INTERNATIONAL JOURNAL OF CYBER THREAT INTELLIGENCE AND SECURE NETWORKING (IJCTISN)

eISSN: 3087-4297

Volume. 03, Issue. 05, pp. 08-17, May 2026

A Longitudinal Analysis of Cybersecurity Technology and Innovation: A Technology Mining Approach Using Bibliometric and Patent Analysis

Dr. Marcus A. Rodriguez
Department of Information Systems, Global School of Business and Technology, Madrid, Spain

Article received: 15/03/2026, Article Accepted: 16/04/2026, Article Published: 02/05/2026

ABSTRACT

Background: The field of cybersecurity R&D has experienced exponential growth, driven by the escalating complexity and frequency of cyber threats. Understanding the evolving landscape of this domain is critical for strategic planning, resource allocation, and maintaining national security. This study addresses a significant gap in the literature by providing a comprehensive, longitudinal analysis that integrates both academic research and technological innovation.

Methods: This research employs a technology mining approach combining bibliometric and patent analyses with social network mapping. Data was systematically collected from major academic and patent databases from 1999 to the present. We used co-citation analysis to map the intellectual structure of the field, and patent citation analysis and h-index to identify influential corporate innovators. Social network analysis was applied to visualize collaboration patterns and pinpoint key actors.

Results: Our findings confirm an exponential annual growth rate of 19.7% in cybersecurity R&D. The U.S. leads in both academic output and patent filings, with notable contributions from Europe and Asia in specific areas like smart grids and cyber-physical security. The analysis identified deep learning, blockchain deterrence, human cybersecurity behavior, and supply chain security as dominant emerging research clusters. IBM stands out as the most influential corporate player, holding 11,652 patent citations and an h-index of 78, followed by Microsoft and Cisco.

Discussion: The study reveals a strong and dynamic interplay between academic and industrial innovation. The identified emerging themes represent critical future priorities for investment and R&D. The combined methodology offers a valuable foresight tool for policymakers, R&D managers, and investors. The results provide actionable insights for steering future research and development efforts to combat next-generation cyber threats.

Keywords: Cybersecurity, Technology Mining, Bibliometrics, Patent Analysis, Social Network Analysis, Innovation, Technology Foresight.

INTRODUCTION

Background and Motivation

The digital landscape has fundamentally reshaped every aspect of modern life, from global commerce to interpersonal communication. However, this transformation has been accompanied by a relentless and escalating wave of cyber threats. From sophisticated phishing campaigns and ransomware attacks to large-scale data breaches and state-sponsored espionage, the challenges facing individuals, organizations, and governments are more complex than ever before [65, 95]. The constant evolution of these threats necessitates a corresponding evolution in our defenses. Consequently, investment in cybersecurity research and development (R&D) has become a global imperative, recognized not just as a business necessity, but as a critical component of national security and economic stability [39].

The motivation for this study stems from the need to comprehensively understand this rapidly evolving domain. While we know that cyber threats are increasing, we lack a clear, long-term, and integrated view of the R&D landscape that is shaping our response. Tracking

the development of cybersecurity technologies is often done in a reactive manner, focusing on the latest breach or a newly discovered vulnerability. This study, however, takes a proactive and strategic approach, viewing the entire R&D ecosystem through the lens of technology mining. This methodology allows us to not only look at where we are now, but also to anticipate future trends and identify key areas for investment and collaboration [26, 52]. The sheer scale and speed of change in this field make a holistic analysis essential for effective policymaking and strategic decision-making [27, 34].

The Evolving Cybersecurity Landscape

The history of cybersecurity is a story of continuous adaptation and escalation. In the early days, threats were relatively simple, often focused on individual computers or local networks. Antivirus software and firewalls were the primary tools of defense. Over time, as networks became more interconnected and data became more centralized, threats became more sophisticated and targeted. The rise of the internet ushered in an era of distributed denial-of-service (DDoS) attacks, worms, and Trojans [40]. More recently, the proliferation of the Internet of Things (IoT), cloud computing, and advanced artificial intelligence (AI) has introduced new attack vectors and vulnerabilities, creating a vast and complex cyber-physical system [42].

This dynamic environment has fueled a corresponding surge in R&D. Our analysis confirms that cybersecurity R&D has grown at an exponential pace, with a remarkable 19.7% annual growth rate since 1999. This growth is a direct reflection of the rising stakes and the urgent need for innovative solutions. Technologies that were once theoretical, like blockchain for securing data or machine learning for threat detection, are now at the forefront of both academic research and commercial application [2, 37]. This study aims to pinpoint the key drivers of this growth and identify the intellectual and innovative hubs where this progress is taking place. We will also examine the roles of major players, from influential academic institutions to dominant corporate entities, and highlight the emerging technologies that are poised to shape the next decade of cybersecurity [1, 2, 4, 38].

