Management Science and Engineering 管理科学与工程, 2025, 14(6), 1012-1019
Published Online November 2025 in Hans. https://www.hanspub.org/journal/mse
https://doi.org/10.12677/mse.2025.146118

Hans汉斯

面向应急响应决策支持的网络安全事理图谱检索机制研究

魏红芹，杨希晨

东华大学旭日工商管理学院，上海

收稿日期：2025年9月20日；录用日期：2025年10月10日；发布日期：2025年10月22日

摘　要

传统网络安全应急决策主要依赖于安全管理人员个人经验积累，缺乏必要系统的知识支撑，难以应对复杂的网络安全新形势。事理图谱技术的引入可以在应急响应各阶段提供更高效决策支持。本文针对事理图谱中的事件检索机制进行研究，在网络安全事件知识表示建模的基础上，采用BERT-wwm-ext模型进行事件要素的向量化语义处理，并提出将余弦相似度计算和动态规划相结合的方法进行事件相似度计算，实现了高关联事件的快速准确检出。研究还结合PDCERF应急响应流程提出了基于事理图谱的网络安全响应决策支持应用框架。本文研究成果对于事理图谱技术在网络安全领域的应用提供了基本思路和实现方法。

关键词

事理图谱，事件检索，网络安全，应急响应，决策支持

Research on Retrieval Mechanism of Cybersecurity Event Evolutionary Graph for Emergency Response Decision Support

Hongqin Wei, Xichen Yang

Glorious Sun School of Business and Management, Donghua University, Shanghai

Received: September 20, 2025; accepted: October 10, 2025; published: October 22, 2025

Abstract

Traditional cybersecurity emergency decision-making primarily relies on the accumulated personal experience of security personnel, lacking systematic knowledge support, which makes it difficult to

文章引用: 魏红芹, 杨希晨. 面向应急响应决策支持的网络安全事理图谱检索机制研究[J]. 管理科学与工程, 2025, 14(6): 1012-1019. DOI: 10.12677/mse.2025.146118

cope with the complex new cybersecurity landscape. Event evolutionary graph technology can provide more efficient decision support at various stages of emergency response. This paper focuses on the event retrieval mechanism in the event evolutionary graph. Based on the knowledge representation modeling of cybersecurity incidents, the BERT-wwm-ext model is employed for vectorized semantic processing of event elements. Additionally, a method combining cosine similarity calculation and dynamic programming is proposed for event similarity computation, enabling rapid and accurate detection of highly correlated events. The paper also presents a decision support application framework for cybersecurity response, aligned with the PDCERF emergency response process. This paper provides fundamental ideas and implementation methods for applying event evolutionary graph technology in the cybersecurity domain.

Keywords

Event Evolutionary Graph, Event Retrieval, Cybersecurity, Emergency Response, Decision Support

1. 引言

随着数智化建设的不断推进，互联网成为社会经济发展高度依赖的核心基础设施之一，网络安全重要性日益突显。与此同时，AI 和大数据技术的发展也催生了各种新型攻击方式，安全事件发生频率和复杂度的不断上升对网络安全治理带来了新的挑战[1]。传统网络应急响应方法在应对网络安全新形势时，暴露出反应不及时、响应措施有效性低等问题，迫切需要引入更有效的辅助响应决策支持技术[2] [3]。

知识图谱通过实体、概念及其关系等基本要素结构化描述领域知识，并以图形进行表示，可以为各类应用中的语义检索和逻辑推理需求提供支持，得到了网络安全领域研究者的关注[4]-[6]。事件知识图谱和事理图谱是知识图谱的两种重要延伸类型[7]，前者以图状结构组织事件及其属性关联关系，实现了离散事件的知识表示。后者则以事件知识图谱为基础，补充事件间的顺承、因果、条件和互斥等内在关系，通过结构化表达存储历史事件的发展脉络和内在逻辑，为态势分析和预测提供有价值的参考信息[8]。网络安全领域存在海量历史事件，利用事理图谱技术结构化存储这些信息，在应急响应中快速检索出历史相似或关联事件信息，对于实现及时准确的时态研判和响应行为具有重要意义。

