

Mapping the Current Status of CTI Knowledge Graphs through a Bibliometric Analysis

Maria Papoutsoglou
School of Informatics,
Aristotle University of Thessaloniki
Thessaloniki, Greece
mpapo@csd.auth.gr

Georgios Meditskos
School of Informatics,
Aristotle University of Thessaloniki
Thessaloniki, Greece
gmeditsk@csd.auth.gr

Nick Bassiliades
School of Informatics,
Aristotle University of Thessaloniki
Thessaloniki, Greece
nbassili@csd.auth.gr

Efstiratos Kontopoulos
Foodpairing NV
Belgium
skontopo2009@gmail.com

Stefanos Vrochidis
Information Technologies Institute,
Centre for Research and Technology
Hellas
Thessaloniki, Greece
stefanos@iti.gr

Abstract

Bibliometric analysis in the field of cybersecurity and Cyber Threat Intelligence (CTI) is crucial for identifying research trends, key themes, and collaborative networks, which can guide future research directions and policy decisions. This paper presents a comprehensive bibliometric analysis of the current status of research on knowledge graphs in cybersecurity, highlighting significant trends and thematic clusters. The analysis reveals a rapidly growing interest in integrating knowledge graphs with advanced machine learning and AI techniques, such as deep learning and neural networks, to enhance cyber threat intelligence and response strategies. Key findings include the prominence of natural language processing, entity recognition, and relation extraction as critical methodologies in this field. Thematic evolution analysis shows the adoption of large language models (LLMs) and an ongoing focus on structured knowledge representation. The study underscores the potential of knowledge graphs to improve cybersecurity through better data organization, threat detection, and intelligence extraction.

CCS Concepts

• **Information systems** → *World Wide Web*; **Web Ontology Language (OWL)**; **Ontologies**.

Keywords

Knowledge Graphs, CTI, Cybersecurity, Bibliometric Analysis

ACM Reference Format:

Maria Papoutsoglou, Georgios Meditskos, Nick Bassiliades, Efstiratos Kontopoulos, and Stefanos Vrochidis. 2024. Mapping the Current Status of CTI Knowledge Graphs through a Bibliometric Analysis. In *13th Conference on Artificial Intelligence (SETN 2024)*, September 11–13, 2024, Piraeus, Greece. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3688671.3688738>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

SETN 2024, September 11–13, 2024, Piraeus, Greece

© 2024 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-0982-1/24/09

<https://doi.org/10.1145/3688671.3688738>

1 Introduction

With the rapid expansion of raw data in the Web 3.0 era and the transition to Web 4.0, the volume of data from online sources is growing exponentially. This increase requires the use of sophisticated data analysis techniques to process raw data, derive meaningful insights, and generate knowledge. Knowledge graphs, ontologies, and the semantic web play a crucial role in meeting this rising need to analyze and meaningfully present raw information. Knowledge graphs enable the representation of data in a structured and interconnected manner, facilitating enhanced data integration and retrieval [9]. Ontologies provide a formal framework for categorizing and relating concepts, improving the consistency and interoperability of data [12]. The semantic web, by extending the principles of the web to data, enhances the ability to link and query disparate data sources seamlessly [17]. Together, these technologies address the challenges of big data by offering robust solutions for data management and knowledge extraction, ultimately supporting more informed decision-making in various domains [3].

Knowledge Graphs [8] are a type of knowledge base that utilize a graph-based abstraction to organize data. They are typically built using Semantic Web (SW) technologies [15], which include various models and languages designed for data representation and utilization. The core of this technology is the Resource Description Framework (RDF), which aims to create a universal standard for modeling specific domains through sets of assertions [5]. Each piece of information in this framework is represented as a statement in the form of an ordered triple of entities or resources. These statements form a directed multi-relational graph, where nodes represent entities (such as individuals, places, or objects) and edges represent the semantic connections between these entities, effectively organizing complex relationships and concepts.