Literature Review and Research Gaps

A substantial body of literature exists on technology forecasting, bibliometrics, and patent analysis. Researchers have successfully used these methods to map the intellectual structure and innovation patterns in various fields, including servitization [5, 6], innovation management [9], technology capability [10], and even specific technologies like blockchain [47] and autonomous vehicles [25]. Bibliometric analysis, in particular, has proven effective in identifying research fronts, key authors, and influential institutions by examining citation networks and co-authorship patterns [3, 54, 55]. Similarly, patent analysis provides a window into corporate R&D strategies, revealing the direction and intensity of technological innovation through patent filings and citations [17, 18, 19, 21].

However, a significant research gap remains in the cybersecurity domain. While some studies have explored specific aspects, such as the intellectual basis of blockchain patents [89], the general research productivity in cybersecurity [74], or the analysis of a specific technology standard [16], a comprehensive and integrated analysis of the entire cybersecurity R&D ecosystem is notably absent. Existing work often focuses on either academic research (bibliometrics) or industrial innovation (patents), rarely combining both to provide a holistic view [24]. This creates a fragmented understanding of how research and development co-evolve, and which academic theories are being translated into commercial technologies. Furthermore, few studies have applied a longitudinal approach to capture the full scope of the exponential growth in the field.

This study directly addresses this gap by synthesizing bibliometric and patent data to create a detailed map of the cybersecurity R&D landscape. By using a combined technology mining approach, we can track the flow of knowledge from fundamental research to applied innovation, identifying not only who is leading the way, but also what technologies are gaining traction and where future opportunities lie. This integrated approach offers a more robust and complete picture of the field's trajectory than any single method could achieve.

Research Questions and Objectives

Based on the identified gaps, this research is guided by the following primary questions:

- RQ1: What are the major intellectual and research clusters in the field of cybersecurity technology, and how have they evolved over time?
- RQ2: How have corporate innovation and patenting activities evolved in cybersecurity, and who are the most influential players in this domain?
- RQ3: What is the relationship between academic research and technological innovation in cybersecurity, and what are the key emerging research frontiers that warrant future attention and investment?

To answer these questions, the study sets forth the following objectives:

1. To map the intellectual structure of cybersecurity research using co-citation and keyword analysis.
2. To identify the key innovators and assess their

influence through a comprehensive patent analysis.

3. To analyze the co-evolution of academic research and corporate patenting to understand the dynamics of knowledge transfer.

4. To provide strategic foresight for policymakers and R&D managers by identifying future priorities and investment opportunities.

Methods

Data Collection and Scoping

The foundation of this study is a robust and comprehensive dataset encompassing both academic and patent information. The data collection process was designed to capture a broad yet relevant scope of the cybersecurity R&D landscape. For the academic literature, we utilized major databases such as Scopus and Web of Science, which are widely recognized for their extensive coverage of scientific publications [57]. We employed a structured search query that included a combination of keywords related to cybersecurity, such as “cyber security,” “information security,” “network security,” “data protection,” and “cyber defense.” To ensure a thorough search, we also included related technical terms like “intrusion detection,” “malware analysis,” and “vulnerability assessment.” The time frame for the search was set from 1999 to the present to capture the exponential growth trend in the field. This initial search yielded a large number of publications, which were then filtered to remove irrelevant articles and ensure that only peer-reviewed journal articles, conference papers, and book chapters were included.

For the patent data, we accessed databases such as the United States Patent and Trademark Office (USPTO) and the European Patent Office (EPO). The patent search queries were developed in parallel with the academic searches, using relevant International Patent Classification (IPC) and Cooperative Patent Classification (CPC) codes related to cryptography, network security, and data privacy [91, 92]. Keywords such as “cyber security,” “cyber defense,” “blockchain,” “AI security,” and “quantum computing” were also used to identify relevant patent families and applications [27, 89]. All collected data was then compiled into a single, standardized format for subsequent analysis.

Bibliometric Analysis

Our bibliometric analysis was conducted using a range of quantitative methods to uncover the underlying structure and dynamics of the cybersecurity research community. We first performed a descriptive analysis of publication trends, including the number of publications and citations over time, to confirm the exponential growth we observed [71]. This provided a foundational understanding of the field's maturity and activity.

To map the intellectual structure of the field, we employed co-citation analysis, a powerful technique that identifies relationships between research papers that are frequently cited together [54]. The logic is that if two papers are co-cited by a third paper, they are likely related in a meaningful way, often sharing a common topic, method, or intellectual foundation. We used software tools like VOSviewer and CiteSpace for this analysis [56, 57]. The resulting co-citation network was then clustered based on the strength of the citation links, revealing distinct research groups or "clusters" that represent the core themes of the field [55, 60, 61]. We examined the titles and keywords of the papers within each cluster to name and interpret the underlying research fronts, such as "Deep Learning for Cybersecurity" or "Human Factors and Behavior."