当前对于事理谱图的研究还处于相对初步阶段，虽然已经有部分关于事理图谱构建方法和应用方向的探索，但对于事件表达、关系抽取、推理机制等方面的研究还不够成熟[9] [10]。特别是对于事理图谱在网络安全领域的应用研究还比较缺乏，有待进一步探索基于事理图谱的应急响应决策支持机制。在决策推理分析中，相关事件的检索速度和准确性直接影响后续决策支持的及时性和有效性，是关键技术之一。本文主要针对网络安全事理图谱的事件检索技术展开研究。

2. 网络安全事理图谱表示模型

2.1. 网络安全事件本体知识模型

本体是一种基于概念之间的语义关系，结构化描述领域知识的一种知识建模方法。本体表示模型可以在信息抽取前确定本体的组成要素、要素角色、实体关系等要素信息[11] [12]，构建网络安全事件本体知识模型利于结构化地梳理网络安全事件的知识构成。

基于《GB/T 20986-2023 信息安全技术网络安全事件分类分级指南》[13]，网络安全事件可分为恶意程序事件、网络攻击事件等 10 类，本文在构建网络安全事件本体知识模型中参考了该指南的分类标准。由于恶意程序和网络漏洞是网络攻击事件中攻击者常用的两种攻击手段，因此本文将恶意程序事件和安全隐患事件并入到网络攻击事件之中并将网络安全事件划分为七个类别。网络安全事件类型划分如图 1 所示。

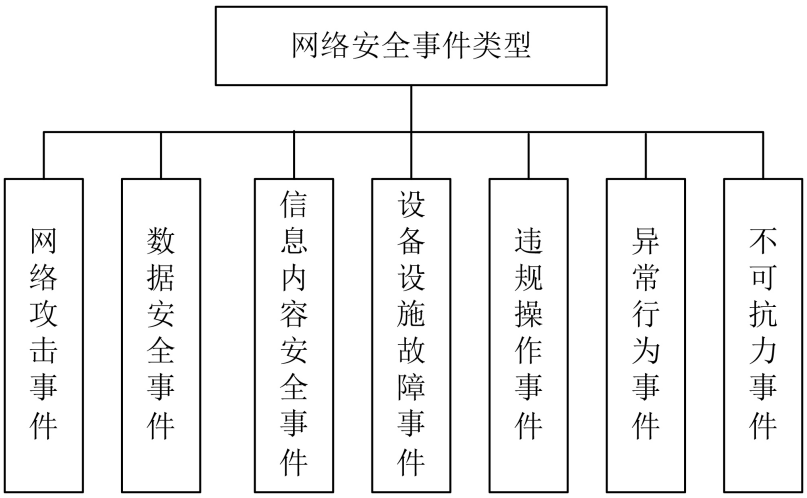

Figure 1. Types of cybersecurity event
图 1. 网络安全事件类型

不同类型的安全事件包含要素不同，其知识表示模型也不同。其中，网络攻击是网络安全事件中最为常见的一种，主要指使用恶意软件、利用漏洞等技术手段对目标网络节点实施主动攻击以达到特定目的的行为。下面以网络攻击事件为例说明事件知识表示模型。

本文将网络攻击事件表示为六元组，包含时间、主体、客体、行动、影响和措施六个元素，可以表示为 case = (Name, Time, Subject, Object, Action, Impact, Measure)。其中，name 是事件的名称；time 是指事件发生的具体时间；subject 是指攻击的发起方或实施方；object 是指攻击的承受方或受影响方；action 是指攻击方在事件中做出的具体行为，impact 是指事件造成的后果，事件的影响可以包括多个层次；measure 则是客体面对该事件时采取的解决方案。表 1 所示为网络攻击事件的表示实例。