In this paper, we focus on the application of knowledge graphs in Cyber Threat Intelligence (CTI). CTI refers to the collection, processing, and analysis of information about potential or current attacks that threaten an organization's security. Cybersecurity, on the other hand, encompasses the practices and technologies used to protect networks, devices, and data from unauthorized access or attacks. The integration of knowledge graphs in CTI provides

significant advantages. Knowledge graphs enable the organization and visualization of complex relationships between different data points, enhancing the ability to detect and respond to threats more efficiently. By structuring data in a graph format, knowledge graphs facilitate advanced analytics, pattern recognition, and the discovery of hidden connections within vast amounts of cybersecurity data [16].

Conducting a bibliometric study in this field is crucial for several reasons. Firstly, it helps identify the current state of research, revealing the most influential studies, prevalent themes, and research gaps [4]. Understanding these patterns can guide future research directions and foster collaboration among researchers. Secondly, as the field of cybersecurity evolves rapidly, a bibliometric analysis provides insights into emerging trends and technologies, such as the adoption of knowledge graphs. This systematic review and analysis help stakeholders stay informed about the latest developments and the overall impact of integrating knowledge graphs in CTI [19].

The rest of the paper is structured as follows. The related work section focuses on existing research on knowledge graphs and CTI, highlighting the need for further investigation in this area. The methodology section outlines our approach to conducting the bibliometric analysis. In the results section, we address three main research questions (RQs). RQ1 examines the yearly evolution and primary thematic trends in research related to knowledge graphs and cybersecurity. RQ2 identifies the main thematic clusters in this research area and explores how they interconnect. RQ3 investigates how research themes in cybersecurity knowledge graphs have evolved from 2016 to 2024. Finally, we present our conclusions and discuss potential directions for future research.

2 Related Work

Cybersecurity knowledge graphs enhance the presentation of threat knowledge, allowing security researchers to efficiently access diverse information and make informed decisions.

In academic research, Kiesling constructed the SEPSES Knowledge Graph (SKG)[11], demonstrating how to derive security alerts from Snort and link them to SKG for deeper insights into cyber threats. Deng et al.[6] established a cybersecurity practices knowledge graph for students, utilizing big data and NLP techniques to explore interconnected cybersecurity concepts. Du et al.[7] created a concise, human-readable threat intelligence recommendation system driven by knowledge graphs, encompassing security items, network entities, and emerging hacker groups. Mozzaquator et al.[13] introduced an ontology-based network security framework for the Internet of Things (IoT), aiding in monitoring devices, categorizing threats, and implementing countermeasures. In practical contexts, enterprises like IBM's X-Force Exchange¹, the 360 Alpha Threat Analysis Platform², and Weibu³ Online have adopted knowledge graphs for proprietary threat intelligence analysis.

Various research initiatives are tackling cybersecurity challenges with innovative approaches. One such initiative, CSKG4APT, leverages knowledge graph technology and ontology for extracting and utilizing open-source cyber threat intelligence, particularly for advanced persistent threats (APTs)[14]. Another framework, powered

by deep learning and knowledge graph question-answering (KGQA), addresses the complexity of IoT environments by efficiently responding to natural language inquiries in forensic analysis[21]. Further research has focused on enhancing Network Security Situation Awareness (NSSA) through an extended cybersecurity ontology, validated in various awareness scenarios[20]. In education, AI-enabled strategies using Knowledge Graphs and tailored ontologies, like AISeckG, transform unstructured materials into interactive learning modules, enhancing cybersecurity education[2]. Other efforts include developing an intelligent classification knowledge graph of botnets for AI applications, aiding in botnet analysis and mitigation[1]. Additionally, integrating machine learning and graph-structured data for intrusion detection, with Graph Neural Networks (GNNs) and Explainable AI (XAI), has shown significant efficacy in reducing false positives[10].

These studies exemplify the multifaceted approach needed to address cybersecurity challenges. The Unified Cyber Ontology (UCO) acts as a foundational structure for connecting various cybersecurity ontologies, aligning with global knowledge sources to facilitate comprehensive applications and data resource utilization[16, 18]. All the aforementioned approaches are empirical and represent state-of-the-art methods in the areas of CTI and cybersecurity using graphs. However, the proposed bibliographic approach aims to provide a more comprehensive overview of the field through the analysis of literature trends. Specifically, the goal is to map the area of knowledge graph usage in the domain of CTI and cybersecurity. To our knowledge, there has not been a comprehensive bibliographic analysis specifically focused on the application of knowledge graphs in CTI and cybersecurity. However, existing literature does include a bibliometric study that examines the general use of knowledge graphs and identifies related trends [19]. Additionally, there is a study that explores empirical aspects of knowledge graphs in CTI, such as the implementation of specific protocols [16].

