doi:10.3969/j.issn.1001-4616.2025.04.013

跨平台工具链探索网络安全知识图谱研究进展与趋势

刘启恒[1],李雪莲[1,2],孙孟娜[1]

(1.南京邮电大学外国语学院,江苏 南京 210023)
(2.南京邮电大学信息产业发展战略研究院,江苏 南京 210023)

[**摘要**] 在数字化时代,网络安全已成为全球性挑战. 网络攻击手段的日益复杂和多变对网络安全领域的研究提出了更高的要求. 本研究基于文献计量方法,融合 CiteSpace 与 SciExplorer-LDGAS 工具链,对 2011—2024 年间的 343 篇中英文文献(含 CNKI 中文核心文献 84 篇、Web of Science 核心英文文献 259 篇)进行系统性分析,探究网络安全知识图谱领域的研究趋势、合作网络及热点演变. 研究结果表明:(1)该领域发文量自 2017 年起显著增长,2023—2024 年达到峰值,反映计算机技术的发展与学术关注度的增强;(2)作者与机构合作呈现区域性聚集特征,中美两国研究贡献领先(分别占比 27%和 25%),欧美国家合作较多,但其余跨国合作网络稀疏;(3)关键词分析揭示国内外研究侧重差异:国内聚焦技术突破,国外则侧重应用优化;中英文文献也呈现出显著趋同性,具体聚焦于网络威胁情报、本体构建以及人工智能(AI)等核心方向;(4)研究热点从早期“态势感知”“可视分析”向“知识图谱构建”“攻击模式预测”演进,凸显人工智能技术驱动的防御体系升级需求. 基于此,本文提出需加强跨国、跨机构协作,建立统一的知识共享平台,推动知识图谱技术与多源威胁情报的深度整合,为构建网络空间命运共同体提供理论与工具支撑.

[**关键词**] 知识图谱,CiteSpace 与 SciExplorer-LDGAS,文献计量分析,网络安全,网络空间命运共同体,人工智能技术

[**中图分类号**]TP393.08;TP391.1　[**文献标志码**]A　[**文章编号**]1001-4616(2025)04-0128-11

Exploring Research Advancements and Trends in Cybersecurity Knowledge Graphs via Cross-Platform Toolchains

Liu Qiheng[1], Li Xuelian[1,2], Sun Mengna[1]

(1.School of Foreign Languages, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)
(2.Institute of Information Industry Development Strategy, Nanjing University of Posts and Telecommunication, Nanjing 210023, China)

Abstract: In the digital era, cybersecurity has become a global challenge. With the increasing complexity and variability of cyberattack methods, research in the cybersecurity field faces heightened demands. This study employs bibliometric methods, integrate the CiteSpace and SciExplorer-LDGAS toolchains, to conduct a systematic analysis of 343 Chinese and English literature articles from 2011 to 2024(including 84 Chinese core articles from CNKI and 259 English core articles from Web of Science). The goal is to explore research trends, collaborative networks, and the evolution of hotspots in the domain of cybersecurity knowledge graphs. The findings reveal that:(1)The volume of publications in this field has grown significantly since 2017, peaking in 2023-2024, reflecting advancements in computer technology and increased academic attention;(2)Author and institutional collaborations exhibit regional clustering, with China and the United States leading in research contributions(27% and 25%, respectively), while European and American countries show stronger intra-regional collaboration, though transnational networks remain sparse;(3)Keyword analysis highlights divergent research focuses: domestic studies prioritize technological breakthroughs, whereas international studies emphasize application optimization.

收稿日期:2025-04-26.
基金项目:国家社会科学基金项目(WYZL2023JS0013)、江苏省社科应用研究精品工程地方志专项课题重点项目(23SFZA-08)、江苏省“双创博士”项目(JSSCBS20220624).
通讯作者:李雪莲,博士,讲师,研究方向:计算语言学、语料库语言学. E-mail:lixuelian@njupt.edu.cn

Both Chinese and English literature demonstrate significant convergence on core directions such as cyber threat intelligence, ontology construction, and artificial intelligence (AI); (4) Research hotspots have evolved from early themes like "situation awareness" and "visual analytics" to "knowledge graph construction" and "attack pattern prediction", underscoring the demand for AI-driven upgrades in defense systems. Based on these findings, this study proposes enhancing transnational and cross-institutional collaboration, establishing unified knowledge-sharing platforms, and promoting deeper integration of knowledge graph technologies with multi-source threat intelligence, thereby providing theoretical and technical support for building a Community of Shared Future in Cyberspace.

Key words: knowledge graph, CiteSpace and SciExplorer-LDGAS, bibliometric analysis, cybersecurity, Community of Shared Future in Cyberspace, artificial intelligence technology

党的十八大以来,习近平总书记深刻把握信息化发展大势,高度关注网络安全挑战,多次在不同场合就网络安全发表一系列重要论述,把我们党对网络安全的认识提升到了新的高度和境界,为树立正确的网络安全观、做好网络安全工作提供了根本遵循和强大动力[1]. 在数字化时代,网络安全已成为全球性挑战,涉及个人隐私、企业数据、国家安全等多个层面. 网络攻击手段的日益复杂和多变,对网络安全领域的研究提出了更高的要求.

在网络安全领域,知识图谱的应用深度与广度持续提升. 网络攻击手段的智能化演进,传统规则匹配方法在复杂攻击场景下溯源效率显著下降[2],将知识图谱引入网络安全领域有助于描绘复杂的网络安全态势,并为威胁识别和态势感知提供技术支持[3]. 知识图谱作为一种实体和概念等知识的高效组织形式,能够充分发挥其知识整合的优势,将零散分布的多源异构数据通过专门设计的框架组织起来,为数据分析和知识挖掘提供支持. 在应用的预测层面,可以通过利用知识表示、知识推理模型补全关系,发现新的关系,为网络空间科学化防御提供辅助决策[4].