In addition to co-citation, we analyzed author and institutional productivity. We used Lotka's Law to examine author productivity patterns and identified the most prolific authors and institutions in the field [71]. We also assessed the citation impact of publications to identify the most influential papers and researchers, which often serve as foundational work for subsequent studies [69].

Patent Analysis

The patent analysis provided a critical look into the industrial side of the cybersecurity R&D ecosystem. We began by cleaning and organizing the collected patent data, which included information on the filing company, grant date, and patent citations [93]. The primary metric we used was patent citation analysis, which is a widely accepted proxy for measuring technological influence and importance [18, 27]. A patent that is frequently cited by subsequent patents is considered to be a foundational or "key" technology [21, 22]. By ranking companies based on their total number of patent citations, we were able to identify the most influential corporate players in the field.

We also calculated the h-index for each corporate player based on their patent portfolios [19, 32]. The h-index, which is commonly used to measure the productivity and impact of a researcher, was adapted to assess the strength of a company's patent portfolio. A high h-index indicates that a company has both a large number of patents and that those patents are highly cited, signifying a strong and influential innovation base [32]. This allowed for a more nuanced comparison of corporate players beyond simple patent counts. By analyzing the content of the patents, we were able to identify the specific technologies that these companies were focusing on, providing a clear view of their strategic R&D priorities [29, 30].

Social Network Analysis (SNA)

To visualize and analyze the collaborative structure of the field, we applied Social Network Analysis (SNA) to both the bibliometric and patent datasets. SNA treats authors, institutions, and countries as "nodes" and their collaborative relationships (e.g., co-authorship) as "edges" [41, 49]. This allowed us to map the patterns of collaboration and identify key actors in the network [58, 59].

We used several SNA metrics to deepen our understanding. Centrality measures, such as betweenness centrality, helped us identify key "gatekeepers" or "brokers" who connect different parts of the network, playing a crucial role in the dissemination of information and knowledge [44, 45, 68]. By analyzing the network's modularity, we could identify clusters of collaboration, which often represent different sub-fields or communities of practice [62]. For the patent data, SNA was used to visualize the co-patenting and co-assignee networks, revealing strategic alliances and collaborations between corporations and research institutions. The integration of SNA with our bibliometric and patent analyses allowed us to move beyond simple counts and understand the dynamic and collaborative nature of the cybersecurity R&D ecosystem [64].

Combined Technology Mining Approach

The true strength of this study lies in its use of a combined technology mining approach. While bibliometrics provides insight into the intellectual and academic underpinnings of the field, and patent analysis reveals the commercial and industrial innovation landscape, neither method alone can provide a complete picture [24, 26]. By integrating both, we can trace the flow of knowledge from the lab to the market. For instance, we can identify a nascent research cluster in academic publications and then cross-reference it with recent patent filings to see if corporations are investing in that same area. This synthesis allows us to not only identify what is being researched but also what is being commercialized, offering a more powerful and accurate form of technology foresight [24, 31]. The following sections will present the results of this integrated analysis.

Results

General Trends in Cybersecurity R&D

Our analysis of the collected data confirms the rapid acceleration of activity in the cybersecurity R&D domain. The number of academic publications and patent filings has shown a clear and exponential growth trend since 1999, averaging a remarkable 19.7% annual growth rate. This is consistent with the increasing global reliance on digital infrastructure and the corresponding rise in cyber threats. The growth is not just in volume but also in diversity, with new journals and research areas emerging to address specific challenges.

Geographically, the data reveals that the United States is the undisputed leader in both academic publications and patent filings. U.S. institutions and companies consistently produce the highest volume of high-impact research and hold the largest and most influential patent portfolios [74]. However, the landscape is not solely dominated by the U.S. We observed strong and growing contributions from other regions, particularly Europe and Asia. Germany, the United Kingdom, and China, in particular, have shown significant increases in both publications and patents, especially in specialized areas like smart grid security and cyber-physical systems. This suggests a global effort to address the multifaceted challenges of cybersecurity, with different regions focusing on their own unique technological strengths [16, 20].

Intellectual Structure and Research Fronts

The co-citation and keyword analysis of the academic literature revealed a highly structured intellectual landscape with several distinct and evolving research clusters. These clusters represent the core themes that have shaped the field over the past two decades.

One of the most prominent and rapidly growing clusters is centered around deep learning and artificial intelligence (AI) for cybersecurity. This cluster includes research on using machine learning for intrusion detection, malware analysis, and automated threat response [4]. Researchers in this area are exploring how AI can be used to predict and neutralize threats more effectively than traditional signature-based methods. Key papers in this cluster are foundational works on neural networks, anomaly detection, and advanced statistical modeling.

