Journal of Applied Economic Sciences
Volume XX, Winter, Issue 4(90), 2025

The Global Economics of Knowledge Protection: A Bibliometric Analysis of Cybersecurity and Intellectual Capital Research

Darya DANCAKOVÁ
https://orcid.org/0000-0003-1621-6431
Department of Banking and Investment
Faculty of Economics, Technical University of Košice, Slovakia
darya.dancakova@tuke.sk

Article's history:
Received 15th of October, 2025; *Revised* 6th of November, 2025; *Accepted* 21th of November, 2025; *Available online*: 30th of December, 2025. *Published* as article in the Volume XX, Winter, Issue 4(90), December, 2025.

Suggested citation:
Dancaková, D. (2025). The Global Economics of Knowledge Protection: A Bibliometric Analysis of Cybersecurity and Intellectual Capital Research. *Journal of Applied Economic Sciences*, Volume XX, Winter, 4(90), 695 – 715. https://doi.org/10.57017/jaes.v20.4(90).04

Abstract:
This study analyses the global patterns of intellectual capital protection, showing how cybersecurity functions as a key mechanism for preserving knowledge assets that support economic development and national security. Using a dataset of 3,772 publications indexed in the Web of Science (2000–2025), a comprehensive bibliometric analysis uncovers the global dynamics driving scientific productivity in this emerging field. The results reveal significant differences in national performance, assessed by publication output, citation impact, and collaboration intensity. The United States and China lead in both volume and influence, acting as key global hubs of international activity. Research networks that enhance global visibility through partnerships. At the author level, the findings indicate that scholarly impact relies less on quantity and more on visibility, collaboration, and citation resonance, highlighting a shift from productivity-driven to influence-oriented research recognition. Overall, the study shows that IC–cybersecurity scholarship is shaped by a highly concentrated global structure, where a few leading nations and influential authors set the intellectual agenda through sustained collaboration and cross-disciplinary engagement.

Keywords: knowledge economy; intangible assets; intellectual capital; economic security; cyber-security; innovation policy.

JEL Classification: O34.

Introduction

The widespread adoption of the internet and the accelerating pace of digitalisation have fostered a cyber environment in which intangible assets and organisational knowledge constitute key drivers of value creation. Technological advancements have progressively redirected attention from physical resources toward intangible forms of capital, such as knowledge, intellectual property, and brand reputation. Within this framework, the period from 2000 to 2025 provides a critical window for analysis, encompassing major developments and structural shifts in the digital landscape. The year 2000 marks the onset of the global internet era, which catalysed unprecedented digital transformation, while 2025 serves as a logical endpoint, capturing the most recent data available and reflecting the anticipated trajectory of ongoing digital evolution. Consequently, organizations no longer rely solely on tangible, traditional sources of value but increasingly recognize the importance of intangible assets, more broadly referred to as intellectual capital (IC), which became the most valuable asset of any modern organization (Balozian et al., 2022).

The fast-evolving cyber environment and the growing complexity of digital threats present significant challenges to the security of organizational intellectual capital. In response to these risks, a new line of research is taking shape within the field of intellectual capital, focusing on the protection of intangible assets from the cyber security perspective (Von Solms & Von Solms, 2018; Renaud et al.,2019; Balozian et al., 2022; Yilmaz & Tuzlukaya, 2024; Hong et al., 2025). When considering the protection of corporate intellectual capital, human capital increasingly emerges as a central point of focus. Existing research underscores that safeguarding intellectual capital constitutes a multifaceted challenge, one that begins with fostering cyber-risk awareness across all levels of organisational human capital, from frontline employees to executive leadership. It is equally important to recognise that the cybersecurity of intellectual capital should not be viewed solely as a corporate responsibility. Universities and higher education institutions also confront significant challenges in protecting their intellectual assets, particularly as they navigate the complex demands of the contemporary cyber landscape (Bongiovanni et al., 2020).

A comprehensive understanding of intellectual capital, enterprise-level cybersecurity, and their interrelationship is essential for advancing research in this area. This study applies bibliometric analysis to address the following research questions:

RQ 1: What identifiable trends exist in the volume and growth of publications at the intersection of intellectual capital and cybersecurity over time?

RQ 2: Which countries lead in research productivity and impact in this area?

RQ 3: How are international research collaborations organized, and which countries act as central or bridging entities within the global network?

RQ 4: Who are the most prolific and influential authors in this field based on bibliometric indicators?

RQ 5: What topics are prominent among the most influential and highly cited global publications, and what do they indicate about emerging research directions?

The paper is organised as follows: The literature review begins by outlining the theoretical foundations of corporate intellectual capital, emphasising its core components, human, structural, and relational capital, and explaining their importance in the digital era. It then examines how intellectual capital interacts with cybersecurity management within organisations. The next section describes the research design, detailing the approach and methods used in the study. Following this, the results section presents and discusses the main findings from the bibliometric analysis. The paper concludes with final remarks that synthesise the key insights and suggest possible directions for future research.

1. Research Background

1.1. Definition of Intellectual Capital in the Cyber Era

The term *intellectual capital* was first introduced in 1969 by economist John Kenneth Galbraith, who characterised it as a dynamic form of capital emerging from creative mental activity (Galbraith, 1969). For several decades, however, corporate intellectual capital remained a somewhat elusive concept, widely acknowledged in theory, yet difficult to define and measure explicitly in practice for several decades, corporate intellectual capital remained an elusive concept, widely acknowledged in theory but difficult to define and measure in practice. A significant shift occurred in the 1990s, when Peter Drucker anticipated the emergence of the "knowledge economy". Drucker argued that knowledge should be regarded as the most important productive resource of the modern age, rather than merely one of several production factors (Drucker, 1993). Similarly, Toffler (1990) foresaw that knowledge, due to its limitless nature, would eventually surpass all other resources as the foundation for sustainable economic development.

Building on these early insights, the concept of intellectual capital has received significant attention over the past three decades in both academic and managerial contexts. Scholars such as Brooking, Edvinsson, Malone, and Stewart advanced the concept, focusing on the identification and classification of intangible assets within organisations (Brooking, 1996; Edvinsson & Malone, 1997; Stewart, 1997). Although intangible assets, by their very nature, lack physical form and often fall outside the scope of traditional financial reporting frameworks, they play an important role in the creation of corporate value (Elsten & Hill, 2017). Considering their growing significance, investments in intangible assets and intellectual capital have increasingly emerged as key drivers of competitive advantage in today's fast-paced, globalised, and digitally oriented economies (Madhani, 2012; Thum-Thysen et al., 2017). For this reason, the academic literature increasingly underscores the strategic importance of corporate intellectual capital, often describing it as one of the most important assets of modern organisations (Renaud et al., 2019; Balozian et al., 2022).

Although the definition of corporate intellectual capital (IC) may vary across studies, it is commonly understood as a multidimensional concept comprising various forms of knowledge and intangible resources that support value creation within organisations (Ali et al., 2021; Cabrilo et al., 2024). Broadly understood, IC exists in all organisations as a stock of knowledge-based resources that can be leveraged in the value creation process (Kianto et al., 2023). It encompasses intellectual material, including knowledge, experience, intellectual property, and information, which organizations utilize to generate value (Dumay, 2016).

In the context of the digital age, intellectual capital is considered essential for maintaining competitiveness and ensuring operational efficiency within organizations (Al-Alawi & Alghasra, 2024). The literature consistently describes corporate intellectual capital (IC) using a three-component framework: human capital, structural capital, and relational capital (Stewart, 1997; Youndt & Subramaniam, 2004; Díaz-Vega, 2024). Specifically, while human capital, primarily represented by employees, is considered a key component of intellectual capital and the most important source of knowledge within a company (Nonala & Kenney, 1991), it also represents the most vulnerable and weakest link in the protection of intellectual capital from a cybersecurity perspective (Balozian et al., 2022; Garcia-Perez et al., 2023). In contrast, structural and relational capital consist of codified forms of knowledge and information, including internal processes, procedures, customer relationships, and organizational frameworks, which are often the primary targets of cybersecurity efforts and therefore require robust protection to ensure secure and uninterrupted value creation. Structural capital facilitates the efficient flow of information, relational capital fosters trust that enables the sharing of cybersecurity knowledge, and human capital promotes a proactive cybersecurity culture. Together, these dimensions allow organizations to pool resources, reduce operational costs, and develop capabilities that strengthen cyber resilience and support sustained value creation (Ali-Hassan, 2009; Ode et al., 2025). Beyond safeguarding existing knowledge, these forms of intellectual capital also play a pivotal role in enhancing organizational readiness for AI adoption. In particular, relational capital reinforces cyber resilience, a critical capability for protecting and creating organizational value. Moreover, cyber resilience serves as a mediating mechanism, linking relational capital to AI readiness and enabling organizations to maintain value creation even in the face of cyber-related disruptions (Ode et al., 2025).