现有研究呈现两大局限,一方面缺乏跨平台、跨语言的系统性文献分析,另一方面知识图谱作为整合工具的系统性研究仍存在缺口,跨国合作研究不足. 网络安全领域文献计量分析的现有研究往往关注网络安全具体问题或概括性评估研究,如网络安全评估研究[5]、国外网络欺凌研究热点与实践对策[6]、网络空间安全研究态势分析[7]、国内外网络治理研究[8]、网络舆情研究[9]、大数据时代信息安全研究[10]等,缺少针对知识图谱这一重要工具的使用和应用发展的系统性研究. 本文聚焦国内外网络安全知识图谱相关研究,旨在通过跨平台将具有一定人工智能技术的 CiteSpace(v.6.3.R1.64-bit)与 SciExplorer-LDGAS 工具链深度协同,融合中英文核心文献,了解当前发文趋势,作者、机构以及国家合作,探索研究现状和热点,推动构建网络空间命运共同体.

1 研究工具

CiteSpace 与 SciExplorer-LDGAS 作为两款具有一定人工智能技术的科学文献数据分析工具,各自具有鲜明的优势. CiteSpace 擅长处理中英文文献,支持时间序列网络、关键词共现网络、作者合作网络等多维度的可视化呈现,能够直观揭示学科领域的研究热点、前沿演变及合作模式. 其通过直观的可视化图像展示研究内容,并有效探测学科发展的关键路径与前沿趋势. 而 SciExplorer-LDGAS 则注重科技文献数据的治理与统计分析,提供用户友好的操作界面及多样化的可视化选择. 其从施引文献的角度,对对象数据集的科研产出、研究领域以及研究主题等进行探索性分析,以考察数据集所表征的科技情报态势,如时间分布、高产学者分布、高产机构分布、高产国家或地区分布等,实现统计与可视化分析.

两者在数据源、功能及用户友好性上形成互补:CiteSpace 的深度可视化与学科探测能力与 SciExplorer-LDGAS 的数据治理、统计分析便捷性相结合,不仅提升了综合分析能力和工作效率,还为创新研究提供了强有力的支持. 这种结合使得两者在科研实践中能够为用户提供更全面、深入的数据分析结果.

为应对知识图谱技术的快速发展,探索知识图谱在网络安全领域的深入应用,针对知识图谱作为整合工具的系统性研究缺口,本研究通过 CiteSpace 与 SciExplorer-LDGAS 工具链的深度协同,系统性地分析网络安全知识图谱领域的研究现状. 以此识别出网络安全知识图谱领域的关键技术和研究主题,发现不同研究机构和学者以及国家与地区之间的合作网络,关注研究热点关键词的发展变化,为网络安全领域的研究提供全面的视角和深入的洞察,推动构建网络空间命运共同体.

2　数据与方法

2.1　数据采集与处理

本次研究选取中国学术期刊网络出版总库(CNKI)和美国科学情报研究所(Institute for Scientific Information,ISI)的 Web of Science(WoS)数据库作为切入点. 首先对网络安全与知识图谱方面中文关键词和英文关键词进行解析,检索关键词如表 1 所示.

表 1　网络安全与知识图谱相关文献检索关键词

Table 1　Keywords for literature search on cybersecurity and knowledge graphs

	中文	英文
关键词	网络安全 知识图谱 网络空间安全 知识图谱	cybersecurity;knowledge graph cyberspace security;knowledge graph
文献数量	84	289

在 CNKI 数据库中,检索主题为“网络安全 知识图谱”以及“网络空间安全 知识图谱”的文献,筛选北大核心和 CSSCI 的核心期刊,最终得到有效中文文献 84 篇,时间跨度为 2014 年到 2024 年,以“RefWorks”格式作为样本导出. 在 WoS 数据库中选择 Core Collection,检索方法为 TS = “cybersecurity; knowledge graph”OR“cyberspace security;knowledge graph”,分别检索并筛选后,收集到 289 篇英文文献,时间跨度为 2011 年到 2024 年,以纯文本文件格式选择“全记录和引用的参考文献”导出. 检索时间为 2024 年 12 月 17 日,文献数据包括题名、作者、机构、摘要、关键词和发表年份等信息. 通过两个数据库检索到有效文献共计 373 篇. Web of Science 核心合集收集了自然科学、社会科学和艺术等领域的世界一流学术性期刊[11],相对于其他数据库拥有更为权威的、高影响力的学术期刊[12].

以上文献经过 CiteSpace 中 Data 功能进一步筛选、除重,识别得到 84 篇中文论文和 129 篇英文论文. 289 篇英文文献经过 SciExplorer-LDGAS 系统进一步筛选去重,得到 259 篇英文文献,均用于数据分析,文献类型如图 1 所示. 共有 127 篇 article(论文),116 篇 proceedings paper(会议论文)和 15 篇 review(综述论文),其余文献为 early access(提前在线发表)以及 editorial material(编辑材料).

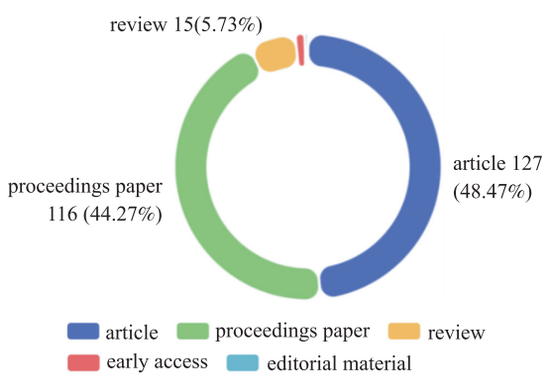


图 1　SciExplorer-LDGAS 对 WoS 259 篇文章划分的文献类型

Fig. 1　Document types of 259 articles in Web of Science(WoS) classified by SciExplorer-LDGAS