3 Methodology

In this study, we employed a systematic methodology to collect and analyze the dataset. We used the Scopus database to gather raw data with the query "knowledge graph*" AND ("cti" OR "cybersecurity"), resulting in a total of 201 papers. This specific keyword string was chosen as it is highly representative of the intersection between knowledge graphs and cybersecurity, capturing the most relevant studies in this domain. The inclusion of both "CTI" and "cybersecurity" ensures comprehensive coverage of related areas, addressing the breadth of research in cyber threat intelligence and broader cybersecurity contexts. To ensure the dataset's quality, we implemented a basic preprocessing step where we retained only English language papers and removed duplicates based on their DOI. This preprocessing resulted in a cleaned dataset of 174 records.

To answer our research questions, we utilized the R programming language and the bibliometrix package (available at ⁴ along with the Bibliometrix Shiny package ⁵ for bibliometric analysis. These tools facilitated comprehensive text-based data analysis, essential for our bibliometric study. Given that bibliometric analysis

¹X-Force Exchange, Available: <https://exchange.xforce.ibmcloud.com>

²<https://ti.360.net>

³<https://x.threatbook.cn>

⁴<https://www.bibliometrix.org>

⁵<https://bibliometrix.org/Biblioshiny.html>

relies heavily on textual data, we implemented n-grams and additional text preprocessing steps, such as the identification and standardization of synonyms, to enhance the accuracy and quality of our analysis results. This methodological approach ensured robust and reliable insights into the research trends, thematic clusters, and evolution of knowledge graphs in the context of cybersecurity and CTI.

4 Results

4.1 RQ1: How is the yearly evolution and what are the primary thematic trends?

The Figure 1 illustrates the bibliographic evolution of research related to "knowledge graphs" in conjunction with "CTI (Cyber Threat Intelligence)" or "cybersecurity," derived from a Scopus search using the keywords "knowledge graph*" AND ("cti" OR "cybersecurity"). The graph demonstrates a rising trend in the volume of publications from 2016 to 2023, reflecting the growing importance and recognition of how knowledge graphs can add value in the field of cybersecurity. This increase underscores the heightened interest and ongoing developments in integrating knowledge graphs with cybersecurity solutions, particularly in enhancing CTI. Knowledge graphs bring structured data and interconnected relationships to the forefront, providing a dynamic and comprehensive framework that aids in the sophisticated analysis and visualization of cyber threats. By leveraging these capabilities, researchers and practitioners can enhance predictive threat modeling, improve the detection of sophisticated cyber threats, and streamline response strategies. The notable peak in 2023 suggests a significant surge in research activity and publications, indicating an increasing acknowledgment of the utility and potential of knowledge graphs in this specialized area. The absence of data for the year 2024 in this plot highlights the need for continued observation to determine if this upward trend will sustain, plateau, or evolve in new directions.

The dataset provides a comprehensive overview of the research landscape in the domain of knowledge graphs and cybersecurity. The annual growth rate of 37.8% highlights the rapidly increasing interest and advancements in this field. With a total of 680 authors contributing to the research, the community is robust and active. Interestingly, there are 5 authors of single-authored documents, which suggests that while collaborative efforts are predominant, individual contributions also play a significant role. The international co-authorship rate stands at 13.43%, indicating a strong global collaboration despite the relative novelty of the topic. On average, each document has 4.42 co-authors, reflecting the collaborative nature of research in this domain. The dataset includes 452 unique author keywords (DE), showcasing the diversity of research topics and areas of focus within the field. The average age of the documents is 2.06 years, pointing to a relatively young but rapidly growing body of literature. Additionally, the average number of citations per document is 7.89, indicating that the published works are being recognized and referenced by the academic community. These main information bibliometric metrics, underscore the dynamic and evolving interest in integrating knowledge graphs with cybersecurity research.