1.2. Managing Intellectual Capital Cyber Security

Cybersecurity has increasingly attracted attention from the academic community, practitioners, stakeholders, and boards of directors due to its profound and long-term implications (Tosun, 2021). While it is often perceived primarily as a technical issue, traditionally handled by IT specialists and technicians, effectively managing cybersecurity has proven to be a complex challenge for both practitioners and researchers (Khadka & Ullah, 2025). In this context, cybersecurity refers to the security, integrity, and confidentiality of information within cyberspace (Schatz et al., 2017). More specifically, it encompasses a set of approaches and actions that fall under the broader umbrella of information security. Nevertheless, the two concepts should not be viewed interchangeably.

The key distinction is that information security is concerned with protecting data in general, whereas cybersecurity specifically focuses on the preservation, retention, and transmission of data in online and networked environments (Von Solms & Von Solms, 2018). Furthermore, it is important to emphasise that whenever the "Internet" is involved in the storage or transmission of any element of intellectual capital, its protection becomes a matter of cybersecurity governance. Given that the informational components of intellectual capital are retained and transmitted digitally, effective cybersecurity governance is therefore essential to ensure their safeguarding and security (Renaud et al., 2019).

The dynamics of cyber risk have intensified considerably during the global COVID-19 pandemic, further complicating the protection of intellectual capital as organisations increasingly rely on digital infrastructure (Petratos, 2021; Garcia-Perez et al., 2023). As cyberattacks and data breaches now occur with alarming frequency, ensuring the protection of intellectual capital has become a strategic priority. This is because cybercrime weakens a company's capacity to create potential value from its intellectual capital, as it threatens the confidentiality, integrity, and availability of essential organisational data (La Torre et al., 2018). Moreover, cyber threats present a significant challenge to the protection of intellectual property (IP) across various sectors, including information technology, pharmaceuticals, media, and manufacturing, as attackers, ranging from cybercriminals and insiders to state-sponsored groups and competitors, exploit digital vulnerabilities to steal trade secrets, proprietary algorithms, and research data (Mavani at al., 2024).

Several studies emphasise that cybersecurity incidents, such as cyber espionage, ransomware attacks, and large-scale data breaches, not only compromise the security of intellectual property but also expose organisations to significant financial, legal, and reputational risks (Snyder & Crescenzi, 2013). For example, Ali et al. (2024) report that such incidents can substantially affect firm performance. Their findings further suggest that effective knowledge management, as embodied in a company's intellectual capital, can help mitigate the loss of investor confidence following a security breach. In a similar vein, Avery (2021) argues that data breaches may act as a catalyst for improving an organisation's long-term effectiveness. Importantly, while breaches generally hurt profitability, the study found no evidence that organisations experience significantly better or worse performance in either the short or long term. Overall, these results indicate that organisations can remain financially sustainable for up to four quarters following the disclosure of a data breach. Consequently, addressing cybersecurity risks requires more than technological solutions alone. It also depends critically on the awareness, behaviour, and engagement of employees, whose everyday actions are central to preventing and mitigating information security incidents (He et al., 2020). As highlighted by recent research, most cyber breaches stem from human error or negligence, underscoring that employees' knowledge, awareness, and behaviour—key components of human capital, are essential to strengthening cybersecurity through continuous training and a robust security culture (Ayereby, 2018; Bana et al., 2025).

2. Research Methodology

This study uses a bibliometric analysis, combining both quantitative and qualitative methods, to explore the research area linking intellectual capital and cybersecurity, considering the growing need to safeguard organizations' intangible assets. Data were sourced from the Web of Science (WoS) database for its extensive coverage of high-quality, peer-reviewed research published in leading academic journals. The dataset was extracted on June 19, 2025, in Bib TeX format.

Relevant publications were identified through a focused bibliometric search that captured research linking intellectual capital and cybersecurity. The search string included keywords related to intangible assets, knowledge management, and intellectual property, combined with a broad range of cybersecurity-related terms. The full query was as follows:

(("intangible" OR "intellectual*" OR "IC theory" OR "intellectual capital" OR "intangible asset*" OR "knowledge management" OR "intellectual material" OR "intellectual asset*" OR "intellectual property protection" OR "knowledge security") AND ("cyber-physical system*" OR "cyber-security" OR "cyber security" OR "cybersecurity" OR "cyber*" OR "cyber awareness" OR "information security" OR "cyber threat*" OR "cyber-attack*" OR "cyber-attack*" OR "cyber risk*" OR "IC security" OR "intellectual property theft*" OR "digital security" OR "information breach" OR "intellectual capital cyber security" OR "cyber breach"))*

To ensure the reliability and transparency of the bibliometric analysis, the PRISMA framework (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) was applied, in line with the methodology developed by Moher et al. (2009) and further updated by the PRISMA Group in 2020 (Page et al., 2021). Although originally designed for systematic reviews and meta-analyses, this structured approach has been adapted for use in bibliometric research to clearly document the identification, screening, and inclusion of relevant records. By applying the PRISMA framework, this study ensures a transparent and methodical approach to data collection and analysis. Such transparency is essential for maintaining the integrity, reliability, and reproducibility of bibliometric research. Rather than emphasizing its roots in evidence-based research, this study focuses on PRISMA's strength in providing clarity and consistency throughout the review process, demonstrating its usefulness across a wide range of research areas.

In interpreting the bibliometric data, the study adopts an applied economic perspective, viewing patterns of publication activity, citation impact, and international collaboration as quantitative signals of national research intensity and knowledge-protection capacity. These indicators collectively reflect the distribution of intellectual capital that underpins innovation performance and long-term economic development (Archibugi & Coco, 2004; de Frutos-Belizón et al., 2024).

2.1 Data Description

The search covered publications from 2000 to 2025 and was limited to full records and cited references. The search process yielded a total of 4,429 documents that matched the intellectual capital and cyber-security related keywords well.

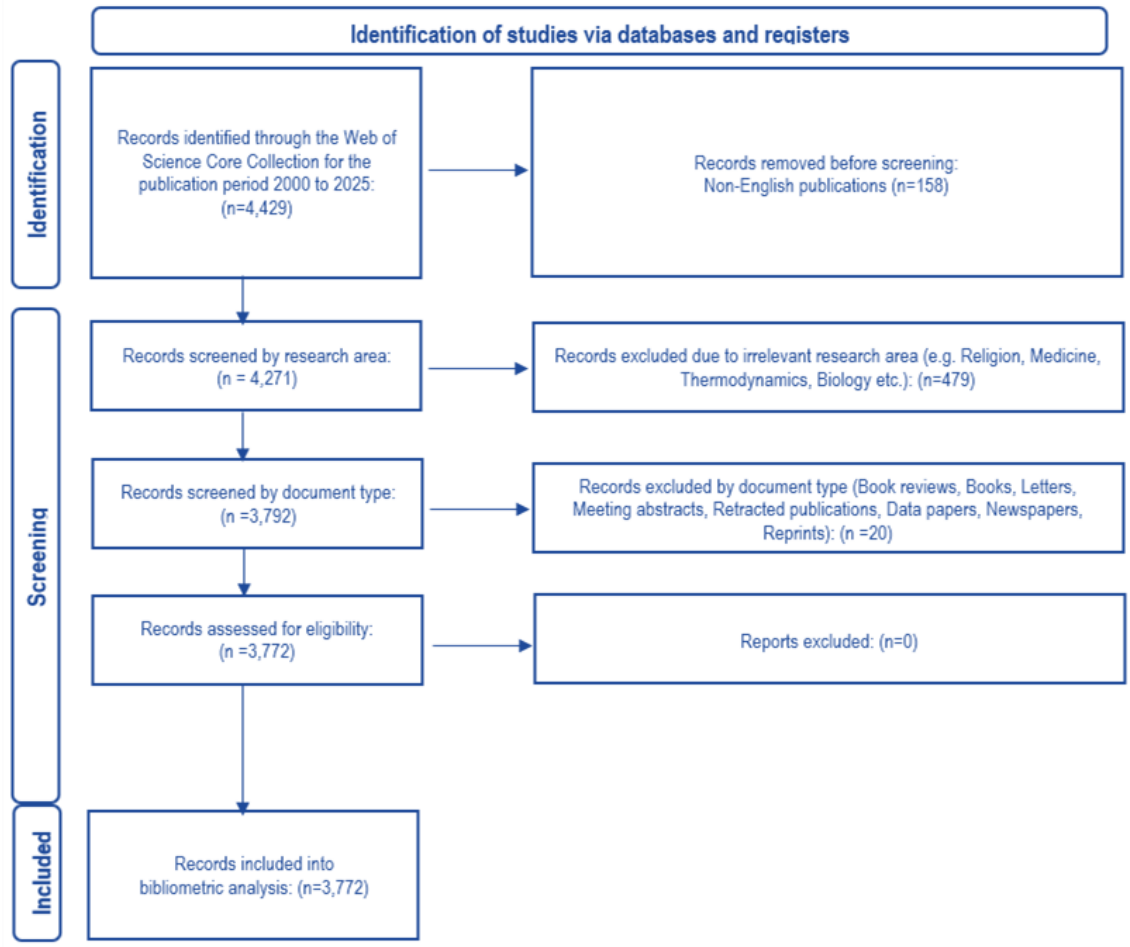
Table 1. Data description

Description	Results
Timespan	2000:2025
Sources (Journals, Books, etc.)	1,967
Documents	3,772
Articles	1,343
Annual Growth Rate %	5,59
Document Average Age	9,11
Average citations per doc	11,08
References	118,094
Keywords Plus (ID)	2,333
Author's Keywords (DE)	10,443
Authors	10,776
Authors of single-authored documents	630
Single-authored documents	678
Co-Authors per Document	3,5
International co-authorships %	20,65

