). An approach of ontology and knowledge base for railway maintenance. *International Journal of Electrical and Computer Engineering*, 13(5), 5282-5295, <https://doi.org/10.11591/ijece.v13i5.pp5282-5295>.
- Rousseau, D.M. (2006). Is there such a thing as evidence-based management? *Academy of Management Review*, 31(2), 256-269.
- Soderi, S., Masti, D., Hämäläinen, M., Iinatti, J. (2023). Cybersecurity considerations for communication based train control. *IEEE Access*, 11, 91133-91148, <https://doi.org/10.1109/ACCESS.2023.3309005>.
- Soderi, S., Masti, D., Lun, Y.Z. (2023). Railway cyber-security in the era of interconnected systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, 24(7), 6764-6779, <https://doi.org/10.1109/TITS.2023.3254442>.
- Thron, E., Faily, S., Dogan, H., Freer, M. (2024). Human factors and cyber-security risks on the railway: The critical role played by signalling operations. *Information & Computer Security*, 32(2), 236-263, <https://doi.org/10.1108/ICS-05-2023-0078>.
- Van Eck, N.J., Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, 84(2), 523-538, <https://doi.org/10.1007/s11192-009-0146-3>.
- Van Laar, E., Van Deursen, A.J.A.M., Van Dijk, J.A.G.M., de Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behavior*, 72, 577-588.
- Visser, M., van Eck, N.J., Waltman, L. (2021). Large-scale comparative analysis of bibliographic data sources: Scopus, Web of Science, Dimensions, Crossref, and Microsoft Academic. *Quantitative Science Studies*, 2(1), 20-41, https://doi.org/10.1162/qss_a_00112.
- Vuorikari, R., Kluzer, S., Carretero, S. (2022). *The Digital Competency Framework for Citizens (DigComp 2.2): With new examples of knowledge, skills, and attitudes and a focus on AI and data literacy*. Publications Office of the European Union, <https://doi.org/10.2760/115376>.
- Wagner, C.S., Leydesdorff, L. (2005). Network structure, self-organization, and the growth of international collaboration in science. *Research Policy*, 34(10), 1608-1618, <https://doi.org/10.1016/j.respol.2005.08.002>.
- Weick, K.E., Sutcliffe, K.M. (2015). *Managing the unexpected: Sustained performance in a complex world*. Wiley.
- Zupic, I., Čater, T. (2015). Bibliometric methods in management and organization. *Organization Research Methods*, 18(3), 429-472, <https://doi.org/10.1177/1094428114562629>.

KOMPETENCJE CYFROWE I ZARZĄDZANIE WIEDZĄ U OPERATORÓW KOLEJOWYCH: GLOBALNE BADANIE BIBLIOMETRYCZNE (1975-2025) ORAZ IMPLIKACJE DLA POLITYKI BEZPIECZEŃSTWA

Streszczenie

Kompetencje cyfrowe stały się jednym z kluczowych obszarów badań współczesnych nauk o zarządzaniu, stanowiąc fundament zarządzania wiedzą, zdolności adaptacyjnych oraz odporności organizacyjnej, szczególnie w sektorach wysokiego ryzyka i wysokiej odpowiedzialności operacyjnej. Ich znaczenie wzrosło wraz z postępującą cyfryzacją procesów organizacyjnych oraz rozwojem technologii wspierających bezpieczeństwo i ciągłość działania.

Celem artykułu jest identyfikacja, analiza oraz wizualizacja globalnych trendów badawczych dotyczących kompetencji cyfrowych w latach 1975-2025, a także określenie implikacji tych badań dla projektowania polityki bezpieczeństwa i rozwoju kompetencji u operatorów kolejowych.

Zastosowano analizę bibliometryczną i scjentometryczną opartą na bazie Scopus, wykorzystując procedurę selekcji PRISMA oraz narzędzie VOSviewer do analizy współwystępowania słów kluczowych i mapowania sieci badawczych.

Wyniki wskazują na wykładniczy wzrost liczby publikacji, dominację nauk społecznych i informatyki oraz relatywnie ograniczoną obecność nauk o zarządzaniu. Literatura dotycząca kompetencji cyfrowych stanowi dojrzałą bazę wiedzy możliwą do wykorzystania przy projektowaniu sektorowych polityk bezpieczeństwa i modeli kompetencyjnych w transporcie kolejowym.

Słowa kluczowe: bibliometria, Scopus, zarządzanie wiedzą, VOSviewer, scjentometria, bezpieczeństwo organizacji, kompetencje cyfrowe