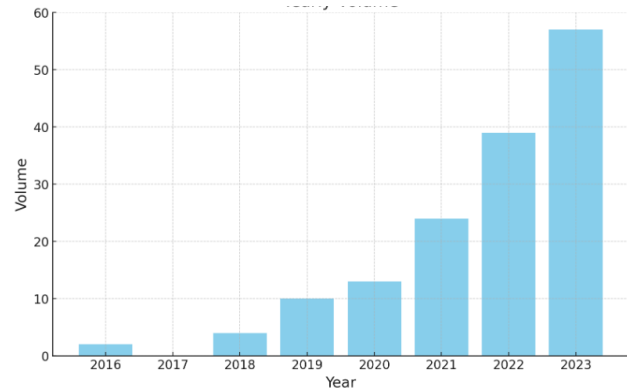


Figure 1: Yearly Evolution

4.2 RQ2: What are the main thematic clusters in research on knowledge graphs and cybersecurity, and how do they interconnect?

Creating a co-occurrence network based on author's keywords is particularly insightful as these keywords are directly provided by the authors to represent the core topics and themes of their research. Unlike Keywords Plus, which are algorithmically generated and may include terms not central to the paper, author's keywords reflect the intentional and precise focus of the research. Using title or abstract words could result in a broad and less focused network, as these texts often include a wider range of terms that might not be central to the research themes. The author's keywords ensure that the network accurately represents the key areas of interest and the specific language used within the research community. The co-occurrence network was constructed using the Louvain algorithm for clustering, which is effective in identifying communities within large networks. Normalization was performed using the Jaccard similarity metric to measure the similarity and enhance the comparability of different nodes. Isolated nodes were removed to focus on the most relevant and connected elements of the network.

The co-occurrence network graph in Figure 2 and its associated metrics provide a detailed overview of the interconnections and thematic clusters within the research on knowledge graphs and cybersecurity. The clusters identified reveal distinct thematic areas. Cluster 1 (see Figure 2-red cluster), which includes nodes such as "knowledge graph," "cybersecurity," "ontology," and "deep learning," highlights general trends and foundational concepts in the field. This cluster underscores the importance of integrating knowledge graphs with cybersecurity measures and advanced data analysis techniques. Cluster 2 (see Figure 2-blue cluster) features terms like "cyber threat intelligence," "named entity recognition," and "relation extraction," indicating a focus on specific analytical methods and their applications in cybersecurity. These methods fall under broader categories of data analysis techniques, emphasizing the role of detailed entity recognition and relationship mapping in threat intelligence.

Additionally, Cluster 3 (see Figure 2-green cluster), including "knowledge graphs," "artificial intelligence," and "threat intelligence,"