Source: Own elaboration

The dataset comprised various document types, including conference papers, research articles, review papers, book chapters, early access documents and other publication categories. Proceedings and conference papers accounted for the largest portion of all publications (2,188), representing more than 49%, followed by research articles, which made up the second largest group with 2,099 documents, accounting for over 47%. While review articles (144) accounted for approximately 3,25 % of all documents, book chapters) accounted for approximately 2,87% of all documents. Editorial documents accounted for nearly 1% of all publications (44 in total). Letters, book reviews, books, meeting abstracts, and other publication categories collectively made up less than 1% of the total number of documents.

Figure 1: PRISMA flow diagram of documents selection



Source: Own elaboration

After applying the PRISMA process, which filtered for English-language publications and relevant research areas, a total of 3,772 records were obtained. This represents over 85% of the initial records retrieved from the Web of Science using the specified keywords. Notably, publications within “Computer Science” were the most prevalent, accounting for more than twice the volume of “Engineering”, which comprised 26.5% of the total. “Business Economics” represented approximately 14%, indicating a share less than half that of “Computer Science.” The remaining research areas each accounted for fewer than 10% of the records. This distribution underscores the central role of “Computer Science” in this research domain, while also highlighting the comparative prominence of “Engineering” over “Business Economics”.

The extracted data were then analysed in RStudio (Version 4.5.0) using the Bibliometrix (Version 4.0.0) package, developed by Aria & Cuccurullo (2017). This approach enabled comprehensive bibliometric mapping of the research landscape, facilitating the identification of key trends, influential publications, and thematic clusters. The analyses covered country-level productivity and collaboration, author-level impact, and the thematic evolution of intellectual capital and cybersecurity research, providing a multidimensional understanding of the field's development.

3. Results and Discussion

The number of publications connecting intellectual capital, intangible assets, cybersecurity, and related topics has increased over time. The trajectory of research output, as shown in Figure 2, reveals distinct periods of accelerated growth, particularly around 2008, 2015, and 2020.

Figure 2: Annual production of publications over the period from 2000 to 2025

Note: The Dotted line is the exponential trend line.
Source: Own elaboration

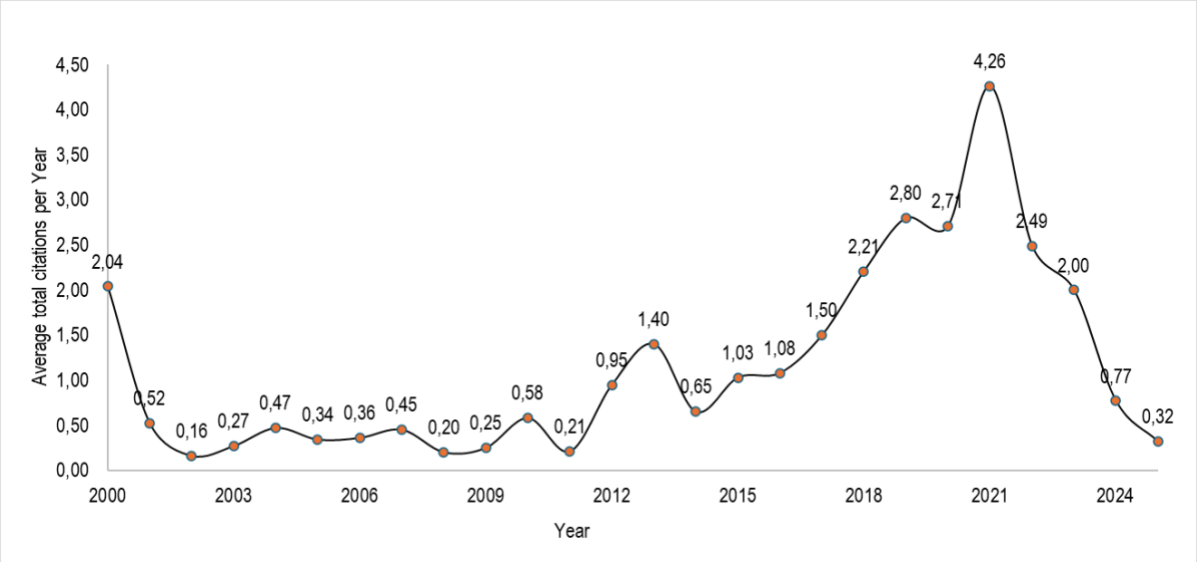
The initial surge in 2008 may be attributed to the global financial crisis, which underscored the strategic importance of intangible sources of value for firms (Landini et al., 2020), along with the rise of Web 2.0 and cloud computing, and heightened attention to intellectual property protection.

We assume that the next wave, which emerged around 2015, was driven by the rise of Industry 4.0 in 2011 and its growing popularity in the subsequent years (Madsen, 2019), along with the rapid expansion of mobile and cloud technologies and a surge in cyberattacks targeting prominent corporations and large retail chains.

The most recent increase in research output, observed after 2020, is linked to the COVID-19 pandemic, escalating geopolitical tensions, and advancements in artificial intelligence. These developments highlight the critical importance of knowledge security and the protection of intangible assets in national security discussions.

Figure 3 presents the annual average citations, defined as the mean number of citations per year received by publications in the dataset, thereby illustrating their overall influence on subsequent research within the field of intellectual capital and cybersecurity. The data indicate that citation activity reached its highest point in 2021, with an average of 4.26 citations per year. The trend shows an initial decline in scholarly attention following 2000, a period of relative stagnation throughout the 2000s, and a steady increase beginning around 2011, culminating in a pronounced surge between 2016 and 2021. This upward movement reflects the expanding academic interest and growing visibility of research at the intersection of intellectual capital and cybersecurity. The decline observed after 2021 likely results from the citation lag typically associated with more recent publications, which have had less time to accumulate scholarly recognition.

Figure 3: Average total annual number of citations



Source: Own elaboration

Research Productivity and International Collaboration by Country

Asia is the most productive region in terms of total research output, as shown in Table 2. China leads worldwide with 709 publications, followed by Malaysia (220), India (131), Japan (91), and Singapore. Although Singapore's output is smaller, it is notable for its impact. Citation performance varies across the region. China has a total of 7,212 citations, but its average citation per publication (AAC = 10.17) suggests a moderate influence relative to its size. Singapore has one of the highest average citations (AAC = 24.83), indicating its research is highly visible despite fewer publications. Malaysia and India have moderate citation impacts (AAC = 8.23 and 10.85), indicating that their research systems are becoming more active, but they have not yet accumulated a high number of citations.

Table 2: Country production and citation impact

	Rank	Country	NoP	Freq	SCP	MCP		Rank	Country	TC	AAC
Publication output	1	China	709	0.1936	592	117	Citation impact	1	USA	12,401	19.778
	2	USA	627	0.1712	503	124		2	China	7,212	10.172
	3	Malaysia	220	0.0601	176	44		3	United Kingdom	3,821	24.812
	4	Germany	188	0.0513	165	23		4	Malaysia	1,810	8.227
	5	Russia	156	0.0426	142	14		5	Italy	1,469	22.953
	6	United Kingdom	154	0.0420	109	45		6	India	1,421	10.847
	7	Ukraine	137	0.0374	111	26		7	Singapore	1,167	24.830
	8	India	131	0.0358	114	17		8	Turkey	1,113	92.750
	9	Australia	103	0.0281	65	38		9	Australia	951	9.233
	10	Japan	91	0.0248	81	10		10	France	868	14.230

Note: NoP – Number of Publications, Freq – The proportion of total publications, SCP – Single country publications, MCP – Multiple countries publications, TC – Total publications, AAC – Average Citation per Publication