Table 1. A example of cybersecurity event case
表 1. 网络攻击事件表示实例

Name	Target 数据泄露事件
Time	2013 年
Subject	攻击者
Object	Target 公司
Action	入侵第三方供应商；通过社交工程获取供应商网络访问权限；渗透内部网络；在支付系统植入恶意软件；窃取敏感数据
Impact	泄露顾客信用卡信息；财物损失；面临客户信任危机
Measure	向受影响客户提供信用监控服务；更换高层管理人员；升级支付系统；引入双因素认证

2.2. 网络安全事理图谱结构模型

事理图谱基本构成包括事件知识和事件间关系信息，可表示为三元组：事件、关系、事件。所有网络安全事件和关系总和形成完整网络安全事理图谱[14]，其结构示意图如图 2 所示。

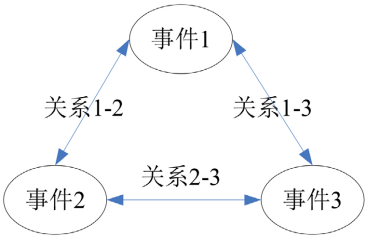

Figure 2. Cybersecurity event evolutionary graph structure diagram
图 2. 网络安全事理图谱结构示意图

网络安全事件之间的关系包含顺承、因果、条件、上下级、互斥、独立等情况。除了独立关系中两个事件互不影响，其他五种关系中均会在事理图谱中形成事件链接，表达事件的演化路径和内在发展逻辑。事理图谱知识中同时存储事件本身的知识信息和事件之间的关系所属类型。

3. 事理图谱检索机制

基于事理图谱的网络安全应急响应中，需要依据已获取的当前安全事件部分信息和决策需求快速检索出有参考价值的历史事件数据集、关联事件、事件演化数据等。为了提高检索匹配准确度，本文基于 BERT 模型进行特征向量抽取，并依据相似度计算结果进行事件匹配。

3.1. 基于 BERT 的事件语义向量化

基于网络安全事理图谱进行事件检索时，首先需要对网络安全事件要素的文本内容进行语义处理，以便提取其特征向量，从而有效捕捉到事件文本之间的潜在关联与语义相似性，为后文匹配当前潜在威胁与历史数据中的相似事件，进而辅助推理可能的应对措施提供依据。

BERT 模型作为一种双向语言处理模型，能够利用语句中的上下文信息来提高文本表示能力[15]。本研究采用哈工大讯飞联合实验室发布的 BERT-wwm-ext 模型对文本进行嵌入表示。BERT-wwm-ext 是一种基于 BERT 结构的中文预训练语言模型。该模型通过大规模中文语料的预训练，在捕捉到中文文本的上下文关系和深层语义信息中具有更高的准确性。通过在预训练过程中对整个词而非单个字进行掩码，在一定程度上克服了中文分词时可能产生的语义断裂问题，能更好地保留中文语言使用中的词语用法和语义信息[16] [17]。通过使用 BERT-wwm-ext 模型，可以将网络安全事件元组的文本信息转化为语义向量，便于后续的结构化存储和推理分析。

本文使用 BERT-wwm-ext 模型对网络安全事件案例要素进行语义表示转换的流程如图 3 所示。该图以 Target 公司遭受网络攻击事件为例，首先将网络安全事件库中的要素短语[14]输入到 BERT-wwm-ext 模型中，通过深度学习对短语进行编码处理，最后获得对应的高维语义向量表示。基于 BERT-wwm-ext 模型的语义表达将作为后续相似度计算的输入，为网络安全事件检索提供语义基础。

3.2. 事件相似度计算

网络安全事件检索的目的是在事件库中查找与当前网络安全状态最相关的事件或事件集。通过计算事件之间的相似度，可以准确了解各个事件之间的相关性。事件的综合相似度基于各个要素的相似度计算完成。

