Management Science and Engineering 管理科学与工程, 2025, 14(1), 145-155
Published Online January 2025 in Hans. https://www.hanspub.org/journal/mse
https://doi.org/10.12677/mse.2025.141016

Hans汉斯

面向网络安全事件的事理图谱构建方法研究

杨希晨，魏红芹*

东华大学旭日工商管理学院，上海

收稿日期：2024年12月10日；录用日期：2025年1月11日；发布日期：2025年1月21日

摘　要

网络安全形势近年来呈现复杂化、广泛化等特点，对响应决策提出更高要求。现有的网络安全知识图谱只能提供静态的专业知识，无法呈现网络安全事件的动态演变。事理图谱通过追踪分析事件演化路径能为网络安全领域提供更好的决策支持。本文基于网络安全事件特征和相关标准分类构建了事理本体模型，采用模板匹配与依存句法分析获取事件表达，进行事件与事件关系抽取，并使用Gephi工具可视化呈现网络安全事理图谱。最后基于事理图谱数据实现网络安全态势预测和响应方案等决策支持。网络安全事理图谱能有效呈现网络安全事件演化的可能性，能为网络安全治理和应急响应决策提供一定参考。本文面向网络安全事件构建事理图谱，扩大了事理图谱的应用领域。

关键词

网络安全，事理图谱，事件抽取，决策支持

Research on Constructing Method of Event Evolutionary Graph for Cybersecurity Events

Xichen Yang, Hongqin Wei*

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

Received: Dec. 10th, 2024; accepted: Jan. 11th, 2025; published: Jan. 21st, 2025

Abstract

The situation of cybersecurity has become complicated and extensive in recent years, which puts forward higher requirements for response decision-making. The existing cybersecurity knowledge graph can only provide static expertise, but cannot present the dynamic evolution of cybersecurity events. Event evolutionary graph provides better decision support for cybersecurity by tracking and analyzing event evolution path. First, the event ontology model was constructed based on the

*通讯作者。

文章引用: 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.
DOI: 10.12677/mse.2025.141016

characteristics of cybersecurity events and related standard classification, then the event expression was obtained by using template matching and dependency parsing to extract event and event relationship, and the cybersecurity event evolutionary graph was visualized by using Gephi. Finally, the decision support of cybersecurity situation prediction and response scheme were realized based on the event evolutionary graph data. The cybersecurity event evolutionary graph can effectively present the possibility of the evolution of cybersecurity events, and provide some reference for cybersecurity governance and emergency response decision-making. This paper builds the event evolutionary graph based on cybersecurity events which expands its application field.

Keywords

Cybersecurity, Event Evolutionary Graph, Event Extraction, Decision Support

1. 引言

随着大数据、云计算等信息技术的发展，网络攻击逐渐多样化、复杂化。APT 攻击、恶意软件、网络漏洞和网络攻击等网络安全事件层出不穷，严重威胁了全球的网络空间安全。据统计，2023 年全球 72%的企业遭受了勒索软件的攻击，数据泄露的平均成本达到了历史最高的 445 万美元[1]。至 2025 年全球网络犯罪预计将造成 10.5 万亿美元的损失[2]。新兴技术的使用对网络安全治理带来了新的挑战。传统的网络应急经验无法应对新型网络安全事件，网络安全防护工作面临着巨大的挑战。为了应对网络安全领域面临的问题，相关学者对网络安全知识图谱开展研究。许多学者根据网络安全应用需要构建了以漏洞数据[3]、威胁情报[4]和恶意域名[5]等为主题的网络安全知识图谱。但知识图谱存在数据源质量参差不齐、未考虑实体动态变化、真实语义难以表示等难点[6]。此外，网络安全知识图谱只展示了静态的知识关系，无法呈现网络安全事件发生时具体的动态变化。