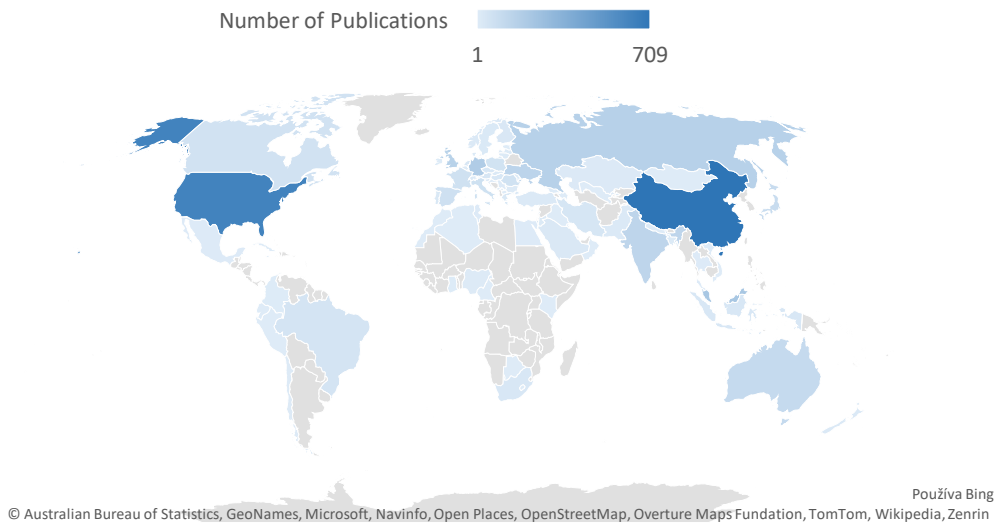
Source: Own elaboration

In North America, the United States remains a global leader in productivity and impact, with 627 publications and 12,401 citations. Its average citation rate (AAC = 19.78) is among the highest, reflecting a steady balance between research output and influence. This combination of strengths emphasizes the United States' key role in international research networks and its ability to generate work that receives significant global recognition.

Across Europe, a pattern of high-impact but smaller-scale productivity is evident. The United Kingdom exemplifies this with 154 publications and a remarkable 3,821 citations, resulting in an AAC of 24.81, which reflects a strong quality-to-quantity ratio. Italy also performs well with an AAC of 22.95, showing the significant influence of its research. Germany and Russia have higher publication counts, 188 and 156 respectively, but do not rank among the top ten by citations, indicating their impacts are more dispersed or specialized. Turkey emerges as an outlier, with fewer publications yet an exceptionally high AAC of 92.75, driven by a few highly cited papers that raise its average. In the Oceania region, Australia produces a significant number of publications (103) and garners a total of 951 citations, resulting in an AAC of 9.23. Although its impact per paper is moderate relative to that of leading European and Asian countries, Australia's prominent international collaborations likely boost its long-term citation reach.

The global distribution of scientific production, illustrated in Figure 4, highlights clear geographic disparities in research intensity. The deep-blue regions, corresponding to the United States and China, represent the highest concentration of publication activity, reflecting their strong R&D investment and advanced innovation ecosystems. By contrast, the lighter shades covering much of Europe, Africa, and Latin America indicate comparatively lower research capacity and limited integration into global knowledge networks. This uneven pattern underscores how the global geography of scientific output often mirrors the broader distribution of economic competitiveness and innovation potential in the digital economy.

Figure 4: Country scientific production map



Source: Own elaboration

Overall, China and the United States stand out as the two leading countries in global research, China excels in total publications, while the United States leads in citation impact, highlighting their respective strengths in volume and influence. This dominance reflects the strategic alignment of digital security research with state-led innovation agendas, creating a self-reinforcing cycle of technological advancement and knowledge-protection capacity (Koca & Çiftçi, 2025). Such concentration has significant consequences for smaller and emerging economies. Limited access to locally generated cybersecurity knowledge and infrastructure often compels firms to rely on imported technologies and expertise, typically at higher cost and with limited adaptability (Farrand et al., 2024).

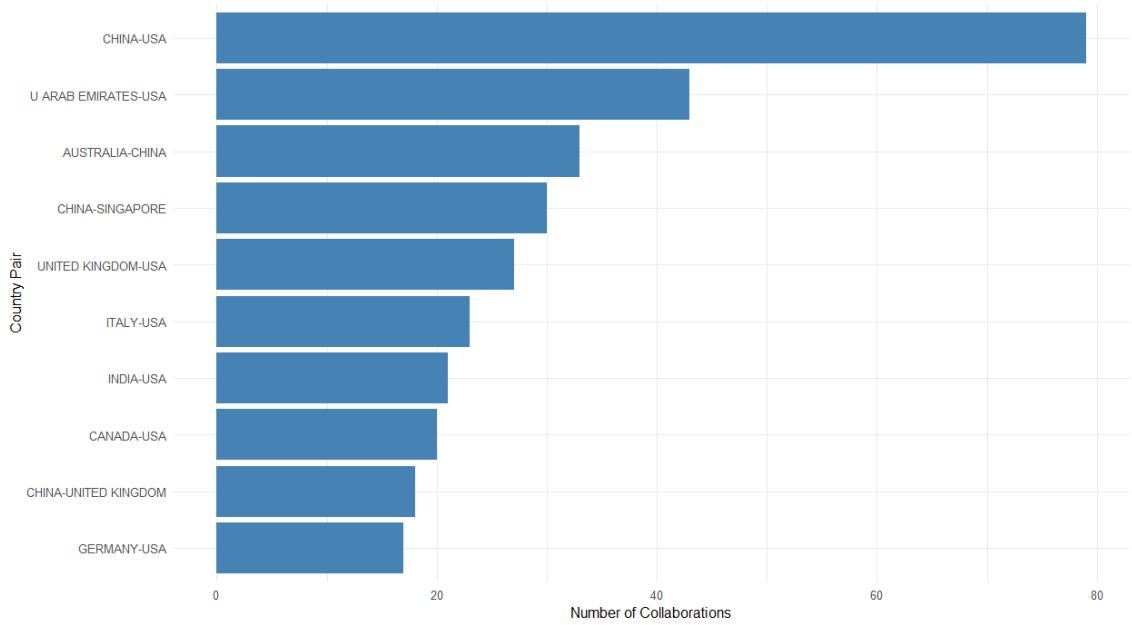
As a result, small and medium-sized enterprises (SMEs) face persistent disadvantages in protecting and leveraging their intellectual capital, constraining innovation and competitiveness. Recent evidence confirms that innovation-intensive SMEs in emerging economies continue to struggle with capability gaps due to weaker intangible-asset investment and limited participation in global R&D networks (Bilal et al., 2025). At the same time, empirical results from the European context reveal that digitalization and innovation remain strongly correlated but highly uneven across countries, wealthier regions with stronger human capital and digital capabilities achieve far greater innovation outcomes (de Rojas et al., 2024). This suggests that the structural asymmetry in knowledge-protection capacity reinforces unequal value creation and widens economic disparities between more digitally advanced and lagging economies (Gerth et al., 2025).

As part of analysing individual countries' research productivity, collaboration between country pairs was also examined based on the number of co-authored publications, as shown in the Figure 5. Author affiliations identify international collaboration: each country represented in a paper through at least one author's affiliation is included in the collaboration count, regardless of the author's position as the first or corresponding author.

The analysis of the most intense collaborations reveals that a few bilateral partnerships dominate. The most prominent is between China and the United States, with 79 joint publications, underscoring both countries' central roles in global scientific output. The United States also serves as a key partner for several other nations, including the United Arab Emirates (43 publications), the United Kingdom (27), Italy (23), India (21), Canada (20), Germany (17), and Australia (17). This trend shows that the USA acts as a global hub of scientific collaboration, connecting advanced economies with emerging research systems.

China has also established strong partnerships outside of the United States, especially with Australia (33 publications), Singapore (30), and the United Kingdom (18). These collaborations highlight the growing importance of regional and international research networks in Asia and Europe, reflecting broader globalization trends in science. Furthermore, it is important to note that international collaboration in this field remains highly concentrated among a select few key players. The dominant positions of the United States and China are further supported by their extensive collaboration networks, which significantly increase their influence within the global research landscape.

Figure 5. Top 10 bilateral partnerships by country

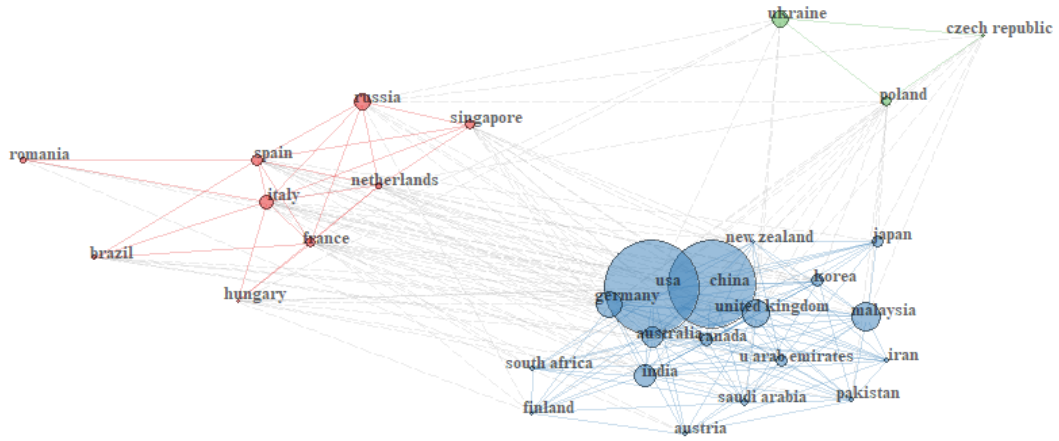


Source: Own elaboration

Building upon the analysis of the most active bilateral partnerships, the network visualization of country collaboration provides a comprehensive view of global research interconnections in the intellectual capital cybersecurity field, as shown in the Figure 6. Node size represents research output volume, while edge thickness indicates collaboration intensity. The largest nodes, representing the United States, China, Germany, and the United Kingdom, highlight these nations' pivotal roles in shaping international research activity. The cluster colours illustrate distinct groups of countries that collaborate more closely among themselves than with others.