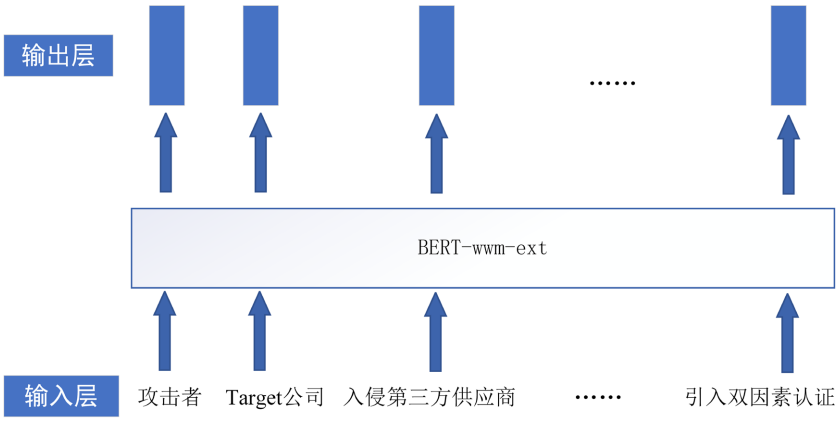

Figure 3. Semantic representation of BERT model
图 3. BERT 模型的语义表示示意图

依据前文对网络安全事件的要素构成设定，网络安全事件可以表示为 case = (Name, Time, Subject, Object, Action, Impact, Measure)。由于本文的研究目的是基于相似事件案例的解决措施为当前潜在的网络安全风险提供可使用的解决措施，即措施要素是相似度计算后需要提供的结果，因此本研究在语义相似度匹配中主要采用时间、主体、客体、行动和影响五个要素。同时，考虑到网络安全事件发生具有突发性的特点且网络安全事件时间往往存在较大差异，对事件解决措施的参考价值较低，因此本研究在计算相似度时降低时间要素的权重。这使得相似度计算能够更精准地捕捉事件的核心特征，将关注点集中在事件执行者、受影响对象、具体行为模式以及可能带来的后果上，从而提高匹配结果的实用性。

在事件检索中，首先使用 BERT-wwm-ext 模型对要素进行向量化处理，获取对应的语义表达。以案例 A 和案例 B 为例，定义其要素向量为 $E_A=(X_1,X_2,\cdots,X_n)$ 和 $E_B=(Y_1,Y_2,\cdots,Y_n)$ 其总体相似度算法如公式(1)所示。

$$sim(A,B)=\sum_{i=1}^{n} w_i\left(sim(X_i,Y_i)\right) \tag{1}$$

其中，$sim(A,B)$ 表示案例 A 和案例 B 的相似度，$sim(X_i,Y_i)$ 表示案例 A 和案例 B 在第 i 个要素上的相似度，w_i 表示不同要素的权重。根据要素的重要程度分配权重以获取总的案例相似度输出措施。

在时间、主体、客体和影响要素层面，由于这些要素多为单一数据，相似度匹配较为简单，因此本文采用余弦相似度计算的方法来衡量要素之间的距离。余弦相似度计算如公式(2)所示。通过计算余弦相似度能够快速评估要素的相似性进行案例检索。

$$\cos(\theta)=\frac{\sum_{i=1}^{n}(X_i\times Y_i)}{\sqrt{\sum_{i=1}^{n}(X_i)^2}+\sqrt{\sum_{i=1}^{n}(Y_i)^2}} \tag{2}$$

而行动要素基于事理图谱的事件链形式，通常表现为长短不一的序列。行动的事件链能够展现网络安全事件发生时主体采取的行动顺序。案例行动的相似度越高，意味着其演化路径越相似，从而能为决策响应支持提供更具价值的参考。在传统的语句相似度计算方法中，通常使用向量表示并计算平均相似度，这种方法仅仅考虑了文本中词汇的相似性，而忽略了事件链存在的先后顺序及其演化过程。为了更好地保留行动顺序并选取与当前事件相似度高的事件链以提供决策支持，本文采取动态规划算法来计算行动中的最长公共子序列，并基于此进行相似度计算。

动态规划是一种将复杂问题分解为多个子问题来避免重复计算的优化方法。使用动态规划可以有效查找事件链最长公共子序列并进行相似度计算。在计算行动要素的事件链时，输入两个案例的行动要素。