事件中蕴含着时间、人物、关系等大量对认识人类社会变化规律具有参考意义的信息，是构成人类社会活动的重要组成部分。2017 年哈尔滨工业大学的刘挺教授在中国计算机大会上提出了事理图谱的概念[7]。不同于知识图谱关注静态的实体关系，事理图谱的研究聚焦于事件的事理逻辑，描述事件的发展方向与发展趋势。事理图谱已被运用到了金融[8]、政策[9]、司法[10]、军事[11]、旅游[12]等研究领域中，应用广泛。但事理图谱在网络安全领域存在较多的研究空白。为进一步了解网络安全事件发生的动态变化，探讨运用事理图谱对网络安全事件治理的可行性，本文通过本体建模、信息抽取和图谱制作等流程，研究网络安全事理图谱作为事理逻辑知识库在呈现网络安全事件的发展方向与发展趋势上的作用，并为网络安全事件的预防与治理提供新的视角与思路。

2. 网络安全事理图谱构建原理

2.1. 基本思路

本文的网络安全事理图谱构建流程主要由数据采集与预处理、事理图谱构建和事理图谱制作三部分组成。在数据采集与预处理部分，本文使用了 Python 中的 Selenium 库爬取安全客等主流网络安全资讯网站中的网络安全事件文本，并对获取到的文本数据进行预处理以备后续使用。在事理图谱构建部分，事件本体建模、事件分类和事件抽取与事件关系抽取为主要内容。事件本体建模对网络安全事件的类别与

属性要素进行了详细规定；事件分类采用 LDA 主题模型判断网络安全事件的类别；事件抽取与事件关系抽取则在模式匹配和依存句法分析的基础上提取由事件表达与事件关系组成的事件元组。在图谱制作部分中，本文使用 Gephi 作图软件绘制网络安全事理图谱。具体流程如图 1 所示。

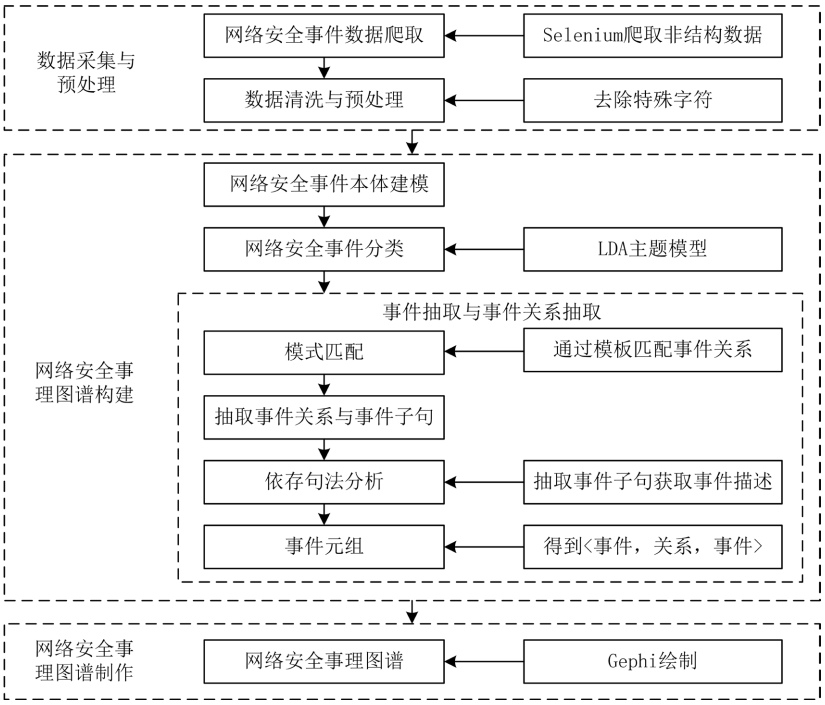

Figure 1. Construction process of cybersecurity event evolutionary graph
图 1. 网络安全事理图谱构建流程

2.2. 网络安全事件本体知识建模

知识建模是一种从数据源中获取规定知识表达的知识结构化过程。本体作为知识建模的一种，是一种通过定义概念和概念间关系来描述事物本质的模型[13]。通过构建网络安全事件本体知识模型有利于结构化梳理网络安全事件的构成，实现事件的统一表示。由于网络安全是事理图谱一个新的应用领域，目前还没有关于网络安全事理图谱本体知识模型的研究工作。