The blue cluster around the United States and China forms the core of the global network, while the red cluster consists mainly of European countries such as Russia, Spain, Italy, France, and the Netherlands. The green cluster includes Central and Eastern European nations such as Ukraine, Poland, and the Czech Republic. The thickness of the connecting lines indicates the strength of collaboration, with the most robust links observed between the United States and China, and secondary connections between the United States and other major research economies. These patterns align with earlier findings of US - China dominance in bilateral research partnerships.

Figure 6: Country collaboration network



Source: Own elaboration

This network configuration reflects the global economic hierarchy of technological capability. Countries at the core, most notably the United States, China, and Germany, combine high research productivity with substantial R&D expenditure and intangible-asset investment, evidencing their concentration of knowledge-protection capital. In contrast, peripheral clusters in Eastern and Southern Europe display weaker interconnectivity and limited participation in global research flows, indicating constrained capacity to generate and retain cybersecurity-related intellectual capital.

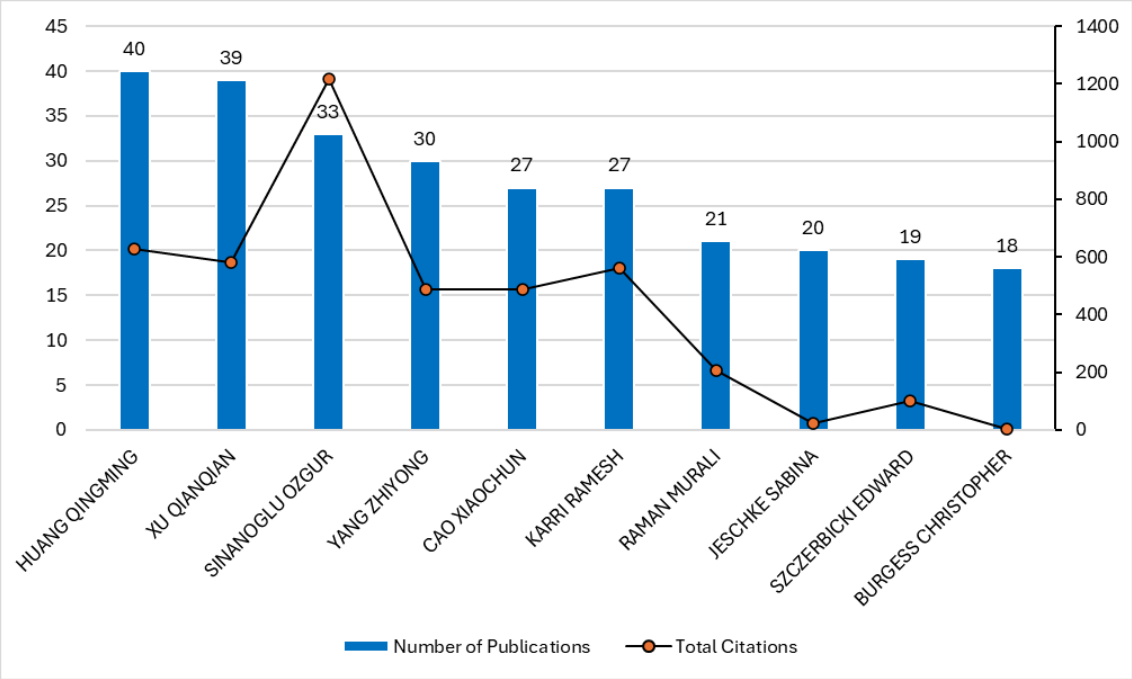
The structure of international collaboration is notably polarized, with a dense core led by the United States and China and smaller, regionally confined clusters in Europe and beyond. This polarization mirrors the uneven global distribution of knowledge-protection capital: central economies possess both the scientific influence and institutional capacity to convert cybersecurity knowledge into strategic and economic advantage. Their dominance in collaborative research reinforces leadership in digital innovation and intangible-asset development, perpetuating a self-reinforcing cycle of technological capacity and protection.

These network asymmetries have measurable economic implications. Economies occupying central positions typically exhibit higher R&D intensity, stronger innovation performance, and more mature knowledge-protection frameworks, core determinants of competitiveness in the digital economy. This finding aligns with applied economic evidence showing that cybersecurity capability and digital transformation enhance national productivity, institutional efficiency, and innovation outcomes (Gerth et al., 2025). Hence, bibliometric collaboration patterns extend beyond academic analysis, serving as empirical signals of how research concentration translates into tangible competitive advantages in knowledge-driven industries.

Author Research Productivity and Citation Impact

The ten most prolific authors in the field were analysed, as shown in Figure 7. The top contributors are Qingming, H., with 40 publications, and Qianqian, X., with 39. Ozgur, S. has produced 33 publications but has the highest citation count, highlighting his work's significant scientific impact. Further analysis shows Yang, Z. with 30 publications, along with Cao, X. and Karri, R., each with 27 publications, also making notable contributions, though with lower citation impacts. These authors mainly focus on artificial intelligence and machine learning, with some work in cybersecurity. The next group includes Raman, M. (21 publications), Jeschke, S. (20), Szczerbicki, E. (19), and Burgess C. (18). Although their publication numbers are smaller, their research is influential, especially in knowledge management.

Figure 7. The most productive authors: Publications vs. citations



Source: Own elaboration

These authors' research contributions span various areas of knowledge management, including safeguarding intellectual capital and fostering knowledge sharing within organizations. The keyword analysis further reveals the multidimensional nature of this field, emphasizing close associations with information security, cybersecurity, machine learning, blockchain, and artificial intelligence. This indicates an increasing integration of knowledge management with emerging digital technologies and security-oriented research. The findings show that having more publications does not always lead to higher citation impact, as some less prolific authors have gained notable scientific influence.

The analysis shows a clear pattern: research productivity and citation impact are not directly proportional. The most productive authors are not always the most cited, suggesting that research influence relies more on the quality, relevance, and visibility of the work than on publication quantity. As shown in Figure 8, this trend highlights a move toward interdisciplinary, high-impact research at the crossroads of knowledge management, technology, and organizational innovation. It also supports the broader conclusion from the country-level analysis, impact and productivity often do not coincide. A more petite body of influential work can achieve significant scholarly impact if it tackles critical issues effectively and resonates within the academic community.

Figure 8: Research areas derived from the Author´s keywords

Source: Own elaboration

Beyond publication counts, bibliometric indicators from the Biblioshiny package can provide a more detailed evaluation of the performance of the most prolific authors. These include metrics such as the H-index, which measures an author's scholarly influence by combining publication volume and citation impact (Hirsch, 2007). They also incorporate the G-index, which places greater weight on highly cited works and thus enables a more nuanced comparison among authors (Egghe, 2006), as well as the M-index, which normalizes citation performance by the number of years since the first publication (Hirsch, 2005). Taken together, these metrics offer a more refined means of comparing groups of authors, capturing not only productivity but also the quality, longevity, and consistency of their contributions to the field.

Table 3. Author´s impact and productivity metrics

Author	H_index	G_index	M_index	TC	TP	Publication Year Start
Ozgur S.	17	33	1,417	1216	33	2014
Qingming H.	12	24	1,5	629	40	2018
Qianqian X.	12	23	1,5	582	39	2018
Xiaochun C.	10	22	1,25	487	27	2018
Ramesh K.	10	23	0,833	560	27	2014
Satwik P.	9	14	1	214	14	2017
Yong S.	9	10	1	307	10	2017
Zhiyong Y.	9	21	1,125	486	30	2018
Mohammed A.	8	11	0,889	369	11	2017
Ji-Bo W.	8	9	0,5	223	9	2010

Note:TC – Total Citations, TP – Total Publications
Source: Own elaboration

Table 3 presents the bibliometric performance of the most prolific authors, combining their productivity and impact indicators. As shown in Table X, Ozgur S. stands out as the most influential author, with the highest H-index (17), G-index (33), and a total of 1,216 citations, even though he has fewer publications (33) than Qingming H. (40) or Qianqian X. (39). This indicates that his work has maintained a significant scholarly influence beyond just number of publications. In contrast, Qingming H. and Qianqian X. have higher publication counts but lower citation totals, likely because their contributions are more recent (from 2018 onwards) and have had less time to accumulate citations. Similarly, Yang Z. (30 publications) and Cao X. (27 publications) show strong productivity but more moderate citation impact. Overall, these findings reinforce the idea that high productivity does not necessarily mean greater scientific influence, as authors like Ozgur S., with fewer publications, can have a larger impact in the field.