假设存在案例 1 的行动事件链为 C，案例 2 的行动事件链 D，其状态转移方程如公式(3)所示

$$dp[i][j]=\begin{cases}dp[i-1][j-1]+1, C[i]=D[j]\\ \max\left(dp[i-1][j], dp[i][j-1]\right), C[i]\neq D[j]\end{cases} \tag{3}$$

其中 $dp[i][j]$表示事件链 C 的前 i 个事件与事件链 D 的前 j 个事件的最长公共子链长度。以事件链[“黑客攻击”“窃取敏感数据”]和事件链[“黑客攻击”“获取网络访问权限”“窃取敏感数据”]为例，其具有[“黑客攻击”“窃取敏感数据”]公共子序列，事件链相似度为 66.7%。

在事件检索过程中，当前事件案例主要通过态势感知获取。在网络安全态势感知在获取当前态势感知结果后，首先提取已知的当前网络安全事件信息及态势预测结果，并将其整理成网络安全事件案例的格式，然后进行事件检索。具体的网络安全事件案例检索算法步骤如图 4 所示。首先输入当前案例和案例库中的某一案例，通过使用 BERT-wwm-ext 模型分别对两个案例的要素进行向量化。在向量化的基础上，使用余弦相似度计算 time，subject，object 和 impact 四个要素的相似度值，并使用动态规划算法计算 action 要素的相似度。通过加权综合方法计算当前案例与案例 i 的总体相似度。通过重复上述相似度计算步骤，完成当前案例和案例库中所有案例的相似度计算，最终得到案例检索结果，为当前案例提供决策参考。

算法　网络安全案例检索算法流程

输入：当前案例和案例库中案例 i 的要素，即< *name, time, subject, object, action, impact, measure* >

输出：与目标案例最相似的前 n 个案例

1：使用 BERT-wwm-ext 模型获取当前案例和案例 i 的要素特征向量

2：使用余弦相似度计算案例间 *time, subject, object* 和 *impact* 要素的相似度

3：使用动态规划计算案例间 *action* 要素的相似度

4：计算当前案例与案例 i 的总体相似度

5：重复上述步骤，完成当前案例和案例库中所有案例的相似度

6：得到案例检索结果

Figure 4. Event case retrieval algorithm flow
图 4. 事件案例检索算法流程

为验证事件检索在响应支持中的可行性，本文使用网络安全事件实例进行验证研究。从事件案例库中选取 5 个事件案例，其具体信息如表 2 所示。将现有事件案例“2023 攻击者公司 F 发送大量数据网络服务延时”按照检索算法流程进行事件案例匹配。经过相似度计算，目标事件与第五个事件案例的相似度最高，相似度为 75.5%，因此在决策过程中可参考该事件的措施。

Table 2. Cybersecurity event case matching
表 2. 网络安全事件案例匹配

Time	Subject	Object	Action	Impact	Measure
2013	攻击者	公司 A	获取网络访问权限 → 渗透内部网络 → 植入恶意软件 → 窃取敏感数据	泄露用户信息；经济损失；	赔付客户；升级系统；引入双因素认证
2022	攻击者	公司 B	利用漏洞 → 获取权限 → 窃取数据	泄露用户信息	修复漏洞；加强防入侵检测
2016	攻击者	公司 C	攻击者冒充管理人员 → 向员工发电子邮件 → 要求转账	经济损失	更新安全技术；加强内部培训；

续表

2016	攻击者	公司 D	利用漏洞 → 传播病毒 → 实施勒索	数据丢失； 经济损失	定期备份； 加强防火墙
2021	攻击者	公司 E	使用恶意软件感染设备 → 发送大量数据	服务无法使用； 系统崩溃	加强防火墙； 加强 DDoS 防护