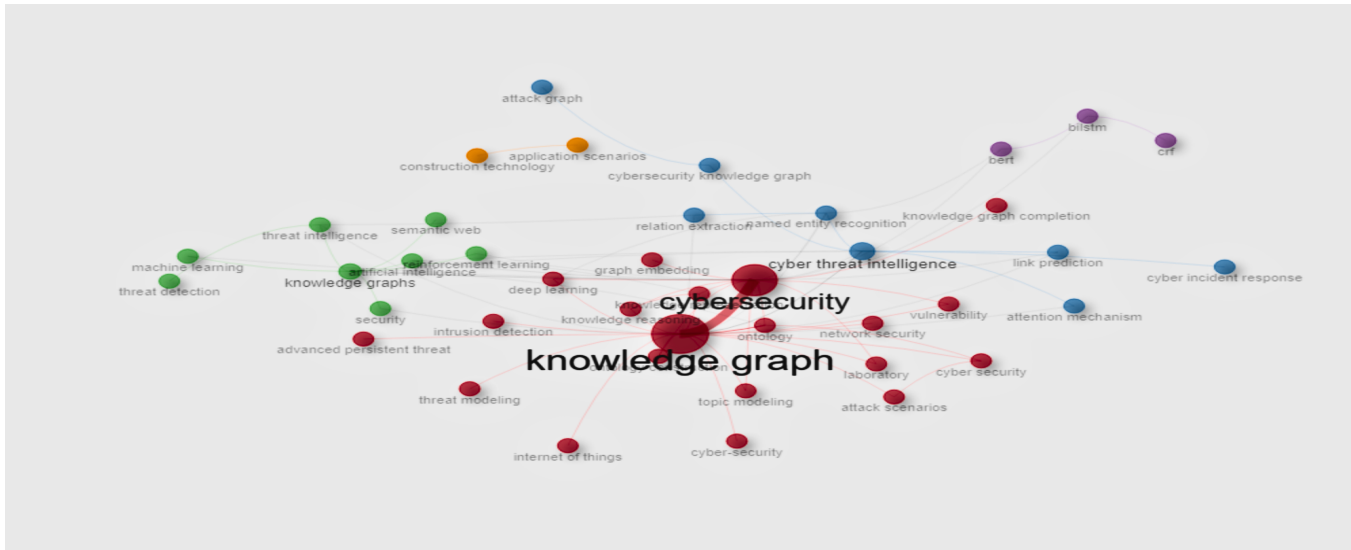


Figure 2: Co-occurrence Network

represents the intersection of knowledge graph technology with AI-driven approaches to enhance security measures and intelligence gathering. This cluster reflects the ongoing efforts to leverage machine learning and AI to improve threat detection and response. Cluster 4 (see Figure 2-purple cluster), with nodes such as "bert," "blstm," and "crf," is centered around specific machine learning models and frameworks used in natural language processing and cybersecurity. These models are critical for processing large volumes of text data and extracting relevant insights for security applications.

Finally, Cluster 5 (see Figure 2-yellow cluster), containing "application scenarios" and "construction technology," suggests a more applied perspective, focusing on the implementation and practical use cases of knowledge graphs in various technological and construction domains. These clusters collectively demonstrate the breadth and depth of research in this area, highlighting both general trends and specific analytical methods used to address the challenges in cybersecurity with the help of knowledge graphs.

4.3 RQ3:How have the research themes in cybersecurity knowledge graphs evolved from 2016 to 2024?

The thematic evolution plot reveals significant trends and transitions between different research themes over the specified periods. During the first period from 2016 to 2020, transitioning to the period from 2021 to 2022, several noteworthy keywords emerged (see Table 1). For instance, the transition from "cybersecurity domain" to "experimental results" highlighted the focus on natural language processing (NLP) techniques in cybersecurity research, with keywords such as "natural language" becoming prominent. Similarly, the shift from "cybersecurity domain" to "knowledge graph" was marked by important keywords like "named entity," "entity recognition," and "deep neural," indicating the adoption of advanced machine learning techniques for entity recognition within cybersecurity contexts. Additionally, the movement from "cybersecurity

ontology" to "knowledge graph" reflected a focus on structured representation with keywords like "cybersecurity ontology."

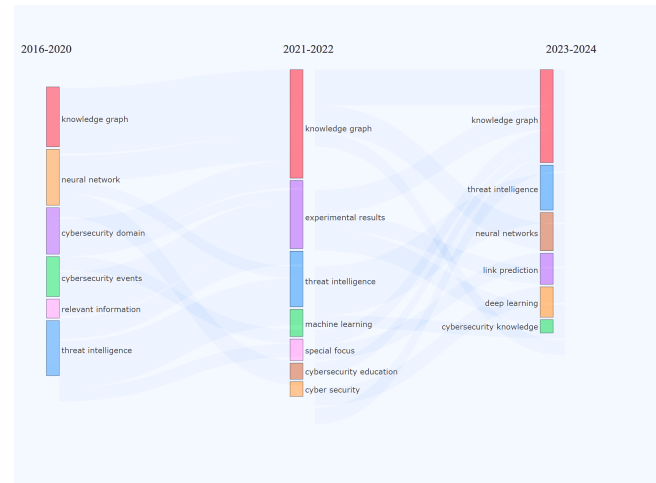


Figure 3: General Thematic Plot

A consistent focus on knowledge graphs for organizing and utilizing cybersecurity knowledge was reflected in the keywords "knowledge graph," "cybersecurity knowledge," and "data sources," seen in the transition from "knowledge graph" to "knowledge graph." The transition from "neural network" to "knowledge graph" brought forward keywords such as "knowledge base," "convolutional neural," and "deep learning," showing the integration of knowledge graph techniques with neural network methodologies.