As shown in Figure 9, Lotka's Law analysis (Lotka, 1926) reveals that author productivity in the IC–cybersecurity field follows an inverse-square distribution, with the majority of researchers contributing only a single publication, while a small group of prolific authors accounts for a disproportionately large share of total output.

Figure 9: Author´s productivity through Lotka´s Law

Source: Own elaboration

This creates a core–periphery structure, where a small group of highly active and influential authors drive most of the research output (Pao, 1986; Kushairi & Ahmi, 2021). Practically, it means knowledge creation is concentrated among key contributors who influence research directions, methods, and themes. At the same time, the prevalence of single-publication authors indicates the field remains open and inclusive, with new researchers entering regularly, supporting its diversity and ongoing development.

Table 4 (Annex 1) clearly shows a consistent thematic and structural pattern among the most influential global publications. The data in Table 4 reveal that the most influential global publications converge around several interrelated themes, most notably artificial intelligence (AI), Industry 4.0, and digital transformation. These studies collectively emphasize the profound impact of emerging technologies on management, production, and society, highlighting both opportunities for innovation and challenges related to privacy, cybersecurity, and intellectual property. Highly cited works in this group demonstrate how the integration of AI, the Internet of Things (IoT), and data-driven processes is reshaping industrial ecosystems, enabling real-time decision-making, and advancing sustainable and collaborative supply chain models.

The most cited publication, with 1,481 citations, is by Dwivedi et al. (2021). This study synthesizes insights from experts across the public sector, industry, and academia, outlining opportunities and challenges arising from the rapid advance of AI in all spheres of socio-economic development. The authors highlight that while AI applications hold significant transformative potential, they also carry risks of social exclusion. The trajectory of AI remains uncertain, and decisions made in the near future will profoundly affect both current and future generations.

The second most cited article, with 1,082 citations, is by Oztemel & Gursev (2020). This work provides a comprehensive definition of Industry 4.0, the earliest among the ten highly cited publications. It identifies major benefits such as enhanced innovation capacity, real-time data-driven decision-making, and more flexible and environmentally sustainable production. However, the study also emphasizes challenges related to privacy, cybersecurity, and intellectual property protection. Industry 4.0 is framed not as an endpoint, but as part of an evolving trajectory towards Industry 5.0, characterized by closer human–machine collaboration.

The third most cited contribution, Jelodar et al. (2019) with 919 citations, addresses data processing and specifically reviews applications of topic modelling (LDA) across domains such as linguistics, political science, medicine, and social networks. The review underscores both the method's versatility and its growing adoption.

Ranked fourth, with 861 citations, is Fortunato et al. (2018), which examines the paradox of modern science. Although not directly aligned with intellectual capital or cybersecurity, the article highlights systemic issues in scientific production and evaluation. Indirectly, it touches upon aspects of human capital by considering collaboration, evaluation frameworks, and the development of intellectual resources.

The fifth most cited article, Majchrzak et al. (2013) with 613 citations, investigates knowledge sharing in cyberspace. The study reveals how social media affordances reshape knowledge exchange, enabling diversity, immediacy, and collaboration, while simultaneously creating challenges such as information overload, knowledge leakage, and fragmented attention. The findings suggest that organizations and researchers must rethink traditional approaches to knowledge management and design frameworks that account for the contradictory effects of digital tools.

The sixth publication, Manavalan & Jayakrishna (2019) with 572 citations, links IoT and Industry 4.0 with sustainable supply chain practices. The authors show how IoT enhances efficiency, enables real-time stakeholder integration, and supports sustainability initiatives such as renewable resource use, closed-loop supply chains, and carbon footprint reduction. They propose a conceptual framework for assessing Industry 4.0 readiness, grounded in five perspectives: business, technology, sustainability, collaboration, and management strategy.

Seventh in the ranking is Rajapathirana & Hui (2018) with 452 citations. This study examines the impact of innovation capability on firm performance in the Sri Lankan insurance industry. The findings reveal that strengthening innovation capability enhances product, process, and marketing innovations, which in turn improve competitiveness and profitability.

The eighth most cited study, Adi et al. (2018), addresses intellectual property protection in artificial intelligence. The authors propose a watermarking scheme for deep neural networks that embeds ownership without compromising performance. This approach contributes to cybersecurity by providing practical protection against model piracy and unauthorized redistribution.

Ranked ninth, with 326 citations, is Ardito et al. (2019). This work explores the role of digital technologies—such as Industrial IoT, cloud computing, analytics, and cybersecurity, in integrating supply chain management with marketing. It emphasizes the strategic need for cyber-protected information ecosystems and highlights innovation trends through patent analysis.

Finally, the tenth-most-cited publication, with 306 citations, is Cohen (2017). In her book, Cohen examines information privacy and its legal protection in the digital age. She argues that data collection architectures reflect deliberate choices and can be redesigned to respect privacy. The study highlights the need for legal frameworks that encourage privacy-enhancing technologies and proposes mechanisms, such as time-limited consent, to safeguard personal data better.

A key pattern from the analysis is the broad scope of these influential publications. The most cited works go beyond traditional management or engineering topics, encompassing information science, law, and social studies, and highlighting the cross-sectoral nature of digital transformation. This indicates a growing academic recognition that technological progress is deeply intertwined with social, ethical, and regulatory dimensions. Practically, the findings show that research impact is increasingly associated with studies combining technological innovation with societal and governance issues. Publications addressing not only technical development but also accountability, data protection, and sustainability receive greater scholarly attention. Overall, the most influential works demonstrate a shift toward interdisciplinary, digitally focused research, positioning technology as both a catalyst for change and a framework for analysing complex organizational and societal challenges.

From a policy perspective, this interdisciplinary evolution also underscores persistent structural asymmetries in digital capacity and knowledge protection. The unequal global distribution of knowledge-protection capital mirrors wider disparities in innovation intensity and digital infrastructure investment. Economies located at the periphery of the research network continue to face challenges in developing cybersecurity capacity and retaining skilled professionals, which limits their participation in high-value digital sectors. Empirical evidence from recent *JAES* studies reinforces this pattern: Nguyen et al. (2024) show that blockchain adoption in digital commerce enhances transparency, trust, and security, offering pathways for institutional strengthening and innovation diffusion in emerging economies, while Kinda (2025) demonstrates that digital innovation promotes sustainable economic outcomes when supported by robust governance frameworks.

Conclusion

This bibliometric study provides a comprehensive view of global research on intellectual capital and cybersecurity, uncovering clear regional and structural asymmetries. Asia, led by China, dominates in research output, Europe excels in citation efficiency and collaboration quality, while North America, particularly the United States, balances scale with global influence. Smaller yet efficient systems such as the United Kingdom, Singapore, and Italy demonstrate that research excellence and international collaboration can yield impact comparable to larger economies. The analysis of the most-cited works also shows a growing integration of technology, governance, and sustainability themes, indicating that research impact increasingly depends on interdisciplinary approaches that link innovation with ethical and regulatory considerations. At the author level, the study confirms that scholarly influence stems not from publication volume alone but from high-impact, cross-disciplinary contributions connecting technology, management, and policy.

The results reveal that the global IC–cybersecurity research landscape remains highly polarized. The dominance of a few economies reflects an uneven accumulation of knowledge-protection capital, translating into measurable disparities in R&D efficiency, innovation output, and intangible-asset competitiveness. From an applied-economic perspective, this concentration warrants further investigation into whether such asymmetries generate market failures or strategic advantages for firms in technologically advanced nations.

Despite its contributions, this study is limited by its reliance on a single bibliometric source and cross-sectional design. Future research should integrate multi-database bibliometric data (e.g., Scopus, Dimensions) with economic indicators such as R&D intensity, digital innovation indices, and high-tech export performance to quantify the relationship between knowledge production and economic outcomes.

Ultimately, the findings emphasize that cybersecurity and intellectual capital are not merely research domains but strategic economic assets shaping national resilience and competitiveness in the digital economy. Building inclusive, innovation-driven ecosystems through targeted R&D incentives, SME digitalisation, and cross-border collaboration remains essential for achieving balanced and sustainable growth in global knowledge protection.

Credit Authorship Contribution Statement

This study was conducted entirely by the author, Darya Dancakova who independently designed the research framework, developed the methodology, collected and analysed the data, and performed the bibliometric analysis. The manuscript, including the literature review, interpretation of findings, and final revisions, represents the author's original work and was approved in its entirety by the author.