为提高研究成果的合理性和适用性，本文以国家相关分类标准为基础来构建网络安全事件本体知识模型。根据中国国家市场监督管理总局和国家标准化管理委员会制定的《GB/T 20986-2023 信息安全技术网络安全事件分类分级指南》，网络安全事件是指由于人为或外力影响使得网络或系统或数据受到危害，造成负面影响的事件，可分为恶意程序事件、网络攻击事件等十类[14]。本文在构建网络安全事件本体模型中参考了该指南的分类标准，同时考虑到恶意软件和漏洞是网络攻击者常用的两种攻击手段，因此将恶意软件事件和安全隐患事件并入到网络攻击事件之中，最终将网络安全事件划分为七个类别，具体分类如下：

1) 网络攻击事件。该事件是指使用恶意软件、利用漏洞等技术手段实施网络攻击的事件。网络攻击事件是网络安全事件中最为常见的一种。

2) 数据安全事件。该事件是指对数据实施篡改、泄露、窃取等造成数据损失的事件。数据泄露、数据假冒、数据滥用等都属于数据安全事件。

3) 信息内容安全事件。该事件是指通过网络传播危害有害信息的事件。

4) 设备设施故障事件。该事件是指网络自身出现故障或设备设施故障的事件。
5) 违规操作事件。该事件是指人为导致的网络安全事件，例如滥用权限等。
6) 异常行为事件。该事件是指网络本身不稳定或违规访问造成的异常行为。
7) 不可抗力事件。该事件是指因自然灾害等突发事件而损害网络的事件。

Table 1. Types and elements of cybersecurity events
表 1. 网络安全事件类型与要素内容

事件类型	事件要素
网络攻击事件	时间、攻击方、被攻击方、攻击方式、影响、措施
数据安全事件	时间、实施方、承受方、操作方式、影响、措施
信息内容安全事件	时间、发布方、发布平台、发布内容、影响、措施
设备设施故障事件	时间、故障方、故障设备、故障原因、影响、措施
违规操作事件	时间、违规操作者、违规操作内容、被影响方、影响、措施
异常行为事件	时间、异常方、异常内容、被影响方、影响、措施
不可抗力事件	时间、不可抗力因素、被影响方、影响、措施

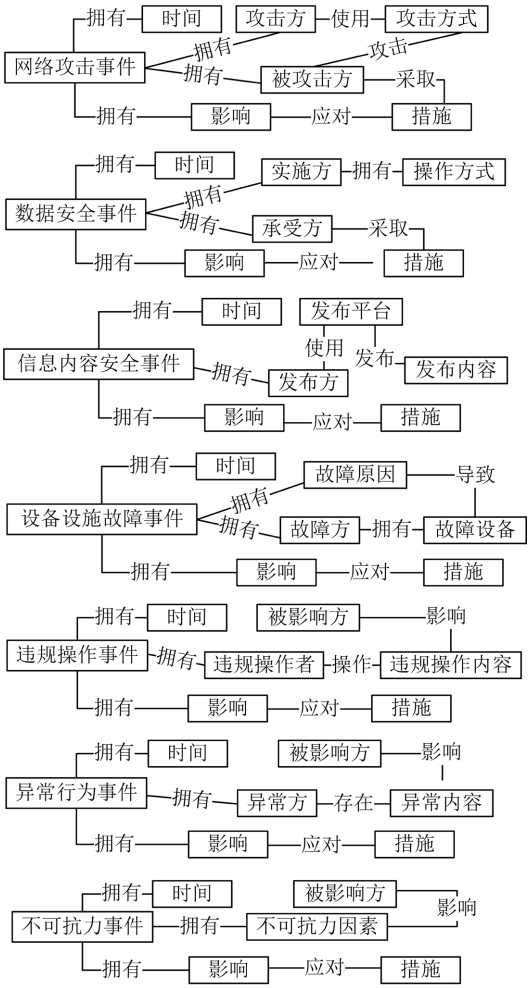

Figure 2. Cybersecurity event ontology knowledge model
图 2. 网络安全事件本体知识模型

不同的网络安全事件类型具有不同的要素。例如，网络攻击事件重点在于攻击，因此其本体模型应围绕攻击方、被攻击方、攻击方式等要素对实体、关系展开定义。表 1 根据每类网络安全事件的定义，给出了针对网络安全事件的事件类型及其具有的事件要素。图 2 则根据表 1 的定义，给出了针对网络安全事件的本体知识模型。与事件节点连接的节点代表本体知识模型的一类实体，节点间的连接代表了它们之间的关系。