In the second period from 2021 to 2022, transitioning to 2023 to 2024, further significant transitions were observed. The shift from "cyber security" to "deep learning" introduced the keyword "model based," signifying the move towards model-based approaches in

deep learning for cybersecurity. The transition from "cyber security" to "knowledge graph" included keywords such as "cyber security" and "graph embedding," indicating the continued integration of cybersecurity with knowledge graph techniques. The movement from "experimental results" to "knowledge graph" featured keywords like "experimental results," "security knowledge," "attack patterns," and "cyber attacks," highlighting a comprehensive approach to using knowledge graphs for documenting and analyzing cybersecurity incidents. The transition from "knowledge graph" to "neural networks" brought forward keywords like "entity recognition," "named entity," "convolutional neural," and "neural networks," showing the merging of knowledge graph techniques with neural network methodologies for enhanced cybersecurity applications. The shift from "machine learning" to "knowledge graph" reaffirmed the continuous application of machine learning techniques within the context of knowledge graphs, with "machine learning" as a prominent keyword.

General observations from the thematic evolution plot indicate a trend towards integrating more sophisticated machine learning techniques, such as deep learning and neural networks, with cybersecurity research. The recurring focus on "cybersecurity knowledge," "cybersecurity ontology," and "cyber threats" across multiple clusters signifies the growing importance of structured knowledge representation and threat intelligence in cybersecurity. The high occurrences of terms like "experimental results" and "threat intelligence" reflect a strong emphasis on empirical research and actionable insights in the cybersecurity domain. These observations illustrate the dynamic and evolving nature of research in cybersecurity, highlighting the integration of advanced computational techniques and the importance of structured knowledge representation in addressing contemporary cybersecurity challenges.

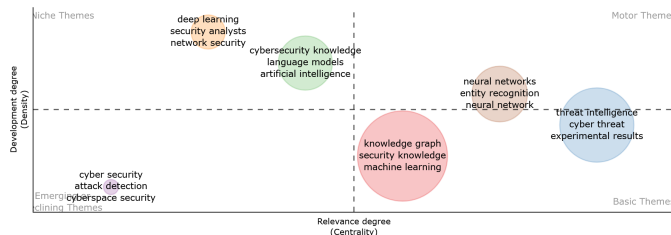


Figure 4: Thematic Evolution Plot for 2023-2024

As shown in Figure 4, the thematic evolution plot for the third time slice (2023-2024) reveals insightful trends and the adoption of new methodologies in cybersecurity research. For instance, the cluster related to "cybersecurity knowledge" prominently features the keyword "language models," indicating the increasing adoption of Large Language Models (LLMs) as a new trend in cybersecurity methods. This cluster highlights the shift towards more advanced natural language processing techniques for analyzing and managing cybersecurity data. Another example is the cluster focusing on "neural networks," which includes keywords like "entity recognition," "named entity," "convolutional neural," and "neural networks." This cluster underscores the merging of knowledge graph techniques with neural network methodologies, reflecting an enhanced

approach to cybersecurity applications that leverage deep learning for better threat detection and intelligence extraction.

Additionally, the "deep learning" cluster includes keywords such as "security analysts," "threat information," "network security," and "knowledge extraction." These keywords emphasize the ongoing integration of deep learning techniques in cybersecurity to improve threat analysis and response strategies. The emphasis on "security analysts" and "threat information" indicates a focus on using machine learning to aid human analysts in making more informed decisions based on vast amounts of data.

5 Conclusions

This bibliometric analysis provides an overview of the evolving research landscape at the intersection of knowledge graphs and cybersecurity. The increasing volume of publications, especially the surge in 2023, highlights the growing recognition of knowledge graphs' value in enhancing cyber threat intelligence (CTI) and response strategies.

Our findings reveal key trends and thematic clusters, emphasizing the integration of knowledge graphs with machine learning and artificial intelligence, particularly deep learning and neural networks. These combinations improve threat detection, entity recognition, and understanding of complex cybersecurity landscapes. Clusters focused on specific methods, like named entity recognition and relation extraction, underscore the importance of detailed data analysis in cybersecurity. The thematic evolution analysis shows a dynamic research environment, with trends such as adopting large language models (LLMs) for natural language processing in cybersecurity. This shift towards advanced methodologies addresses modern cybersecurity challenges. The recurring focus on structured knowledge representation highlights the importance of organizing and leveraging cybersecurity data effectively.