Acknowledgments/Funding

This study was supported by the Slovak Research and Development Agency under Contract No. VV-MVP-24-0272.

Conflict of Interest Statement

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Data Availability Statement

Bibliometric data for this research were sourced from the *Web of Science Core Collection* and are available through the database's public access portal at https://www.webofscience.com.

References

Adi, Y., Baum, C., Cisse, M., Pinkas, B., & Keshet, J. (2018). Turning your weakness into a strength: Watermarking deep neural networks by backdooring. In *27th USENIX security symposium (USENIX Security 18)* (pp. 1615-1631). https://doi.org/10.5555/3277203.3277324

Al-Alawi, A., & Alghasra, A. (2024). *A Systematic Review Investigating Cyberthreats and the Preservation of Intellectual Capital in Big Data* (p. 11). https://doi.org/10.1109/ICETSIS61505.2024.10459611

Ali, M. A., Hussin, N., Haddad, H., Al-Araj, R., & Abed, I. A. (2021). A Multidimensional View of Intellectual Capital: The Impact on Innovation Performance. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(4), 216. https://doi.org/10.3390/joitmc7040216

Ali, S. E. A., Lai, F.-W., Jan, A. A., Rahman, H. ur, Shah, S. Q. A., & Hamad, S. (2024). Does intellectual capital curb the long-term effect of information security breaches on firms' market value? *Quality & Quantity*, *58*(4), 3673–3702. https://doi.org/10.1007/s11135-023-01797-3

Ali-Hassan, H., & Ali-Hassan, H. (2009). *Social Capital Theory* (social-capital-theory) [Chapter]. https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/978-1-60566-659-4.Ch024, IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-60566-659-4.ch024

Archibugi, D., & Coco, A. (2004). A new indicator of technological capabilities for developed and developing countries (ArCo). *World Development*, *32*(4), 629-654. https://doi.org/10.1016/j.worlddev.2003.10.008

Ardito, L., Petruzzelli, A. M., Panniello, U., & Garavelli, A. C. (2018). Towards Industry 4.0: Mapping digital technologies for supply chain management-marketing integration. *Business Process Management Journal*, *25*(2), 323–346. https://doi.org/10.1108/BPMJ-04-2017-0088

Aria, M., & 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

Avery, A. (2021). After the disclosure: measuring the short-term and long-term impacts of data breach disclosures on the financial performance of organizations. *Information & Computer Security*, *29*(3), 500-525. https://doi.org/10.1108/ICS-10-2020-0161

Ayereby, M. (2018). Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems. *Walden Dissertations and Doctoral Studies*. https://scholarworks.waldenu.edu/dissertations/6163

Balozian, P., Leidner, D., & Xue, B. (2021). Toward an intellectual capital cyber security theory: Insights from Lebanon. *Journal of Intellectual Capital*, *23*(6), 1328–1347. https://doi.org/10.1108/JIC-05-2021-0123

Bana, S., Brynjolfsson, E., Jin, W., Steffen, S., & Wang, X. (2023). *Human Capital Acquisition in Response to Data Breaches* (SSRN Scholarly Paper No. 3806060). Social Science Research Network. https://doi.org/10.2139/ssrn.3806060

Bilal, M., Xicang, Z., Jiying, W., Sohu, J. M., Akhtar, S., & Hassan, M. I. U. (2025). *Digital transformation and SME innovation: A comprehensive analysis of mediating and moderating effects. Journal of the Knowledge Economy, 16*(1), 1153–1182. https://doi.org/10.1007/s13132-024-02145-y

Bongiovanni, I., Renaud, K., & Cairns, G. (2020). Securing intellectual capital: An exploratory study in Australian universities. *Journal of Intellectual Capital*, *21*(3), 481–505. https://doi.org/10.1108/JIC-08-2019-0197

Brooking, A. (1997). Intellectual Capital. International Thomson Business Press. ISBN-10: 1861520239, ISBN-13: 9781861520234

Cabrilo, S., Dahms, S., & Tsai, F.-S. (2024). Synergy between multidimensional intellectual capital and digital knowledge management: Uncovering innovation performance complexities. *Journal of Innovation & Knowledge*, *9*(4), 100568. https://doi.org/10.1016/j.jik.2024.100568

Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, *52*(5), 1373–1438. https://doi.org/10.2307/1229517

de Frutos-Belizón, J., García-Carbonell, N., Guerrero-Alba, F., & Sánchez-Gardey, G. (2024). An empirical analysis of individual and collective determinants of international research collaboration. *Scientometrics*, *129*(5), 2749-2770 https://doi.org/10.1007/s11192-024-04999-0

de Rojas, F. H., Pita, P. R., & Martínez, J. E. P. (2024). Assessing the European association between digitalization and innovation. *Telecommunications Policy*, *48*(7), 102810. https://doi.org/10.1016/j.telpol.2024.102810

Díaz-Vega, M. I., & Gutierrez-Rincon, V. (2024). The Effects of Structural, Relational and Human Capital on Entrepreneurship and Innovation in Colombian Micro and Small Software Companies. *Journal of Technology Management and Innovation*, *19*(2), 3–15. https://doi.org/10.4067/S0718-27242024000200003

Drucker, P. F. (Ed.). (1993). Other books by Peter F. Drucker. In *Post-Capitalist Society* (p. ii). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-7506-0921-0.50001-X

Dumay, J. (2016). A critical reflection on the future of intellectual capital: From reporting to disclosure. *Journal of Intellectual Capital*, *17*(1), 168–184. https://doi.org/10.1108/JIC-08-2015-0072

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., … Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Egghe, L. (2006). Theory and practise of the g-index. *Scientometrics*, *69*(1), 131–152. https://doi.org/10.1007/s11192-006-0144-7

Elsten, C., & Hill, N. (2017). *Intangible Asset Market Value Study?* (SSRN Scholarly Paper No. 3009783). Social Science Research Network. https://papers.ssrn.com/abstract=3009783

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: security, economy and sovereignty. *International Affairs*, *100*(6), 2379-2397. https://doi.org/10.1093/ia/iiae231

Fortunato, S., Bergstrom, C. T., Börner, K., Evans, J. A., Helbing, D., Milojević, S., Petersen, A. M., Radicchi, F., Sinatra, R., Uzzi, B., Vespignani, A., Waltman, L., Wang, D., & Barabási, A.-L. (2018). Science of science. *Science*, *359*(6379), eaao0185. https://doi.org/10.1126/science.aao0185

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2021). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: An intellectual capital perspective. *Journal of Intellectual Capital*, *24*(2), 465–486. https://doi.org/10.1108/JIC-06-2021-0166

Gerth, F., Tan, A. W. K., Kwa, P. T. H. & Roche, O. P. (2025). Cybersecurity Job Requirements in Asian countries: An analysis of workforce trends and future implications. *Journal of Applied Economic Sciences*, Volume XX, Summer, 2(88), 192206. https://doi.org/10.57017/jaes.v20.2(88).02

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, *21*(2), 203–213. https://doi.org/10.1108/JIC-05-2019-0112

Hirsch, J. E. (2005). An index to quantify an individual's scientific research output. *Proceedings of the National Academy of Sciences of the United States of America*, *102*(46), 16569–16572. https://doi.org/10.1073/pnas.0507655102

Hirsch, J. E. (2007). Does the h index have predictive power? *Proceedings of the National Academy of Sciences*, *104*(49), 19193-19198. https://doi.org/10.1073/pnas.070796210

Hong, Y., Chen, T., & Zhang, Y. (2025). Individual intellectual capital, creative process engagement and information security policy compliance. *Journal of Intellectual Capital*, 1–24. https://doi.org/10.1108/JIC-04-2025-0141

Jelodar, H., Wang, Y., Yuan, C., Feng, X., Jiang, X., Li, Y., & Zhao, L. (2019). Latent Dirichlet allocation (LDA) and topic modelling: Models, applications, a survey. *Multimedia Tools and Applications*, *78*(11), 15169–15211. https://doi.org/10.1007/s11042-018-6894-4

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3), 119. https://doi.org/10.1007/s10207-025-01032-0

Kianto, A., & Cabrilo, S. (2023). Futurizing the Intellectual Capital Theory. *European Conference on Knowledge Management*, *24*(1), 178–183. https://doi.org/10.34190/eckm.24.1.1758

Kinda, A. (2025). Effects of digital innovations on sustainable development in West African Economic and Monetary Union (WAEMU). *Journal of Applied Economic Sciences,* Volume XX, Summer, 2(88), 220 – 231. https://doi.org/10.57017/jaes.v20.2(88).04

Koca, M., & Çiftçi, S. (2025). A comprehensive bibliometric analysis of Big Data and Cyber Security: intellectual structure, trends, and global collaborations, *Knowledge and Information Systems*, 1-26. https://doi.org/10.1007/s10115-025-02531-1