2.2　研究方法

为系统分析研究现状,本文采用 CiteSpace 与 SciExplorer-LDGAS 工具链对中英文文献进行量化分析. 分别构建作者、机构、国家合作图谱和关键词共现、关键词聚类、关键词凸显图谱;并采用 SciExplorer-LDGAS 对 WoS 论文进行文献数据分析. 为了将英文文献和中文文献进行融合和对比,将引文翻译成了中文,旨在保证研究的科学性和有效性. 其中,本次研究所选用的分析工具 CiteSpace 是美国德雷赛尔大学陈超美博士开发的引文网络可视化工具,其具备研究领域现状的解释功能与研究领域未来前景的预见功能,直观易用[13]. SciExplorer 科学计量数据可视化分析系统(SciExplorer:Scientometrics Data Analysis and Visualization System)是由中国科学院文献情报中心高层次人才引进项目资助开发的科技文献数据分析平台.

3　研究结果

3.1　研究成果发表趋势

图 2 所示的发文数量趋势图清晰地呈现了 2011 年至 2024 年网络安全知识图谱领域的学术关注度演变. 在 WoS 数据库中,最早的研究产出在 2011 年,Mahoney 等[14]基于语义网技术构建 SCADASiM,一个用于控制系统仿真以及针对网络安全的近实时监管合规性监测的集成框架. CNKI

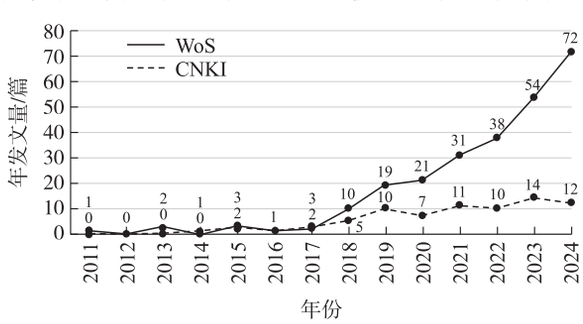


图 2　2011—2024 年研究成果发表趋势图

Fig. 2　Trends in research output publications from 2011 to 2024

数据库显示,2015 年之前,该领域的学术关注度相对较低,以文献计量分析为主,仍处于新兴阶段. 自 2018 年起,发文数量显著增长,贾焰等[15]提出一种构建网络安全知识图谱的实用方法. 这表明学术界对网络安全知识图谱重要性的逐步认可. 王通等[16]进一步研究基于深度学习的威胁情报知识图谱构建技术. 在 2023—2024 年间该领域的出版物达到了峰值,这一增长趋势可以归因于该研究得到了重视、资金的增加以及跨学科合作的增强. 随着大语言模型的不断发展,于丰瑞[17]深入分析基于传统自然语言处理、机器学习和大语言模型三种研究思路,用于网络威胁技战术情报自动化识别提取. 这些因素共同推动了该领域的研究范围拓展和学术影响力的扩大.

3.2 数据分析总览

针对量级较大的英文文献,使用 SciExplorer-LDGAS 对 289 篇论文去重得到 259 篇论文语料并进行数据分析,如图 3 所示. 可见,在 2011 年到 2024 年的英文文献中,来源数量为 192 个,共有 5 种文章类型,论文作者共 896 位,来自 402 个不同的机构,分属 55 个国家或地区;论文中包括了 Web of Science 的 58 个学科分类,包含 35 个研究领域;语料中,作者关键词共 861 个,扩充关键词有 190 个;这 259 篇论文的作者有 64 次跨国合作,共引用文章 2 243 次,即平均每篇 8 份;h-index 是衡量研究者产出的指标,表示有 h 篇论文至少被引用 h 次. 该领域期刊 h-index 为 23,表明领域仍然较新,需加强高质量论文产出,推动标杆性研究.

Timespan	Documents	Sources	Documents type	Authors
2011:2024	259	192	5	896
Institutions	**Countries/Regions**	**Web of Science categories**	**Research areas**	**Author's keywords**
402	55	58	35	861
Keywords plus	**International co-authorships**	**Total citations**	**Average citations per doc**	**h-index**
190	64	2243	8	23

图 3　SciExplorer-LDGAS 英文文献数据总览图

Fig. 3　Overview of English literature data by SciExplorer-LDGAS

3.3 作者合作图谱

作者合作知识图谱(图 4)反映了不同作者之间围绕网络安知识图谱研究做出的贡献和相关性,展示了 WoS 和 CNKI 数据库中的作者对这个话题的贡献,表 2 呈现了作者发文量排名前十. WoS 数据库的作者合作图谱图中有 190 个节点,204 条联系线,网络密度为 0.0114;CNKI 数据库的作者合作图谱图中有 180 个节点,226 条联系线,网络密度为 0.014. 从数据来看,在网络安全知识图谱相关研究中,两个平台发表的文献均未形成相对稳定的合作研究网络.



图 4　中外作者合作图谱对比图

Fig. 4　Comparison of international and domestic author collaboration networks

中文文献的发文作者郭启全、高春东、江东等作者之间的连接线和关节点明显,表明合作频次较高. 董继平等[18]梳理了基于图深度学习的漏洞检测方法,归纳了数据集、图数据、图深度学习模型构建及结果评估 4 个主要阶段. 但从作者图谱聚类上看,关键点总体呈现分散状态,这意味着部分作者之间可能存在较为稳定的合作关系,但是整体合作较少,并且很难突破该研究圈子.