网络安全子事理图谱制作时应按照构建的网络安全事件本体进行信息抽取。以网络攻击事件“黑客组织 KillNet 声称对 FBI 网站遭到了 DDoS 攻击负责。”为例，应提取攻击方“黑客组织 KillNet”、被攻击方“FBI 网站”和攻击方式“DDos 攻击”三个元素。网络安全事件本体模型规定了事件的抽取内容，为后续网络安全子事理图谱的构建奠定了信息结构化基础。

2.3. 事件与事件关系抽取

事件抽取与事件关系抽取是事理图谱研究的关键。事件抽取任务主要为确定事件类型和标记论元角色[15]。事件关系抽取任务则为识别事件与事件之间的逻辑关系。基于模式匹配、基于机器学习和基于深度学习是事件与事件关系抽取的三种主要方法[16]。基于模式匹配的方法一般需要人工构建规则与模板，再在模板的基础上抽取事件与关系。基于机器学习的方法则在模式匹配方法的基础上提升了可移植性，例如使用最大熵分类器抽取事件论元[17]和使用 Relief 算法抽取事件[18]。近年来，动态多池卷积神经网络[19]、BERT 模型[20]等基于深度学习的方法逐渐成为了研究的热门。

目前，主流的研究方法是使用 ACE2005 [21]、CEC [22]等数据集进行模型训练来高效抽取事件与事件关系。但通用领域数据集中涉及到网络安全领域事件的数据少，无法满足本研究需要。CASIE [23]和 CySecED [24]虽然是网络安全领域内的事件数据集，但数据内容均为英文。由于缺乏大量可供训练的中文数据，本文采用基于规则模板的方式抽取事件与事件关系。在关系抽取方面，本文主要抽取顺承关系和因果关系来了解网络安全事件的演变。

2.3.1. 事件分类

由于收集到的网络安全事件文本种类繁多，将网络安全事件按照类型划分有利于后续事理图谱的制作。本文使用 LDA 主题模型来判断网络安全事件的具体类型。LDA 主题模型是一种由文档、主题和词三层贝叶斯概率模型组成的生成概率模型，能够获取文本中的主题和对应主题的词分布。通过获得的主题与词语分布，能对文本的主题进行推测。使用 LDA 主题模型进行网络安全事件分类的具体流程如图 3 所示。

为了确保分类的准确性，在使用 LDA 主题模型前需要进行添加自定义词典、分词和去除停用词等预处理。使用词向量的方法对文本词语进行结构化表达，再使用 LDA 模型得到主题和主题对应的具体主题词。按照获取得到的文本主题词将文本归入到对应的网络安全事件类别之中。

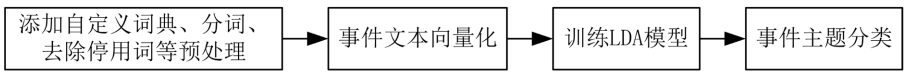

Figure 3. Flowchart of cybersecurity event classification
图 3. 网络安全事件分类流程图

2.3.2. 规则匹配

使用规则和模板匹配是对显性事件关系抽取较为有效的方法。显性关系是指在语句存在明显的关系关联词。例如，“因为”表示句子存在因果关系，而“接下来”则表明句子存在顺承关系。识别句子里的关联词能有效判别句子的逻辑关系，而关联词的选择则决定模版抽取的有效程度。在模版关联词选择上，本文通过遍历已爬取的网络安全事件文本，对文本进行分词与词频统计，使用出现的因果与顺承关联词