Another significant cluster is blockchain deterrence and decentralized security. This area focuses on using the principles of distributed ledger technology to enhance data integrity, identity management, and secure communication [37]. Research in this cluster examines how blockchain can create immutable audit trails, secure transactions, and protect against data tampering. The intellectual basis for this cluster draws from foundational papers on cryptography and distributed systems.

A more recent but highly active cluster is dedicated to human cybersecurity behavior and awareness. This research goes beyond technical solutions to examine the "human element" in cybersecurity. It investigates factors such as phishing susceptibility, social engineering, and the effectiveness of cybersecurity training [87, 88]. This cluster highlights the recognition that technology alone cannot solve the problem; human awareness and behavior are equally critical components of a robust defense.

Finally, we identified a cluster focused on supply chain security and critical infrastructure protection. This cluster is driven by the increasing interconnectedness of global supply chains and the growing threat to critical infrastructure, such as power grids and transportation systems [42]. Research in this area addresses vulnerabilities in interconnected systems and proposes methods for ensuring the security and resilience of these vital networks [97]. This cluster also includes work on standards and policy, showing the multidisciplinary nature of this research front [1, 84].

Overall, the intellectual structure shows a clear shift from focusing on technical, low-level vulnerabilities to a more holistic, system-level approach that includes social, organizational, and behavioral factors.

Innovation Landscape: Key Players and Patenting Activity

The patent analysis provided a clear picture of the industrial side of cybersecurity innovation, revealing who is leading the technological charge. The results of our analysis confirm that IBM is the most influential corporate player in the cybersecurity domain. Our data shows that IBM holds an impressive 11,652 patent citations and a strong h-index of 78. This high number of citations indicates that IBM's patents are not just numerous, but they are also foundational and highly influential, serving as the basis for subsequent innovations by other companies.

Following IBM, Microsoft and Cisco emerged as the next most influential players. Microsoft's strong presence is not surprising given its dominance in operating systems and enterprise software, where security is a paramount concern. Cisco, as a leader in networking hardware and software, holds a large portfolio of patents related to network security and infrastructure. Other significant players include major technology firms and defense contractors, reflecting the dual-use nature of many cybersecurity technologies.

The patenting activity of these leading companies aligns closely with the academic research clusters we identified. For example, a significant portion of the patents filed by these companies relates to deep learning for threat detection and the use of blockchain for securing data and identities. This strong correlation suggests a rapid transfer of knowledge from academic research to commercial application, a key indicator of a healthy and dynamic innovation ecosystem. We also found a large number of patents related to cyber-physical systems, smart grid security, and cloud security, indicating that these are key areas of strategic investment for leading firms [16, 19, 20].

Bridging Academia and Industry

Our combined analysis offers compelling evidence of the symbiotic relationship between academic research and industrial innovation in cybersecurity. The intellectual clusters identified in our bibliometric analysis are mirrored by the patenting activity of the most influential corporations. For instance, the academic research front on blockchain deterrence has a direct parallel in the high volume of blockchain-related patents filed by companies like IBM. Similarly, the growing academic interest in deep learning for threat detection is reflected in the patent portfolios of Microsoft and Cisco.

This close alignment is a testament to the efficient transfer of knowledge in this field. It shows that companies are not just waiting for academic breakthroughs; they are actively monitoring research trends and translating them into tangible, patented technologies. This dynamic is crucial for a field like cybersecurity, where the speed of innovation is a key determinant of success [27, 30]. The social network analysis further supports this, showing strong collaboration patterns between academic institutions and corporate R&D divisions, particularly in regions like the U.S. and Europe. These collaborative networks act as bridges, facilitating the flow of information and expertise between the two domains [78, 80].

Comparative Analysis: Bridging the Academic-Industrial Divide

The separate analyses of the academic and patent landscapes, while informative on their own, gain a new level of significance when they are directly compared. This comparative analysis reveals a clear and compelling narrative: a highly efficient, symbiotic relationship exists between academic research and corporate innovation in the cybersecurity domain. The intellectual shifts we observed in the bibliometric data are not abstract academic pursuits; they are the direct precursors to the commercial technologies being developed and patented by the most influential companies in the field.

To illustrate this, we conducted a deeper, qualitative-quantitative comparison by mapping the key topics and intellectual foundations of the top research clusters (identified in Section 3.2) to the technological classes and claims of the most cited patents (identified in Section 3.3). This analysis provides concrete evidence of how knowledge flows from the university lab to the corporate R&D pipeline.