Future research should explore practical applications of knowledge graphs in real-world scenarios, developing scalable solutions for integration with existing cybersecurity infrastructures and assessing their effectiveness. Enhancing the interoperability of different cybersecurity ontologies and frameworks will facilitate broader data sharing and collaboration. Integrating explainable AI (XAI) techniques with knowledge graphs is another promising avenue, providing transparent insights and improving trust in AI-driven decisions. Expanding the use of knowledge graphs in areas like IoT security and cloud computing could offer new solutions to contemporary cybersecurity challenges.

In conclusion, the fusion of knowledge graphs with advanced machine learning and AI techniques marks a significant advancement in cybersecurity. Future work should focus on practical implementations, interoperability, and explainability to fully harness these technologies' potential in safeguarding digital environments.

Acknowledgment

This research has received funding from the Horizon Europe Framework Program under Grant Agreement No 101070670 ENCRYPT. The content of this publication reflects the opinion of its authors and does not, in any way, represent opinions of the funders. The European Commission are not responsible for any use that may be made of the information that this publication contains.

Period	From	To	Keywords
2016-2020 to 2021-2022	cybersecurity domain	experimental results	natural language
2016-2020 to 2021-2022	cybersecurity domain	knowledge graph	named entity; entity recognition; deep neural
2016-2020 to 2021-2022	cybersecurity domain	machine learning	cybersecurity domain
2016-2020 to 2021-2022	cybersecurity ontology	knowledge graph	cybersecurity ontology
2016-2020 to 2021-2022	knowledge graph	knowledge graph	knowledge graph; cybersecurity knowledge; data sources
2016-2020 to 2021-2022	neural network	knowledge graph	knowledge base; convolutional neural; deep learning; neural networks
2016-2020 to 2021-2022	threat intelligence	threat intelligence	threat intelligence; cyber threat; security analysts; intelligence cti; intelligence osint
2021-2022 to 2023-2024	cyber security	knowledge graph	cyber security; graph embedding
2021-2022 to 2023-2024	experimental results	deep learning	network security; advanced persistent; apt attacks; persistent threat; threat apt; apt attack
2021-2022 to 2023-2024	knowledge graph	knowledge graph	knowledge graph; graph based; data sources
2021-2022 to 2023-2024	knowledge graph	neural networks	entity recognition; named entity; convolutional neural; neural networks; entity extraction; recognition ner; conditional random; cybersecurity corpus; cybersecurity datasets; cybersecurity entities
2021-2022 to 2023-2024	machine learning	neural networks	intrusion detection; cybersecurity domain
2021-2022 to 2023-2024	threat intelligence	deep learning	security analysts; threat information
2021-2022 to 2023-2024	threat intelligence	neural networks	neural network
2021-2022 to 2023-2024	threat intelligence	threat intelligence	threat intelligence; cyber threat; intelligence cti; relation extraction; information extraction; application scenarios