和常见关联词进行模板编写，编写规则模板共 11 条规则。

通过规则模版匹配判定事件关系。假设句子合集为S，词合集为W，因果关联词合集为C_1，顺承关联词为C_2，则$S=\{w_1,w_1,\ldots,w_n\}$表示一个句子中存在的词。在识别时，如果S中的某个s存在$w_i \in C_j$，则判定该句子存在对应的因果或顺序关系。例如在句子s“黑客攻击导致数据泄露”中存在关联词“导致”$w_3 \in C_1$，匹配因果模板输出原因子事件“黑客攻击”和结果子事件“数据泄露”。

2.3.3. 事件表达

提取依存句法分析中的成分是事件表示的一种有效方法。依存句法分析是一种通过识别句子中词汇与词汇间的互相依存关系来表示语句句法结构的自然语言处理技术。其中，修饰词被称为“从属词”，被修饰词被称为“核心词”，从属词和核心词之间存在的语义关系则被称为依存关系。通过识别词汇与词汇之间的依存关系，按照相应规则抽取可以获得的语义表达。常见的依存关系如表 2 所示。

Table 2. Common dependencies
表 2. 常见的依存关系

依存关系类型	依存关系标注	依存关系类型	依存关系标注
主谓关系	SBV	状中关系	ADV
动宾关系	VOB	并列关系	COO
间宾关系	IOB	动补关系	CMP
前置宾语	FOB	介宾关系	POB
定中关系	ATT	核心关系	HED
兼语	DBL	独立结构	IS
左附加关系	LDA	右附加关系	RDA

网络安全事件的大多数文本具有较为完整的主谓宾句子结构，且文本中的语句量较大。为更好地保留语句含义、删去不必要的内容，本文抽取依存句法中由核心词串联的主谓关系(SBV)、动宾关系(VOB)或前置宾语(FOB)。不同于只根据依存句法关系组合抽取句子中的信息，抽取由核心词串联的依存句法关系更能确保抽取的是句子核心。以句子“澳大利亚维多利亚州的法庭记录数据库遭到黑客攻击”为例，其依存句法分析结果如图 4 所示。该句的核心词为“遭到”，与它存在主谓关系(SBV)与动宾关系(VOB)的词为“数据库”和“攻击”。而“黑客”和“攻击”之间存在主谓关系(SBV)。因此，该句的抽取结果为“数据库遭到黑客攻击”。

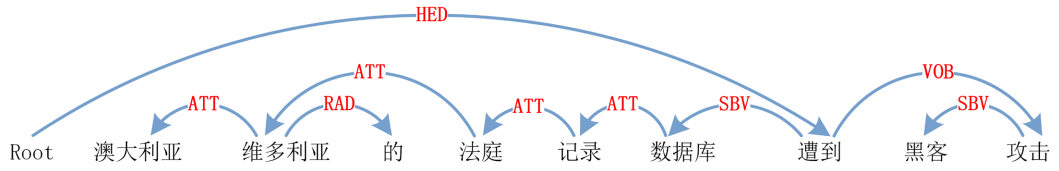

Figure 4. Dependency parsing example
图 4. 依存句法分析实例

在规则模版匹配后，存储以为<事件，关系，事件>为形式的事件元组。以“澳大利亚维多利亚州的法庭记录数据库遭到黑客攻击，导致法庭视听网络中断。”为例，存在因果关联词“导致”，提取事件子句后再对其使用依存句法分析，最终得到<数据库遭到黑客攻击，因果关系，网络中断>的网络安全事件

关系三元组。获取到的网络安全事件三元组将作为图谱制作的数据来源。

2.4. 事件融合分析与事理图谱构建

网络安全事理图谱以提取到的网络安全事件抽取和分析结果为数据源，使用 Gephi 工具绘制。本文将根据事件关系强弱分析分别构建网络安全子事理图谱和网络安全总事理图谱。