Deep Learning for Cybersecurity: From Algorithm to Application

Our bibliometric analysis showed a major, recent surge in academic interest in deep learning for cybersecurity. The intellectual foundation of this cluster is built upon foundational works in neural networks, such as those by Hinton, LeCun, and Bengio, as well as classic machine

learning papers on support vector machines and clustering [94]. We identified a series of highly-cited academic papers that propose novel algorithms for a variety of security applications:

- Intrusion Detection: Academic research has explored the use of recurrent neural networks (RNNs) and convolutional neural networks (CNNs) to analyze network traffic patterns and identify anomalies that signal an intrusion [65]. These papers lay out the theoretical models and test them on open-source datasets.

- Malware Classification: Research has focused on training deep neural networks to automatically classify malware variants from raw code, bypassing the need for manual feature engineering [33].

- Spam and Phishing Detection: Academic work has proposed and validated models that use natural language processing (NLP) and deep learning to detect the subtle linguistic cues of phishing emails with high accuracy.

When we cross-referenced these academic developments with our patent data, we found a direct and powerful correlation. Major companies, particularly IBM and Microsoft, have filed a significant number of patents that are direct applications of these academic principles. For example, patents filed by these companies describe systems for “automated threat detection using machine learning models” and “behavioral analysis for anomaly detection.” These patents often cite the very academic papers that introduced the underlying algorithms. This shows that the corporate strategy is not to reinvent the wheel, but to take cutting-edge academic theory and translate it into proprietary, commercial systems. This is a core reason for the high citation count and h-index we observed for IBM [27, 28].

Blockchain and Decentralized Security: The Evolution of Trust

The academic cluster focused on blockchain deterrence and decentralized security is a perfect example of a theoretical concept gaining rapid commercial traction. The intellectual basis of this cluster is rooted in cryptography and distributed systems, with foundational work on secure ledgers, hash functions, and consensus mechanisms [37, 89]. Academic researchers have been exploring a wide range of applications:

- Immutable Data Logging: Research has proposed using blockchain to create tamper-proof logs for digital evidence and supply chain data, ensuring the integrity of critical information [81].

- Decentralized Identity Management: Academic papers have investigated how blockchain can be used to create self-sovereign identities, giving users full control over their personal data without relying on a centralized authority.

- IoT Security: Researchers have proposed using blockchain to secure communication between a vast number of IoT devices, creating a distributed network that is resistant to single points of failure.

This academic push has a direct parallel in the patenting activity of our key players. IBM, in particular, has a large and influential portfolio of patents related to blockchain. Their patents do not simply replicate academic research; they focus on the practical implementation and application of these ideas. We found patents on "systems and methods for securing a supply chain using a distributed ledger," "blockchain-based access control for IoT devices," and "privacy-preserving data sharing using smart contracts." These patents often build directly on the theoretical principles validated in academic research [47, 89]. The strong alignment between the academic and corporate landscapes in this area highlights the rapid shift toward decentralized security models and the commercial recognition of blockchain’s potential as a foundational security primitive.

The Human Element: From Social Science Theory to Corporate Training

The emergence of human cybersecurity behavior as a key research cluster is particularly telling. This is a departure from the purely technical focus of the past and signifies a maturation of the field. The academic literature in this area draws heavily from social science theories, including social network theory, organizational behavior, and psychology [45, 87]. Research in this cluster investigates how social engineering attacks work, what factors influence a user's compliance with security protocols, and how to design more effective cybersecurity awareness training programs [88].

While this area might seem less "technical" and therefore less ripe for patenting, our analysis shows a different story. Companies are not patenting the social theories themselves, but the systems and methods that apply these theories to real-world problems. We found an increasing number of patents for “adaptive cybersecurity training systems” that use machine learning to tailor content to an individual’s observed behavioral patterns. We also identified patents for “social network risk assessment platforms” that analyze an organization's internal communication to identify potential vulnerabilities based on employee interactions and information flows [86]. This demonstrates that corporations are not just interested in the technical solutions; they are actively seeking to create intellectual property around the entire security ecosystem, including the human and organizational components.

Supply Chain and Critical Infrastructure Security: A

Systems-Level Approach

Finally, the academic cluster on supply chain and critical infrastructure security directly mirrors a major area of corporate investment. Academic research in this area uses systems-level thinking to model complex networks, identify vulnerabilities, and propose resilience-building strategies [42, 63]. Papers in this cluster often involve multi-disciplinary teams and utilize methodologies like social network analysis and risk assessment to understand the interconnectedness of modern supply chains and infrastructure.

The patenting activity in this area is heavily dominated by large, B2B-focused companies like Cisco and IBM. Their patents focus on securing the physical and digital components of these complex systems. We found patents for "methods for securing industrial control systems," "IoT device authentication within a large network," and "supply chain monitoring and anomaly detection." This close alignment shows that both academia and industry are moving beyond simple endpoint security to address the far more complex challenges of securing entire interconnected systems, from the factory floor to the cloud.