表 2　作者发文量

Table 2　Publication counts by author

WoS 数据库		CNKI 数据库		WoS 数据库		CNKI 数据库	
作者	数量	作者	数量	作者	数量	作者	数量
JOSHI,A	11	LIU,JY	4	刘斌	3	李杰	2
MITTAL,S	10	CONTI,M	3	努尔布力	3	江东	2
FININ,T	9	DENG,YL	3	申国伟	3	邹红霞	2
PIPLAI,A	8	HUANG,C	3	郭启全	3	高春东	2
LIU,H	4	LI,AP	3	张海霞	2	黄智勇	2

外文文献的研究中,Sudip,Finin 等作者存在联系,连接线突出,表明合作发文次数相对较多,他们的合作较为紧密. Mitra 等[19]构建了一个用于捕获情报的溯源信息的系统,并将其与捕获的网络威胁情报(CTI)一同呈现. 对现有的网络安全知识图谱(CKG)模型进行了增强,以纳入情报溯源信息,并将溯源图与 CKG 相融合. 包含 CTI 信息及其溯源的知识图谱能够为依赖的人工智能系统和人类分析师提供专业知识. 整体上 WoS 平台上学者的合作网络相较更加紧密,CNKI 平台上作者尚未呈现相对广泛的合作关系. 因此,本板块的讨论应旨在推动建立网络安全知识图谱研究联盟,建立更加突出和稳定的学术关系,产出更多优质成果.

3.4　机构合作图谱

机构合作图谱通过视觉来展示不同机构之间的合作关系. 在学术或研究环境中,机构合作图谱揭示合作网络、合作强度、合作的范围和领域、合作的地理分布、关键机构、时间动态、合作影响. 机构合作知识图谱是信息可视化和网络分析工具的重要组成部分,帮助研究者、决策者和政策制定者理解和评估合作模式,促进新合作的形成,以及识别潜在的合作机会[20].

从表 3 期刊/会议发文量可见,在 CNKI 数据库中期刊发文量居前三的为:信息网络安全(6 篇)、计算机科学(6 篇)、情报杂志(4 篇). 在 WoS 数据库中,发文量居前三的机构分别是:IEEE Access(16 篇)、Computers & Security(14 篇)、Electronics(9 篇). 网络安全和人工智能领域的会议发文量突出,例如“Collaboration and Internet Computing”与“Intelligence and Security Informatics”等会议均名列前茅.

表 3　期刊/会议刊文量

Table 3　Publication counts by journals and conferences

WoS 数据库		CNKI 数据库	
期刊/会议	数量	期刊	数量
IEEE Access	16	信息网络安全	6
Computers & Security	14	计算机科学	6
Electronics	9	情报杂志	4
Information	5	现代电子技术	4
19th International Conference on Availability,Reliability,and Security(ARES 2024)	4	计算机工程	4
Applied Sciences-Basel	4	小型微型计算机系统	3
IEEE Transactions on Knowledge and Data Engineering	3	科技导报	3
International Journal of Critical Infrastructure Protection	3	计算机工程与应用	3
2018 4th IEEE International Conference on Collaboration and Internet Computing(CIC 2018)	2	计算机研究与发展	3
2020 IEEE International Conference on Intelligence and Security Informatics(ISI 2020)	2	中国安全科学学报	2

图 5 阐述了机构合作共现图谱对比的情况,左侧为 WoS 平台数据,右侧为 CNKI 平台数据. WoS 数据的机构共现图中有 157 个节点,有 113 条连接线,网络密度仅为 0.009 2,表明机构之间的合作较为薄弱. 发文机构以大学为主,部分关节点突出但连接不突出,形成以 University of North Carolina 与 University of Maryland Baltimore County 为中心的结构松散的合作网络.

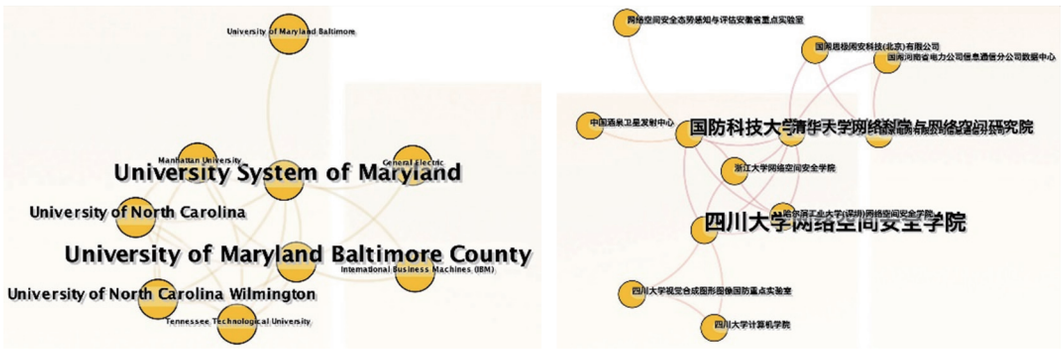


图 5　机构合作图谱对比图

Fig. 5　Comparison of institutional collaboration networks

CNKI 数据的机构共现图谱中共有 143 个节点,136 条连接线,网络密度为 0.0136,机构之间的合作较为稀疏,基本形成较为显著的以四川大学网络空间安全学院与国防科技大学电子对抗学院为核心的合作网络,在网络空间安全领域表现突出,其中王琪凯等[21]设计并实现了一种基于表格填充的关系三元组抽取模型,能够更准确地捕捉句子中的复杂结构和依赖关系. 谢腾等[22]研究基于 BERT-BiLSTM-CRF 模型的中文实体识别,提高了实体识别性能. 其余发文机构以国家电网等公司为主. 从整体来看,CNKI 上形成较为中心的发文机构合作网络,各个机构之间的合作较多,展现出较多的多元性.

3.5　国家与地区分析

针对 WoS 数据库中的 259 篇英文文献,使用 SciExplorer-LDGAS 平台进行国家与地区分析,发文前十国家如表 4 所示. 其中,美国和中国的网络安全知识图谱相关研究数量最多,分别有 70 篇和 65 篇,相差小,发文量为世界领先. 接下来德国有 19 篇论文,澳大利亚 14 篇,意大利和英国皆有 12 篇.