Table 1: Thematic Evolution of Keywords from 2016 to 2024

References

- [1] Omotola Adekanmbi, Hayden Wimmer, and Atef Shalan. 2023. Semantic Web Ontology for Botnet Classification. In *Semantic Intelligence: Select Proceedings of ISIC 2022*. Springer, 43–54.
- [2] Garima Agrawal. 2023. Aiseckg: Knowledge graph dataset for cybersecurity education. *AAAI-MAKE 2023: Challenges Requiring the Combination of Machine Learning 2023* (2023).
- [3] Min Chen, Shiwen Mao, Yin Zhang, Victor CM Leung, et al. 2014. *Big data: related technologies, challenges and future prospects*. Vol. 100. Springer.
- [4] Xieling Chen, Haoran Xie, Zongxi Li, and Gary Cheng. 2021. Topic analysis and development in knowledge graph research: A bibliometric review on three decades. *Neurocomputing* 461 (2021), 497–515.
- [5] S. Decker, P. Mitra, and S. Melnik. 2000. Framework for the semantic Web: an RDF tutorial. *IEEE Internet Computing* 4, 6 (2000), 68–73.
- [6] Yuli Deng, Duo Lu, Dijiang Huang, Chun-Jen Chung, and Fanjie Lin. 2019. Knowledge graph based learning guidance for cybersecurity hands-on labs. In *Proceedings of the ACM conference on global computing education*. 194–200.
- [7] Ming Du, Jun Jiang, Zhengwei Jiang, Zhigang Lu, and Xiangyu Du. 2019. PRTIRG: a knowledge graph for people-readable threat intelligence recommendation. In *Knowledge Science, Engineering and Management: 12th International Conference, KSEM 2019, Athens, Greece, August 28–30, 2019, Proceedings, Part I* 12. Springer, 47–59.
- [8] Dieter Fensel, Umutcan Şimşek, Kevin Angele, Elwin Huaman, Elias Kärle, Oleksandra Panasiuk, Ioan Toma, Jürgen Umbrich, and Alexander Wahler. 2020. *Introduction: What Is a Knowledge Graph?* Springer International Publishing, Cham, 1–10.
- [9] Dieter Fensel, Umutcan Simsek, Kevin Angele, Elwin Huaman, Elias Kärle, Oleksandra Panasiuk, Ioan Toma, Jürgen Umbrich, and Alexander Wahler. 2020. *Knowledge graphs*. Springer.
- [10] Anna Himmelhuber, Dominik Dold, Stephan Grimm, Sonia Zillner, and Thomas Runkler. 2022. Detection, Explanation and Filtering of Cyber Attacks Combining Symbolic and Sub-Symbolic Methods. In *2022 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 381–388.
- [11] Elmar Kiesling, Andreas Ekelhart, Kabul Kurniawan, and Fajar Ekaputra. 2019. The SEPSSES knowledge graph: an integrated resource for cybersecurity. In *International Semantic Web Conference*. Springer, 198–214.
- [12] Gabriel da Silva Serapião Leal, Wided Guédria, and Hervé Panetto. 2019. An ontology for interoperability assessment: A systemic approach. *Journal of Industrial Information Integration* 16 (2019), 100100.
- [13] Bruno Augusti Mozzaquatro, Carlos Agostinho, Diogo Goncalves, João Martins, and Ricardo Jardim-Goncalves. 2018. An ontology-based cybersecurity framework for the internet of things. *Sensors* 18, 9 (2018), 3053.
- [14] Yitong Ren, Yanjun Xiao, Yinghai Zhou, Zhiyong Zhang, and Zhihong Tian. 2022. Cskg4apt: A cybersecurity knowledge graph for advanced persistent threat organization attribution. *IEEE Transactions on Knowledge and Data Engineering* 35, 6 (2022), 5695–5709.
- [15] N. Shadbolt, T. Berners-Lee, and W. Hall. 2006. The Semantic Web Revisited. *IEEE Intelligent Systems* 21, 3 (2006), 96–101.
- [16] Leslie F Sikos. 2023. Cybersecurity knowledge graphs. *Knowledge and Information Systems* 65, 9 (2023), 3511–3531.
- [17] Dimitrios-Emmanuel Spanos, Periklis Stavrou, and Nikolas Mitrou. 2012. Bringing relational databases into the semantic web: A survey. *Semantic Web* 3, 2 (2012), 169–209.
- [18] Zareen Syed, Ankur Padia, Tim Finin, Lisa Mathews, and Anupam Joshi. 2016. UCO: A unified cybersecurity ontology. In *Workshops at the thirtieth AAAI conference on artificial intelligence*.
- [19] Gang Wang and Jing He. 2024. A Bibliometric Analysis of Recent Developments and Trends in Knowledge Graph Research (2013-2022). *IEEE Access* (2024).
- [20] Yixuan Wang, Bo Zhao, Weidong Li, and Lingzi Zhu. 2023. An Ontology-Centric Approach for Network Security Situation Awareness. In *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 777–787.
- [21] Ruipeng Zhang and Mengjun Xie. 2023. A knowledge graph question answering approach to iot forensics. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*. 446–447.