The overall comparative analysis demonstrates that the relationship between academic research and corporate innovation in cybersecurity is both direct and dynamic. Academic work often serves as a "signal" for where the next wave of commercial innovation will occur. Companies that successfully monitor and engage with this academic landscape are the ones that are building the most influential and valuable patent portfolios. This process is a key driver of the exponential growth we observed and provides a robust framework for technology foresight.

Discussion

The Interplay of Research and Innovation

The results of this study paint a clear picture of a highly dynamic and interconnected cybersecurity R&D ecosystem. The exponential growth in both academic publications and patents confirms that the field is maturing at an unprecedented rate, driven by a cycle of increasing threats and technological responses. The most significant finding is the strong and tangible interplay between academic research and industrial innovation. Academic research provides the intellectual foundation and theoretical breakthroughs, which are then rapidly translated into practical, patented technologies by corporate leaders.

This rapid transfer of knowledge is essential for a field where the speed of development is a critical factor in staying ahead of adversaries. The identified research clusters—deep learning, blockchain, human behavior, and supply chain security—are not isolated academic curiosities; they are the direct forerunners of the next generation of cybersecurity products and services. The fact that the patenting activity of dominant players like IBM, Microsoft, and Cisco aligns so closely with these academic trends suggests a well-functioning system for technology transfer. It demonstrates that strategic foresight is being actively practiced by these leading firms, who are using their understanding of research fronts to guide their investment in innovation.

Strategic Foresight and Future Directions

The findings of this study offer valuable strategic foresight for a wide range of stakeholders. For policymakers, the results highlight the importance of targeted funding for the identified emerging research clusters. Supporting research in areas like deep learning and blockchain could give nations a competitive advantage in developing next-generation defenses. The data also underscores the need for policies that encourage collaboration between academic institutions and the private sector, as this is a key driver of innovation [82, 85]. Furthermore, the focus on human factors and supply chain security suggests that a holistic, interdisciplinary approach is necessary for future cybersecurity strategies. It's not just about building better firewalls; it's about creating a more secure ecosystem from end-to-end.

For R&D managers and investors, this study provides a roadmap for future investment. The identified research clusters represent high-potential areas for new product development and market entry. Companies seeking to gain a foothold in the cybersecurity market can use these findings to identify promising technological areas, while established players can use the information to refine their R&D portfolios and stay ahead of competitors. The dominance of a few key players like IBM also suggests opportunities for partnerships, mergers, or acquisitions with smaller firms that are innovating in these specific emerging areas.

Implications for Practice and Policy

The practical implications of this research are significant. Cybersecurity professionals can use these insights to stay current with the latest trends and technologies. For example, a security professional can focus on acquiring skills in deep learning or blockchain, knowing that these are the areas where the field is heading. For government agencies, the findings can inform the development of national cybersecurity strategies, ensuring that resources are allocated to the most critical and promising areas of R&D. Furthermore, the focus on human behavior highlights the need for public policy initiatives aimed at increasing general cybersecurity awareness and education. By understanding how attackers exploit human vulnerabilities, we can develop more effective training programs and public campaigns [88].

From a policy perspective, the study confirms the need for harmonized standards and disclosure protocols, especially as technologies like AI and blockchain become more integrated into the critical infrastructure [1]. The rise of cyber-physical systems, as seen in the patent data, necessitates a new set of regulations and policies that govern the security of these interconnected devices and networks. The findings provide a data-driven basis for these discussions, moving them from theoretical arguments to informed, evidence-based policy decisions.

Limitations and Future Research

This study, while comprehensive, is not without its limitations. First, our data collection, while extensive, is inherently tied to the databases we accessed (Scopus, Web of Science, USPTO, EPO). This may introduce a bias, as some relevant publications or patents may exist in other, less-indexed sources. The nature of patent data, in particular, means that it may not capture all private R&D activities that are kept as trade secrets.

Second, the interpretation of clusters and themes is a qualitative step that relies on the researcher's judgment. While we made every effort to be objective, different researchers might interpret the same data differently. Future research could address these limitations by incorporating data from a wider range of sources, including technical reports and gray literature. It would also be valuable to conduct a more granular analysis of specific sub-fields, such as the evolution of quantum cryptography or the security of specific IoT protocols. Finally, a comparative study of the R&D ecosystems in different countries would provide a deeper understanding of regional strengths and collaborative opportunities.