4. 基于事理图谱检索和推理的网络安全应急响应决策支持机制

基于事理图谱的网络安全应急响应决策支持以经典 PDCERF 应急响应框架[18]为核心，在准备、检测、抑制、根除、恢复和跟踪六个阶段通过从事理图谱中获取相关历史事件信息，为判断推理和决策方案制定提供帮助。在准备、检测和抑制阶段引入态势感知模块实时监控网络环境并预判网络安全事件带来的潜在影响，在恢复和根除阶段引入事件检索与响应支持来匹配相似事件案例及解决措施，从而为应急响应的各个阶段提供全面决策支持。具体方法流程如图 5 所示。

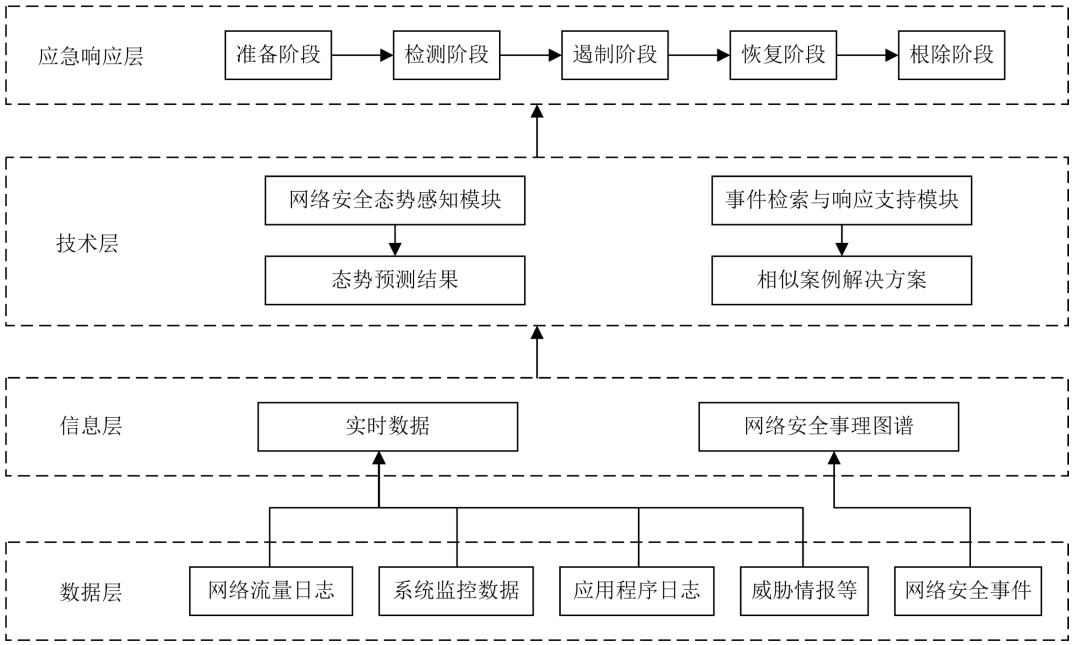

Figure 5. Cybersecurity emergency response decision support method
图 5. 基于事理图谱的网络安全应急响应决策支持机制

本方法由数据层、信息层、技术层和应急响应层构成。在数据层中，网络流量日志、系统监控数据等多种信息源为应急响应提供了实时数据，前文收集到的网络安全事件信息则为应急响应提供了历史数据。在信息层中，实时数据和由历史数据构建的网络安全事理图谱为后续的技术使用提供了信息支持。在技术层中，网络安全态势感知和事件检索与响应支持两个模块能为应急响应层快速响应网络安全风险、预测事件演化路径和制定有效决策提供技术支撑。

5. 结束语

本文针对网络安全事理图谱的事件检索机制进行研究，在事件要素向量化处理中引入了 BERT-wwm-ext 模型进行语义处理，并使用余弦相似度和动态规划方法进行事件相似度计算，以快速和准确地检索出关联度高的历史事件和演化路径知识，为网络安全管理提供响应支持。本文还提出了基于事理图谱的网