表 4　国家发文量

Table 4　Publication counts by country

国家	数量	国家	数量
United States of America(USA)	70	United Kingdom(UK)	12
People's Republic of China(PRC)	65	Spain	11
Germany	19	France	9
Australia	14	India	8
Italy	12	Netherlands	8

使用 CiteSpace 平台构建国家合作图谱,如图 6 所示,从整体来看,欧美国家对网络安全的研究与相互合作较为突出. 由此可知,世界范围内对网络安全知识图谱的重视度高,国家与地区之间的合作频繁. 在此基础上,各国可考虑建立专门的协调机构,以引领和统筹跨国研究合作,促进研究成果的共享与交流,从



图 6　国家与地区合作图谱

Fig. 6　Collaboration network of countries and regions

而更有效地应对网络威胁和恶意攻击. 这种跨国家、跨领域的合作模式,不仅有助于提升全球网络安全的整体防御能力,还将为构建更加安全、稳定、开放的网络空间提供有力支持.

3.6　关键词共现分析

根据 SciExplorer-LDGAS 的统计,84 篇 CNKI 文献中,关键词出现次数排名前三的是:知识图谱(53 次)、网络安全(28 次)、本体(6 次),其他出现频次高的关键词包括“威胁情报”“态势感知”“知识推理”“人工智能”等. 而在 259 篇 WoS 文献中,cybersecurity(网络安全)出现 89 次,次数最多;接下来 knowledge graph(知识图谱)出现 52 次,cyber threat intelligenc(网络威胁情报)22 次,ontology(本体)16 次. 其他出现频次高的关键词包括“computer security(计算机安全威胁情报)”、“security(安全)”和“artificial intelligence(人工智能)等.

根据 CiteSpace 构建的关键词共现分析图谱如图 7 所示. 可见网络安全知识图谱领域主要以“网络安全”与“知识图谱”作为核心要素. 国内研究主要聚焦于知识图谱构建所涉及的实体识别、本体构建、知识推理、知识融合等内容,以及针对网络攻击的态势感知、漏洞挖掘、威胁情报等内容. 国外研究则侧重于计算机安全、入侵检测、网络安全教育等内容. 同时,本研究通过关键词共现分析发现,中英文文献在网络安全知识图谱研究领域呈现出显著趋同性,具体聚焦于网络威胁情报、本体构建以及人工智能等核心方向. 这一趋势既契合数字时代网络安全防护体系智能化升级的技术需求,也顺应互联网基础设施演进对知识结构化表征的客观要求,进一步推动网络安全知识图谱研究向人工智能驱动型技术架构与场景化应用范式纵深发展.

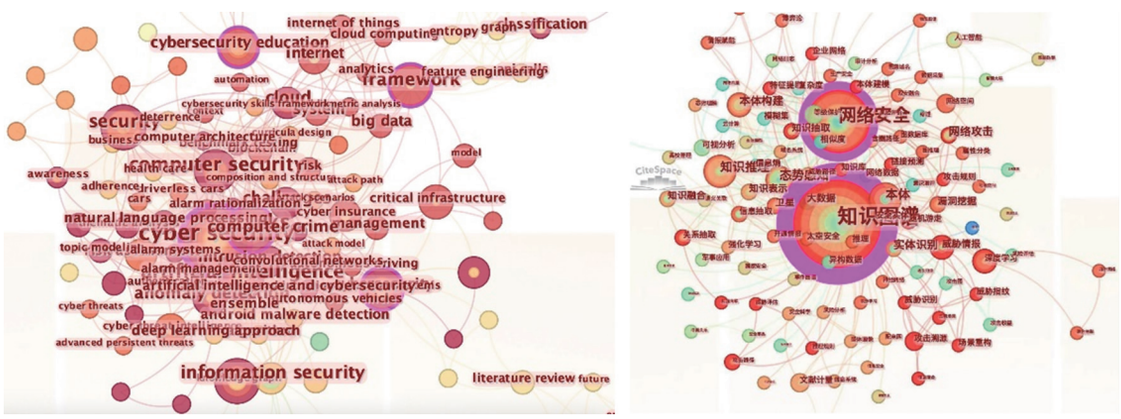


图 7　关键词共现分析对比图

Fig. 7　Comparison of keyword co-occurrence analysis

3.7　关键词聚类分析

基于 Web of Science(WoS)和中国知网(CNKI)的文献数据集,构建关键词聚类知分析对比图,见图 8. CiteSpace 软件的关键词聚类按照相关程度快速聚合,并按照聚类规模大小进行排序[13]. 本次聚类共提取出 14 个核心聚类类别,揭示了该领域当前的主导研究方向与学术关注焦点,其关键词分布特征及语义关联详见表 5,系统探索网络安全与知识图谱领域的关键研究主题及前沿热点.



图 8　关键词聚类知分析对比图

Fig. 8　Comparison of keyword clustering analysis

网络安全知识图谱这一主题涵盖了系统性综述、人工智能、语境应用意义、网络威胁建模框架、网络安全行为、攻击模式、领域、知识图谱构建、知识融合、卫星、属性分类、网络攻击、攻击溯源技术架构等多个方面,不仅涉及对网络安全技术、策略、法规的深度理解,也囊括了对新兴威胁、数据泄露、用户教育等议题的关注与讨论. 聚焦于网络安全知识图谱的技术基础,包括如何构建高效的知识图谱、选择合适的图数据库,以及如何利用人工智能和自动化工具来提升网络安全防护的效率和准确性.

CNKI 获得的中文论文的关键词聚类主要分为知识图谱构建与攻击溯源两大类. 属性分类与知识融合都是知识图谱构建聚类的核心议题,涵盖了网络安全、模糊集、本体模型等多个方面,在知识图谱实体识别、网络安全威胁情报分析[23]、网络攻击模式预测[24]等方向不断突破. 周锦等[25]将双向长短时记忆网络-条件随机场(BiLSTM-CRF)训练模型作为实体识别的方法引入网络安全知识图谱领域,其实体识别准确率达到较高水平,预测准确率达到 96.70%. 随着知识融合技术的发展,知识图谱可以将不同来源、不同格式的知识进行有效整合和利用,提高知识的质量和价值. 该聚类强调了对知识的深度挖掘和整合能力的重要性,以及通过技术手段实现知识的自动化融合和智能应用的可能性.