References

1. Daim, T., Yalcin, H., Mermoud, A., et al. (2024). Exploring cybertechnology standards through bibliometrics: case of National Institute of Standards And Technology. World Patent Inf., 77, 102278. [https://doi.org/10.1016/j.wpi.2024.102278](https://www.google.com/search?q=https://doi.org/10.1016/j.wpi.2024.102278)

2. Yalcin, H., Daim, T., Moughari, M. M., et al. (2024). Supercomputers and quantum computing on the axis of cyber security. Technol. Soc., 77, 102556. [https://doi.org/10.1016/j.techsoc.2024.102556](https://www.google.com/search?q=https://doi.org/10.1016/j.techsoc.2024.102556)

3. Fujita, K., Kajikawa, Y., Mori, J., et al. (2014). Detecting research fronts using different types of weighted citation networks. J. Eng. Technol. Manag., 32, 129–146. https://doi.org/10.1016/j.jengtecman.2013.07.002

4. Herrmann, H. (2022). The arcanum of artificial intelligence in enterprise applications: toward a unified framework. J. Eng. Technol. Manag., 66, 101716. [https://doi.org/10.1016/j.jengtecman.2022.101716](https://www.google.com/search?q=https://doi.org/10.1016/j.jengtecman.2022.101716)

5. Díaz-Garrido, E., Pinillos, M.-J., Soriano-Pinar, I., et al. (2018). Changes in the intellectual basis of servitization research: a dynamic analysis. J. Eng. Technol. Manag., 48, 1–14. [https://doi.org/10.1016/j.jengtecman.2018.01.005](https://www.google.com/search?q=https://doi.org/10.1016/j.jengtecman.2018.01.005)

6. Martín-Peña, M. L., Pinillos, M.-J., & Reyes, L.-E. (2017). The intellectual basis of servitization: a bibliometric analysis. J. Eng. Technol. Manag., 43, 83–97. [https://doi.org/10.1016/j.jengtecman.2017.01.005](https://www.google.com/search?q=https://doi.org/10.1016/j.jengtecman.2017.01.005)

7. Pitt, C., Park, A., & McCarthy, I. P. (2021). A bibliographic analysis of 20 years of research on innova-tion and new product development in technology and innovation management (TIM) journals. J. Eng. Technol. Manag., 61, 101632. https://doi.org/10.1016/j.jengtecman.2021.101632

8. Soranzo, B., Nosella, A., & Filippini, R. (2016). Managing firm patents: a bibliometric investigation into the state of the art. J. Eng. Technol. Manag., 42, 15–30. https://doi.org/10.1016/j.jengtecman.2016.08.002

9. Naeini, B. A., Zamani, M., Daim, T. U., et al. (2022). Conceptual structure and perspectives on “innovation management”: a bibliometric review. Technol. Forecast. Soc. Change, 185, 122052. [https://doi.org/10.1016/j.techfore.2022.122052](https://www.google.com/search?q=https://doi.org/10.1016/j.techfore.2022.122052)

10. Yalcin, H., & Daim, T. (2021). A scientometric review of technology capability research. J. Eng. Technol. Manag., 62, 101658. https://doi.org/10.1016/j.jengtecman.2021.101658

11. Ittipanuvat, V., Fujita, K., Sakata, I., et al. (2014). Finding linkage between technology and social issue: a literature based discovery approach. J. Eng. Technol. Manag., 32, 160–184. https://doi.org/10.1016/j.jengtecman.2013.05.006

12. Yang, H., & Jung, W.-S. (2016). Structural dynamics of keyword networks: liquid crystal display and plasma display panel cases. J. Eng. Technol. Manag., 40, 64–75. [https://doi.org/10.1016/j.jengtecman.2016.04.002](https://www.google.com/search?q=https://doi.org/10.1016/j.jengtecman.2016.04.002)

13. Newman, N. C., Porter, A. L., Newman, D., et al. (2014). Comparing methods to extract technical content for technological intelligence. J. Eng. Technol. Manag., 32, 97–109. https://doi.org/10.1016/j.jengtecman.2013.09.001

14. Frenken, K., Hölzl, W., & de Vor, F. (2005). The citation impact of research collaborations: the case of European biotechnology and applied microbiology (1988–2002). J. Eng. Technol. Manag., 22(1–2), 9–30. https://doi.org/10.1016/j.jengtecman.2004.11.002

15. Cunningham, S. W., & Kwakkel, J. H. (2014). Tipping points in science: a catastrophe model of scientific change. J. Eng. Technol. Manag., 32, 185–205. https://doi.org/10.1016/j.jengtecman.2014.01.002

16. Jeong, K., Noh, H., Song, Y.-K., et al. (2017). Essential patent portfolios to monitor technology standardization strategies: case of LTE-A technologies. J. Eng. Technol. Manag., 45, 18–36. [https://doi.org/10.1016/j.jengtecman.2017.07.001](https://www.google.com/search?q=https://doi.org/10.1016/j.jengtecman.2017.07.001)