网络安全子事理图谱以一组强相关的网络安全事件为例，按照本体建模中设定的事件论元和事件与事件关系元组对事件进行抽取并绘制事理图谱

网络安全总事理图谱则对收集到的所有数据进行事件图谱绘制。由于一些事件表达存在表述不一致却意思相近的情况，本文为减少冗余对相似的事件进行精简合并。具体步骤如下：

步骤一：将事件表达转化为词向量的形式。

将自然语言转化为数值向量的词向量是计算机处理文本信息的第一步。本文使用 TF-IDF 算法将经过处理的事件表达转化为词向量的形式。TF-IDF 通过计算词频和逆文档频率获得事件表达的向量。TF-IDF 公式如下：

$$TF-IDF=TF\left(t,d\right)\times IDF\left(t\right) \tag{1}$$

其中，t 表示事件表达中的特定词汇，d 表示事件表达，$TF\left(t,d\right)$ 表示该词汇在事件表达中出现的频率，$IDF\left(t\right)$ 表示该词汇在所有事件表达中常见程度。

步骤二：计算语义相似度

使用余弦相似度计算事件表达的语义相似度。余弦相似度通过计算向量在空间方向上的差异判断向量的相似程度。对于两个向量化的事件表达 $A_i=\left(A_1,A_2,\ldots,A_n\right)$ 和 $B_i=\left(B_1,B_2,\ldots,B_n\right)$，其余弦相似度计算公式如下：

$$\cos\left(\theta\right)=\frac{\sum_{i=1}^{n}\left(A_i\times B_i\right)}{\sqrt{\sum_{i=1}^{n}\left(A_i\right)^2}+\sqrt{\sum_{i=1}^{n}\left(B_i\right)^2}} \tag{2}$$

步骤三：合并事件表达

设定阈值，导出相似度大于阈值的事件表达组。根据导出结果，将类似的事件表述合并为一类。例如，相似事件表达组[“泄露数据”“大量敏感数据泄露”“数据泄漏被传输境外”]中的事件表达都可合并简化为“数据泄露”。

3. 实例分析

3.1. 数据采集与预处理

本文数据来源于网络资讯网站平台发布的网络安全事件新闻。实验使用自动化测试工具 Selenium 模拟浏览器自动访问资讯网站并使用 xpath 定位获取数据，实现页面跳转爬取网络安全事件的文本内容。由于网络安全领域的特殊性，需要在自定义字典中添加网络安全领域内的专有词语，例如“钓鱼攻击”“撞库”等，再对文本进行分词、词性标注等预处理以便后续实验使用。

3.2. 事件抽取与表达

事件抽取与表达在经过预处理的文本的基础上进行。导入先前制定的因果关联词词表和顺承关联词词表，对事件关系进行判断。确定事件关系后，再根据前面定义的规则模板与依存句法分析规则抽取事件表达。对获取到的事件表达进行进一步整理，获得网络安全事件发展的事件链路。某个网络安全事件文本抽取到的事件表达与事件关系如表 3 所示。

Table 3. Examples of event extraction and representation
表 3. 事件抽取与表达示例

事件	事件关系	事件
数据访问工具一个小变化	因果	引发故障
引发故障	因果	代码堆栈需要完全重写
引发故障	因果	Twitter 用户访问问题
引发故障	顺承	Twitter 已修复故障

3.3. 事理图谱构建

3.3.1. 图谱构建

本文使用可视化工具 Gephi 对构建网络安全事理图谱。对于网络安全子事理图谱，其节点为网络安全事件的论元要素，边为要素与事件之间的关系；对于网络安全总事理图谱，其节点为事件节点，有向边为事件与事件之间的关系。此外，网络安全总事理图谱中还存在用于串联图谱的网络安全事件主题源节点为和与其相连的用于连接具体事件的网络安全事件类别节点。

3.3.2. 网络安全子事理图谱

网络安全子事理图谱以具体事件为基础，对事件的各个要素进行提取。本文以药房“内鬼”盗卖数据的网络安全事件为案例，构造具体的事理图谱。经过 LDA 主题识别，该事件因具有关键词“数据泄露”被判定为数据安全事件。按照构造的网络安全事件本体模型，该事件应具有时间、实施方、承受方、影响、措施等元素。图谱制作时先使用语义角色标注工具辅助抽取要素，再使用规则模板和依存句法分析得到对应的事件关系和事件表达，最后使用 Gephi 作图。得到的药房“内鬼”盗卖数据的具体事理图谱如图 5 所示。