网络攻击与攻击溯源是应对网络攻击的热点议题,包括网络威胁建模框架的构建和对网络攻击的溯源研究. 该聚类强调了对关键基础设施的保护和对网络攻击行为的预防和应对能力,为网络安全防护提供了重要的指导和建议. 通过深入分析网络攻击的数据和特征,该类研究为网络安全事件的应急响应和调查提供了科学依据和有效策略. 罗养霞等[26]提出通过 NER 模型去抽取恶意软件名称、发现地等文本实体信息,以此构建恶意软件知识图谱,并通过知识图谱发现其多样性、演化路径、威胁方式与分类关联等,对推进网络安全知识简易化和防御体系知识普及化具有重要意义. 张玉臣等[27]针对攻击威胁特征识别难的问题,提出了知识图谱驱动的网络攻击溯源方法,以脆弱性利用动作为核心构建攻击事件框架,并以事件为单位实施告警关联,重构攻击场景. 在此基础上,利用威胁指纹知识图谱,整合已公开的威胁情报知识,并抽取攻击场景中的威胁特征作为指纹,分析两者相似性,溯源攻击者. 通过对网络攻击行为的溯源分析,可以根据网络攻击的数据和特征,增强对关键基础设施的保护和对网络攻击行为的预防和应对能力. 赖清楠等[23]设计了一个基于大语言模型的网络威胁情报知识图谱构建框架 AutoCTI2KG,通过指令提示和上下文学习,自动从网络威胁情报中生成网络安全知识图谱和攻击知识图谱,并提供可操作的防护建议. 实验结果表明,所提出的框架在网络安全知识图谱和攻击知识图谱构建方面表现出色,F1 值在 0.90 左右,展示了大语言模型在网络安全领域知识图谱构建的潜力,并为网络安全事件的应急响应和调查提供科学依据和有效策略.

WoS 获得的英文文献主要关注以下几个议题:系统性综述与基础方法论,人工智能驱动的安全分析,语境应用与教育实践,用户行为与安全策略等. 系统性综述与基础方法论侧重于对网络安全知识图谱领域的知识体系梳理和研究方法的优化,通过文献计量工具分析研究趋势和学术合作网络. 人工智能驱动的安全分析结合深度学习和知识图谱技术,开发自动化威胁检测框架,提升复杂攻击场景下的识别效率. 语境应用与教育实践探索知识图谱在安全教育培训中的应用,构建交互式学习系统以提升从业人员技能. 网络威胁建模与风险评估基于攻击图建模关键基础设施威胁路径,量化风险等级并制定防御策略. Sills 等[28]应对物联网(IoT)设备在医疗环境中的应用引入了日益增长的安全漏洞和威胁清单. 通过扩充情报存储库,与先前研究中的网络安全知识图谱(CKG)中的威胁情报相结合. 扩充后的图嵌入在查询相关信息以及各种 AI 辅助网络安全任务中具有重要作用. 扩充后的 CKG 产生了更高质量的图表示. 在信息检索任务中计算得出,扩充后的 CKG 使平均精度均值(MAP)提高了 31%. Nour 等[29]提出一种名为 AUTOMA 的解决方案,通过知识发现自动化生成相关假设及其变体,AUTOMA 能够生成相关假设(前 3 位),并实现大幅的假设数量缩减(最高达 99%),同时具备快速执行能力(生成相关假设耗时最多 8 分钟,生成变体仅需 10 s).

国内研究侧重技术层面,专注创新性技术的开发,强调技术的深度和广度. 例如知识图谱的构建过程中的知识融合、属性分类技术,通过知识融合技术整合不同来源的知识,以及通过攻击溯源技术深入分析攻击行为. 国外研究侧重应用层面,强调与其他技术的结合,强调多方面的应用和优化,例如知识图谱在安全教育培训中的应用、基于知识图谱的内部威胁检测系统等. 强调与其他技术的结合,例如人工智能、深度学习、自然语言处理等技术在网络安全知识图谱中的应用. 更侧重于技术的应用层面,涵盖了从系统

性综述到用户行为分析等多个方向,强调技术的实用性和与其他技术的结合.

表 5　网络安全知识图谱关键词聚类分析

Table 5　Keyword clustering analysis of cybersecurity knowledge graphs

聚类序号	聚类名称	关键词
0	Systematic Review(系统性综述)	Bibliometrics(文献计量)、Information Retrieval(信息检索)
1	Artificial Intelligence(人工智能)	Anomaly Detection(异常检测)、Knowledge Graph(知识图谱)、Framework(框架)
2	Context Application Benefit(语境应用意义)	Information Security(信息安全)、Literature Review(文献综述)、Cybersecurity Education(网络安全教育)
3	Cybersecurity Behavior(网络安全行为)	Cybersecurity(网络安全)、Behavior(行为)
4	Attack Pattern(攻击模式)	Attack Pattern(攻击模式)、Critical Infrastructure(关键基础设施)
5	Field(领域)	Classification(分类)、Generation(生成)
6	知识图谱构建	网络安全,模糊集,本体模型,政治安全,实体分类,文本分类,数据采集,风险评价,网络空间
7	知识融合	信息抽取,知识融合,语义关联,强化学习,开源情报,知识表示,共指消解,情报赋能,关系抽取,知识推理,本体构建
8	卫星	网络流量,可视化分析,推理,态势感知,本体,态势理解,威胁路径,卫星,太空安全知识库推理,语义约束
9	属性分类	云计算,网络数据,图数据库,异构数据,漏洞挖掘,大数据,深度学习,实体识别
10	网络攻击	智慧大脑,人工智能,链接预测,网络防御,攻击规则,随机游走,网络攻击,表示学习
11	攻击溯源	攻击溯源,场景重构,威胁指纹,神经网络,威胁情报
12	网络安全	文献计量,风险分析,攻击路径,安全科学,信息系统,威胁评估,整体画像,推理规划