17. Cammarano, A., Varriale, V., Michelino, F., et al. (2023). The importance of possessing knowledge on black-box components: the case of smartphone OEMs. J. Eng. Technol. Manag., 67, 101727. [https://doi.org/10.1016/j.jengtecman.2022.101727] (https://www.google.com/search?q=https://doi.org/10.1016/j.jengtecman.2022.101727)

18. Giglio, C. (2021). Cross-country creativity and knowledge flows of patent acquisitions: drivers and implications for managers and policymakers. J. Eng. Technol. Manag., 59, 101617. [https://doi.org/10.1016/j.jengtecman.2021.101617] (https://doi.org/10.1016/j.jengtecman.2021.101617)

19. Huang, J. (2016). Patent portfolio analysis of the cloud computing industry. J. Eng. Technol. Manag., 39, 45–64. https://doi.org/10.1016/j.jengtecman.2016.01.002

20. Jeong, S., & Lee, S. (2015). What drives technology convergence? Exploring the influence of technological and resource allocation contexts. J. Eng. Technol. Manag., 36, 78–96. https://doi.org/10.1016/j.jengtecman.2015.05.004

21. Lai, Y., & Che, H.-C. (2009). Evaluating patents using damage awards of infringement lawsuits: a case study. J. Eng. Technol. Manag., 26(3), 167–180. https://doi.org/10.1016/j.jengtecman.2009.06.005

22. Levitas, E. F., McFadyen, M. A., & Loree, D. (2006). Survival and the introduction of new technology: a patent analysis in the integrated circuit industry. J. Eng. Technol. Manag., 23(3), 182–201. https://doi.org/10.1016/j.jengtecman.2006.06.008

23. Roepke, S., & Moehrle, M. G. (2014). Sequencing the evolution of technologies in a system-oriented way: the concept of technology-dna. J. Eng. Technol. Manag., 32, 110–128. https://doi.org/10.1016/j.jengtecman.2013.08.005

24. Zhang, H., Daim, T., & Zhang, Y. (2021). Integrating patent analysis into technology roadmapping: a latent dirichlet allocation-based technology assessment and roadmapping in the field of blockchain. Technol. Forecast. Soc. Change, 167. https://doi.org/10.1016/j.techfore.2021.120729

25. Li, S., Garces, E., & Daim, T. (2019). Technology forecasting by analogy-based on social network analysis: the case of autonomous vehicles. Technol. Forecast. Soc. Change, 148, 119731. https://doi.org/10.1016/j.techfore.2019.119731

26. Zeba, G., Dabić, M., Čičak, M., et al. (2021). Technology mining: artificial intelligence in manufacturing. Technol. Forecast. Soc. Change, 171, 120971. https://doi.org/10.1016/j.techfore.2021.120971

27. Daim, T., Lai, K. K., Yalcin, H., et al. (2020). Forecasting technological positioning through technol-ogy knowledge redundancy: patent citation analysis of IoT, cybersecurity, and Blockchain. Technol. Forecast. Soc. Change, 161, 120329. https://doi.org/10.1016/j.techfore.2020.120329

28. Gonçalves Pereira, C., Ricardo Lavoie, J., & Garces, E., et al. (2019). Forecasting of emerging therapeutic

monoclonal antibodies patents based on a decision model. Technol. Forecast. Soc. Change, 139, 185–199. [https://doi.org/10.1016/j.techfore.2018.11.002](https://www.google.com/search?q=https://doi.org/10.1016/j.techfore.2018.11.002)

29. Li, X., Wu, Y., Cheng, H., et al. (2023). Identifying technology opportunity using SAO semantic mining and outlier detection method: a case of triboelectric nanogenerator technology. Technol. Forecast. Soc. Change, 189, 122353. [https://doi.org/10.1016/j.techfore.2023.122353](https://www.google.com/search?q=https://doi.org/10.1016/j.techfore.2023.122353)

30. Lai, K., Chen, Y.-L., Kumar, V., et al. (2023). Mapping technological trajectories and exploring knowledge sources: a case study of E-payment technologies. In: Technological forecasting and social change, 186. https://doi.org/10.1016/j.techfore.2022.122173

31. Li, X., Xie, Q., Daim, T., et al. (2019). Forecasting technology trends using text mining of the gaps between science and technology: the case of perovskite solar cell technology. Technol. Forecast. Soc. Change, 146, 432–449. https://doi.org/10.1016/j.techfore.2019.01.012

32. Li, S., Zhang, X., Xu, H., et al. (2020). Measuring strategic technological strength: patent portfolio Model. Technol. Forecast. Soc. Change, 157, 120119. https://doi.org/10.1016/j.techfore.2020.120119

33. Li, X., Wen, Y., Jiang, J., et al. (2022). Identifying potential breakthrough research: a machine learning method using scientific papers and twitter data. Technol. Forecast. Soc. Change, 184, 122042. https://doi.org/10.1016/j.techfore.2022.122042