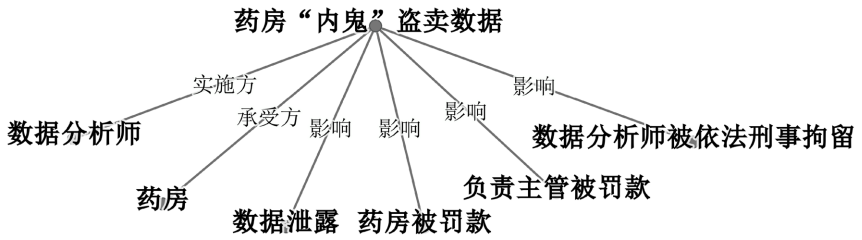

Figure 5. Pharmacy “inside man” stealing and selling data event evolutionary graph
图 5. 药房“内鬼”盗卖数据事理图谱

从图 5 可知，药房“内鬼”盗卖数据事件是药房内的数据分析盗卖药房数据造成的。其造成了数据泄漏、药房被罚款、负责主管被罚款和数据分析师被依法刑事拘留的后果。由此可见，构建网络安全子事理图谱可以得到网络安全事件的各项组成信息和了解把握事件的具体脉络。

3.3.3. 网络安全总事理图谱

网络安全总事理图谱以所有抽取好的事件关系三元组为基础。经过事件汇总去重、短语向量化、计算余弦相似度和将类似的文本归类的处理后，将文本按照规定的网络安全事件分类进行绘制得到网络安全总事理图谱。网络安全总事理图谱呈现了网络安全事件的所有可能性与演化过程。基于部分数据的网络安全总事理图谱节选如图 6 所示。

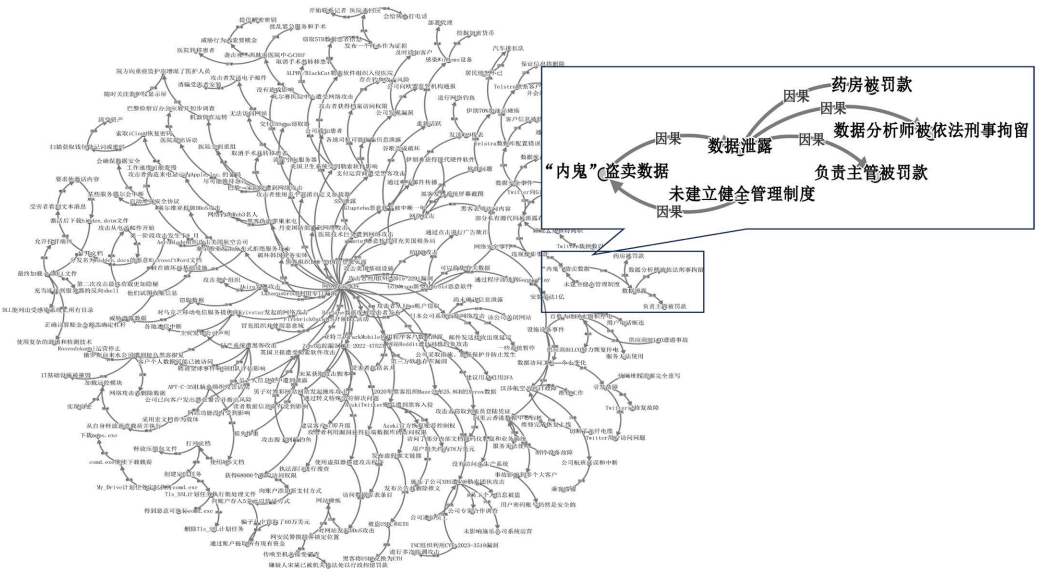

Figure 6. Cybersecurity overall event evolutionary graph (part)
图 6. 网络安全总事理图谱(部分)