3.8　关键词凸现分析

表 6 展示了 2011 年至 2024 年,来源于 WoS 和 CNKI 的网络安全知识图谱相关的凸现分析结果,旨在揭示该时期内学术研究的焦点变化与发展趋势. 强度反映了关键词在特定时间段内的学术关注程度或引用频率的增加速度. 数值越高,表明该关键词在研究领域内越受到重视,其相关研究成果可能在学术或实践中产生较大影响. 凸现期表示关键词凸现的时间范围,即关键词开始受到广泛关注到关注度开始下降的时间段. 这段时间内,相关研究的兴起与发展最为活跃,体现了学术界对某一议题兴趣的集中表现.

在网络安全知识图谱领域,研究热点随着时代发展与需求转换而演进,经历了从信息安全、网络安全、态势感知、可视分析、大数据向人工智能、知识图谱构建以及网络安全教育的变化. 计算机犯罪、网络攻击的强度较高,指出了信息技术进步带来的新形式犯罪行为. 随着网络技术和金融科技的发展,网络安全威胁的持续存在,网络攻击手段持续智能化演进,如何有效解决多源异构数据因信息格式差异大、数据特征属性多所造成的数据存储和融合困难等问题成为新课题[30]. 知识图谱构建技术(如知识推理、知识融合、本体构建、知识表示等)的强度突出,且在近五年不断凸显,可见建立统一描述的网络安全态势要素知识图谱的需求庞大.

表 6　网络安全知识图谱的关键词凸现分析

Table 6　Keyword salience analysis of cybersecurity knowledge graphs

关键词	强度	出现年份	开始年份	结束年份	凸现期
生态安全	1.35	2014	2014	2015	2014—2015
信息安全	1.24	2015	2015	2016	2015—2016
网络安全	0.37	2017	2017	2018	2017—2018
态势感知	0.99	2018	2020	2021	2020—2021
可视分析	1.19	2018	2018	2020	2018—2020
大数据	1.01	2018	2018	2019	2018—2019
安全	1.58	2018	2021	2022	2021—2022
计算机犯罪	0.96	2020	2020	2021	2020—2021
批判性思维	0.68	2020	2020	2022	2020—2022
知识推理	1.12	2020	2020	2022	2020—2022
人工智能	0.95	2020	2020	2021	2020—2021
网络攻击	0.73	2020	2020	2021	2020—2021
知识融合	0.6	2020	2020	2022	2020—2022
研究热点	0.72	2019	2019	2021	2019—2021

续表 6

Table 6 continued

关键词	强度	出现年份	开始年份	结束年份	凸现期
网络安全教育	0.79	2018	2021	2024	2021—2024
文献计量	1.23	2021	2021	2022	2021—2022
本体构建	0.94	2021	2021	2022	2021—2022
知识表示	0.81	2021	2021	2022	2021—2022
深度学习	0.7	2022	2022	2024	2022—2024
卫星	0.63	2022	2022	2024	2022—2024
漏洞挖掘	0.63	2022	2022	2024	2022—2024
本体	0.5	2019	2022	2024	2022—2024

4 结论

本文梳理分析了网络安全知识图谱领域研究,基于 CiteSpace 构建了作者、机构、关键词共现、关键词凸显、关键词聚类图谱;并采用 SciExplorer-LDGAS 对 WoS 论文进行文献数据分析与国别研究.

研究结果表明该领域发文量自 2017 年起显著增长,2023—2024 年达到峰值,反映学术关注度与跨学科合作的增强. 发文数量趋势研究显示,网络安全知识图谱将持续作为研究热点. 随着互联网的普及,网络安全不断受到重视. 知识图谱作为新型工具,其作用不断凸显:在系统整合方面,网络攻击知识图谱具有全面性和结构化优势;在信息共享方面,网络攻击知识图谱具有全球化优势,有利于促进国际合作. 在处理威胁情报、进行攻击溯源方面,网络安全知识图谱具有巨大潜力和运算能力.

研究文献经过可视化表明,作者与机构合作呈现区域性聚集特征,中美两国研究贡献领先,但跨国合作网络稀疏,跨国、跨领域的作者、机构乃至国家或地区之间的合作有待加强. 总体上看,国内外普遍的情况是部分作者之间存在较为稳定的合作关系,但是整体合作较少,并且很难突破该研究领域;以及不同机构之间的合作稀疏,缺少多元性,没有形成中心机构起领头作用;尽管世界范围内对网络安全的重视度高,但跨国、板块的合作比较稀少.

根据关键词共现、聚类、凸显分析,国内外研究呈现侧重差异:国内聚焦技术突破,国外则侧重应用优化;这些研究方向共同涵盖了知识图谱构建与攻击溯源的核心议题,强调了技术的创新性和实用性,为网络安全领域的研究和实践提供了重要的指导和参考. 研究热点从早期“态势感知”“可视分析”向“知识图谱构建”“攻击模式预测”演进,凸显技术驱动的防御体系升级需求.

基于此,本文提出需加强跨国、跨机构协作,建立统一的知识共享平台,推动知识图谱技术与多源威胁情报的深度整合,为构建网络空间命运共同体提供理论与工具支撑. 网络空间是人类共同的活动空间,网络空间前途命运应由世界各国共同掌握. 各国应当加强合作,互联互通,共同探讨世界互联网技术的发展方向,推动互联网全球治理体系的变革,加快建设网络社会,进一步建立网络安全知识图谱研究联盟,建立更加突出和稳定的学术关系,产出更多优质成果,共同探讨世界互联网技术的发展方向,推动互联网全球治理体系的变革,加快建设网络社会,构建网络空间命运共同体.