Kushairi, N., & Ahmi, A. (2021). Flipped classroom in the second decade of the Millenia: A Bibliometrics analysis with Lotka's law. *Education and Information Technologies*, *26*(4), 4401–4431. https://doi.org/10.1007/s10639-021-10457-8

La Torre, M., Dumay, J., & Rea, M. A. (2018). Breaching intellectual capital: Critical reflections on Big Data security. *Meditari Accountancy Research*, *26*(3), 463–482. https://doi.org/10.1108/MEDAR-06-2017-0154

Landini, F., Arrighetti, A., & Lasagni, A. (2020). Economic crisis and firm exit: do intangibles matter? *Industry and Innovation*, *27*(5), 445-479. https://doi.org/10.1080/13662716.2018.1544065

Lotka, A. J. (1926). The frequency distribution of scientific productivity. *Journal of the Washington Academy of Sciences*, *16*(12), 317–323. https://www.jstor.org/stable/24529203

Madhani, P. M. (2012). Intangible Assets: Value Drivers for Competitive Advantage. In G. N. Gregoriou & N. Finch (Eds), *Best Practices in Management Accounting* (pp. 146–165). Palgrave Macmillan UK. https://doi.org/10.1057/9780230361553_10

Madsen, D. Ø. (2019). The emergence and rise of Industry 4.0 viewed through the lens of management fashion theory. *Administrative Sciences*, *9*(3), 71. https://doi.org/10.3390/admsci9030071

Majchrzak, A., Faraj, S., Kane, G. C., & Azad, B. (2013). The Contradictory Influence of Social Media Affordances on Online Communal Knowledge Sharing. *Journal of Computer-Mediated Communication*, *19*(1), 38–55. https://doi.org/10.1111/jcc4.12030

Manavalan, E., & Jayakrishna, K. (2019). A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. *Computers & Industrial Engineering*, *127*, 925–953. https://doi.org/10.1016/j.cie.2018.11.030

Mavani, C., Mistry, H., Patel, R., & Goswami, A. (2024). The Role of Cybersecurity in Protecting Intellectual Property. *International Journal on Recent and Innovation Trends in Computing and Communication*, *12*, 529–538. https://ijritcc.org/index.php/ijritcc/article/view/10935

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine*, *6*(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Nguyen Thi Phuong, G., Thai Dong, T., Nguyen Binh Phuong, D., Le Huu, H., & Chau Huyen, T. (2024). Assess the impact of blockchain application in electronic commerce on customer's shopping experience. *Journal of Applied Economic Sciences,* Volume XIX, Fall, 3(85), 305 – 316. https://doi.org/10.57017/jaes.v19.3(85).06

Nonala, I., & Kenney, M. (1991). Towards a new theory of innovation management: A case study comparing Canon, Inc. and Apple Computer, Inc. *Journal of Engineering and Technology Management*, *8*(1), 67–83. https://doi.org/10.1016/0923-4748(91)90005-C

Ode, E., Awolowo, I. F., Nana, R., & Olawoyin, F. S. (2025). Social Capital and Artificial Intelligence Readiness: The Mediating Role of Cyber Resilience and Value Construction of SMEs in Resource-Constrained Environments. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-025-10608-z

Oztemel, E., & Gursev, S. (2020). Literature review of Industry 4.0 and related technologies. *Journal of Intelligent Manufacturing*, *31*(1), 127–182. https://doi.org/10.1007/s10845-018-1433-8

Pao, M. L. (1986). An empirical examination of Lotka's Law. *Journal of the American Society for Information Science*, 37(1), 26–33. https://doi.org/10.1002/asi.4630370105

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ (Clinical Research Ed.)*, *372*, n71. https://doi.org/10.1136/bmj.n71

Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons*, *64*(6), 763–774. https://doi.org/10.1016/j.bushor.2021.07.012

Rajapathirana, R. P. J., & Hui, Y. (2018). Relationship between innovation capability, innovation type, and firm performance. *Journal of Innovation & Knowledge*, *3*(1), 44–55. https://doi.org/10.1016/j.jik.2017.06.002

Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security? *Journal of Intellectual Capital*, *20*(5), 621-641. https://doi.org/10.1108/JIC-04-2019-0079

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8. https://doi.org/10.15394/jdfsl.2017.1476

Snyder, H., & Crescenzi, A. (2013). Intellectual capital and economic espionage: New crimes and new protections. In *Transnational Financial Crime*. Routledge. https://doi.org/10.4324/9781315084572-24

Thum-Thysen, A., Voigt, P., Maier, C., Bilbao-Osorio, B., & Ognyanova, D. (2017). Unlocking investment in intangible assets in Europe. *Quarterly Report on the Euro Area (QREA)*, *16*(1), 23–35. https://economy-finance.ec.europa.eu/document/download/b7d987bc-2ea1-48ab-ad11-320f7493a359_en?filename=dp047_en.pdf

Toffler, A. (1990). Powershift: Knowledge. Wealth and Violence at the Edge of the 21st Century. ISBN: 0-553-05776-62-253-06261-8

Tosun, O. K. (2019). *Cyber Attacks and Stock Market Activity* (SSRN Scholarly Paper No. 3190454). Social Science Research Network. https://doi.org/10.2139/ssrn.3190454

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Yilmaz, A. A., & Tuzlukaya, S. E. (2023). The relation between intellectual capital and digital transformation: A bibliometric analysis. *International Journal of Innovation Science*, *16*(2), 244–264. https://doi.org/10.1108/IJIS-08-2022-0145

Youndt, M. A., Subramaniam, M., & Snell, S. A. (2004). Intellectual capital profiles: An examination of investments and returns. *Journal of Management Studies*, *41*(2), 335-361. https://doi.org/10.1111/j.1467-6486.2004.00435.x

ANNEX 1

Table 4: The top 10 globally cited publications

Rank	Authors	Title	Source	Journal H index (Q) as of SJR 2024	DOI	TC	TC per year	Topics
1	Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... & Williams, M. D. (2021)	Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy	International Journal of Information Management	196 (Q1)	10.1016/j.ijinfomgt.2019.08.002	1481	296,20	Artificial Intelligence (AI) and its implications for society and management
2	Oztemel, E., & Gursev, S. (2020)	Literature review of Industry 4.0 and related technologies	Journal of Intelligent Manufacturing	113 (Q1)	10.1007/s10845-018-1433-8	1082	180,33	Industry 4.0, IoT, and the digital transformation of production and supply chains
3	Jelodar, H., Wang, Y., Yuan, C., Feng, X., Jiang, X., Li, Y., & Zhao, L. (2019).	Latent Dirichlet allocation (LDA) and topic modelling: models, applications, a survey	Multimedia Tools and Applications	116 (Q1)	10.1007/s11042-018-6894-4	919	131,29	Artificial Intelligence (AI) and its implications for society and management
4	Fortunato, S., Bergstrom, C. T., Börner, K., Evans, J. A., Helbing, D., Milojević, S., ... & Barabási, A. L. (2018).	Science of science	Science	1382(Q1)	10.1126/science.aao0185	861	107,63	Artificial Intelligence (AI) and its implications for society and management
5	Majchrzak, A., Faraj, S., Kane, G. C., & Azad, B. (2013).	The Contradictory Influence of Social Media Affordances on Online Communal Knowledge Sharing	Journal of Computer-Mediated Communication	144 (Q1)	10.1111/jcc4.12030	613	47,15	Digital security, cyber space and security, legal issues
6	Manavalan, E., & Jayakrishna, K. (2019).	A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements	Computers & industrial engineering	176 (Q1)	10.1016/j.cie.2018.11.030	572	81,71	Industry 4.0, IoT, and the digital transformation of production and supply chains
7	Rajapathirana, R. J., & Hui, Y. (2018).	Relationship between innovation capability, innovation type, and firm performance	Journal of Innovation & Knowledge	70 (Q1)	10.1016/j.jik.2017.06.002	452	56,50	Industry 4.0, IoT, and the digital transformation of production and supply chains
8	Adi, Y., Baum, C., Cisse, M., Pinkas, B., & Keshet, J. (2018).	Turning your weakness into a strength: watermarking deep neural networks by backdooring	Proceedings of the 27th USENIX Security Symposium	43 (-)	10.5555/3277203.3277324	386	48,25	Digital security, cyber space and security, legal issues
9	Ardito, L., Petruzzelli, A. M., Panniello, U., & Garavelli, A. C. (2019).	Mapping digital technologies for supply chain management-marketing integration	Business Process Management Journal	102 (Q1)	10.1108/BPMJ-04-2017-0088	326	46,57	Industry 4.0, IoT, and the digital transformation of production and supply chains
10	Cohen, J. E. (2017).	Examined lives: Informational privacy and the subject as object.	Law and Society Approaches to Cyberspace	Book	10.2307/1229517	306	11,77	Digital security, cyber space and security, legal issues

Note: TC – Total Citations, TC per Year – Total Citations per Year Source: Own elaboration