络安全应急响应决策支持机制，通过将网络空间中的实时数据与事理图谱中的历史数据相结合，该框架能够在网络攻击发生的各个阶段为相关人员提供高效、准确的决策支持帮助。

传统的网络安全应急响应模型通常依赖事先制定的应急计划，难以实时调整并快速响应，缺乏前瞻性和主动性，事理图谱技术的引入为网络安全治理提供了新的思路，本文提出的网络安全事理图谱检索方法和基于事理图谱的应急响应支持机制给出了该方法的具体实现技术和应用框架。本文的研究成果对于事理图谱技术在其他领域的应用实现也具有一定的参考意义。

本研究也存在一定的局限性，如：对于复杂攻击模式的表达能力不足、所提出的事件检索算法对权重敏感、对于检索结果事件的排序处理较为简化等，后续研究可以在提高事件表示模型适用性、增强检索算法鲁棒性和基于事理图谱事件关系优化检索结果排序等方向进一步展开。

参考文献

[1] 桂畅旎, 刘星. 2023 年国际网络空间形势回顾及发展动向[J]. 中国信息安全, 2023(12): 19-23.

[2] 孙珵珵. 网络安全治理对策研究[J]. 信息网络安全, 2023, 23(6): 104-110.

[3] Shiau, W., Wang, X. and Zheng, F. (2023) What Are the Trend and Core Knowledge of Information Security? A Citation and Co-Citation Analysis. *Information & Management*, **60**, Article ID: 103774. https://doi.org/10.1016/j.im.2023.103774

[4] 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.

[5] 刘善玲, 祁正华. 基于知识图谱的恶意域名检测[J]. 南京邮电大学学报(自然科学版), 2023, 43(3): 96-102.

[6] 王晓狄, 黄诚, 刘嘉勇. 面向网络安全开源情报的知识图谱研究综述[J]. 信息网络安全, 2023, 23(6): 11-21.

[7] 徐增林, 盛泳潘, 贺丽荣, 等. 知识图谱技术综述[J]. 电子科技大学学报, 2016, 45(4): 589-606.

[8] 魏建香, 梁帅, 朱云霞, 等. 事理图谱研究进展[J]. 情报资料工作, 2023, 44(6): 35-43.

[9] 赵文正, 王羽, 姜晓夏, 等. 军事事理图谱构建与交互式分析工具[J]. 指挥信息系统与技术, 2022, 13(3): 59-64.

[10] 高龙, 卫青延, 陶剑, 等. 事理图谱赋能的航空数据智能技术研究[J]. 航空工程进展, 2023, 14(2): 178-190.

[11] 高昂, 程越, 李进, 等. 网络新闻事件分类体系及事件本体建模语料库标准化研究[J]. 情报工程, 2017, 3(5): 43-52.

[12] 付雨萌, 程瑾, 罗准辰, 等. 基于本体的军事活动事件知识建模研究[J]. 中华医学图书情报杂志, 2020, 29(3): 47-52

[13] 全国网络安全标准化技术委员会. GB/T20986-2023 信息安全技术网络安全事件分类分级指南[S]. 北京: 中国标准出版社, 2023.

[14] 杨希晨, 魏红芹. 面向网络安全事件的事理图谱构建方法研究[J]. 管理科学与工程, 2025, 14(1): 145-155.

[15] Devlin, J., Chang, M.W., Lee, K., et al. (2019) BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding. *The* 2019 *Conference of the North American Chapter of the Association for Computational Linguistics*: *Human Language Technologies*, Minneapolis, 2-7 June 2019, 4171-4186.

[16] 郑光敏, 易天源, 唐东昕等. 基于 BERT-BiLSTM-CRF 模型的中国民族药知识抽取[J]. 武汉大学学报(理学版), 2021, 67(5): 393-402.

[17] 李书琴, 庞文婷. 嵌入词汇信息的 BERT-CRF 玉米育种实体关系联合抽取方法[J]. 农业机械学报, 2023(2): 1-16.

[18] 陈亮, 杨海. 网络安全事件应急响应亟需标准化[J]. 中国电信业, 2022(9): 74-76.