[参考文献]

[1] 习近平:没有网络安全就没有国家安全[EB/OL]. (2021-10-10)[2025-1-9]. http://www.qstheory.cn/zhuanqu/2021-10/10/c_1127943608.htm.

[2] SOMMER R, PAXSON V. Outside the closed world: on using machine learning for network intrusion detection[C]//2010 IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE, 2010: 305-316.

[3] LI H, SHI Z, PAN C, et al. Cybersecurity knowledge graphs construction and quality assessment[J]. Complex Intelligent systems, 2024(10): 1201-1217.

[4] 丁兆云,刘凯,刘斌,等. 网络安全知识图谱研究综述[J]. 华中科技大学学报(自然科学版),2021,49(7):79-91.

[5] 邢家绵,边晶,康静雨,等. 国内外网络安全评估研究的热点及趋势——基于 CiteSpace 的知识图谱可视化分析[J]. 电脑知识与技术,2022,18(20):37-40.

[6] 肖婉,张舒予. 国外网络欺凌研究热点与实践对策——基于 CiteSpace 知识图谱软件的量化分析[J]. 比较教育研究,2016,38(4):66-72.
[7] 李杰,蔡彬清,许璐. 基于 CiteSpace 的我国网络空间安全研究态势分析[J]. 福建工程学院学报,2018,16(2):174-178.
[8] 马超,陈亚丽. 基于 CiteSpace 和 Vosviewer 的国内外网络治理研究的可视化分析[J]. 西南民族大学学报(人文社会科学版),2021,42(8):229-240.
[9] 林玲,陈福集. 基于 CiteSpace 的国内网络舆情研究知识图谱分析[J]. 情报科学,2017,35(2):119-125.
[10] 张宁,盛武. 基于 CiteSpace 的大数据时代信息安全研究现状[J]. 华北水利水电大学学报(社会科学版),2018,34(3):156-160.
[11] 陈琴,蒋合领. 基于 WoS 核心合集的国际智库研究可视化分析[J]. 情报资料工作,2016(1):68-73.
[12] 董淑龙,马姜明,辛文杰. 景观视觉评价研究进展与趋势——基于 CiteSpace 的知识图谱分析[J]. 广西师范大学学报(自然科学版),2023,41(5):1-13.
[13] 何静,冯元柳,邵靖雯. 基于 CiteSpace 的多源数据融合研究进展[J]. 广西师范大学学报(自然科学版),2024,42(5):13-27.
[14] MAHONEY W,GANDHI R A. An integrated framework for control system simulation and regulatory compliance monitoring[J]. International Journal of Critical Infrastructure Protection,2011(4(1)):41-53.
[15] 贾焰,亓玉璐,尚怀军,等. 一种构建网络安全知识图谱的实用方法[J]. Engineering,2018,4(1):117-133.
[16] 王通,艾中良,张先国. 基于深度学习的威胁情报知识图谱构建技术[J]. 计算机与现代化,2018,(12):21-26.
[17] 于丰瑞. 网络威胁技战术情报自动化识别提取研究综述[J]. 计算机工程与应用,2024,60(13):1-22.
[18] 董继平,郭启全,高春东,等. 基于图深度学习的漏洞检测[J]. 科技导报,2023,41(13):41-59.
[19] MITRA S,PIPLAI A,MITTAL S,et al. Combating fake cyber threat intelligence using provenance in cybersecurity knowledge graphs[C]//2021 IEEE International Conference on Big Data(Big Data). Piscataway,NJ,USA:IEEE,2021:3316-3323.
[20] 安宁,安璐. 跨平台网络舆情知识图谱构建及对比分析[J]. 情报科学,2022,40(3):159-165.
[21] 王琪凯,刘孙俊,何俊江,等. 基于表格填充的网络威胁情报关系三元组抽取[J]. 微电子学与计算机,2025,42(7):82-92.
[22] 谢腾,杨俊安,刘辉. 基于 BERT-BiLSTM-CRF 模型的中文实体识别[J]. 计算机系统应用,2020,29(7):48-55.
[23] 赖清楠,金建栋,周昌令. 基于大语言模型的网络威胁情报知识图谱构建技术研究[J]. 通信学报,2024,45(S2):33-43.
[24] 黄智勇,刘昕宇,林仁明,等. 基于知识图谱的网络攻击预测方法研究及应用[J]. 现代电子技术,2024,47(9):91-96.
[25] 周锦,薛钰,杨秉杰,等. 基于深度学习 BiLSTM-CRF 模型的网络安全知识图谱实体识别方法[J]. 网络安全技术与应用,2024,(9):41-44.
[26] 罗养霞,李浩,武晨明. 恶意软件知识图谱的构建与研究[J]. 计算机工程与科学,2025,47(1):86-94.
[27] 张玉臣,孙澄,姜迎畅,等. 融合威胁情报与知识图谱的网络攻击溯源方法[J]. 情报杂志,2024,43(8):72-83,91.
[28] SILLS M,RANADE P,MITTAL S. Cybersecurity threat intelligence augmentation and embedding improvement:a healthcare usecase[C]//2020 IEEE International Conference on Intelligence and Security Informatics(ISI). Arlington,VA,USA:IEEE,2020:1-6.
[29] NOUR B,POURZANDI M,QURESHI R K,et al. AUTOMA:automated generation of attack hypotheses and their variants for threat hunting using knowledge discovery[C]//IEEE Transactions on Network and Service Management. Piscataway,NJ,USA:IEEE,2024,21(5):5178-5196.
[30] 司成,张红旗,汪永伟,等. 基于本体的网络安全态势要素知识库模型研究[J]. 计算机科学,2015,42(5):173-177.

[责任编辑:杜忆忱]