3.4. 事理图谱的应用

从构建的事理图谱可以看出，网络安全事件中存在原因、过程、影响和解决方案等成分。使用图数据库或算法查询节点有助于了解网络安全事件的情况并进行针对性治理。为评估网络安全事理图谱的可应用性，本文在已构建的事理图谱上进行可行性分析。

3.4.1. 基于事理图谱的攻击态势预测

对于主要呈现网络攻击技术路径的网络安全事件文本，事理图谱可以有效展现网络攻击的路径。图 7 主要展示了 APT-C-35 肚脑虫组织常见的两种攻击路径。一种采用宏文档作为载体，其自身会释放恶意载荷，执行恶意载荷后会加载远控模式来实现窃密。另一种则为使用 XLS 文档，该路径会释放压缩包文件和创建定时任务。My_Drive 定时任务会下载 comd.exe，继而下载 mnps.exe；Tls_SSL 定时任务会执行 comd.exe 并删除 Tsl_SSL 任务。

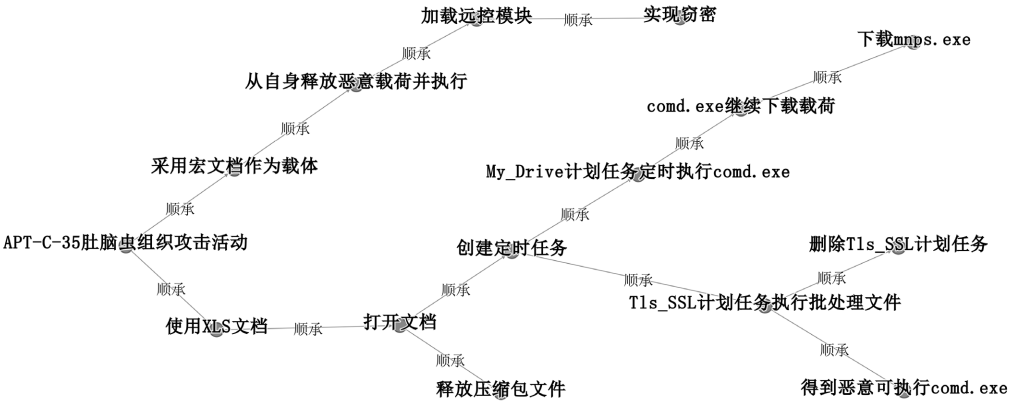

Figure 7. Examples of APT-C-35 in the cybersecurity overall event evolutionary graph
图 7. 网络安全总事理图谱中的 APT-C-35 事例

基于事理图谱可以得出以下判断，APT-C-35 肚脑虫组织攻击时若使用宏文档，则可预判其下一步操作为释放恶意载荷；若使用 XLS 文档，则可预判其下一步操作为释放压缩包与创建定时任务。由此可见，根据事理图谱中攻击流程的节点位置，相关技术人员可以了解攻击的上下游操作，预测网络攻击态势，以实现对攻击的及时阻断与应对。因此，基于事理图谱的攻击态势预测具有一定的可行性。

3.4.2. 基于事理图谱的响应决策可行性分析

响应决策支持是事件发生时利用方法或工具来帮助决策者制定响应策略和方案的过程，其目标是降低事件可能带来的损失。网络安全事件往往是突发性，很难在事前预测，因此事后的应急响应决策在事件应对中显得尤为重要。在整个应急响应过程中网络安全事件的态势是动态变化的，而事理图谱的存在可以展现事件的动态变化辅助响应决策。

事理图谱的应用有助于应急响应团队在事件发生后迅速识别潜在风险和优化资源分配。基于事理图谱可以发现各类网络安全事件可能带来的后续影响，例如网络攻击可能造成设备感染、数据泄露、基础设施被摧毁、资产受损等后果。在受到攻击时，有关人员可以根据类似的攻击事件分析可能存在的风险并合理分配资源。

以图 8 某一 DDOS 攻击事件为例。根据网络安全事理图谱中的事件因果链可知，DDOS 的攻击目标为 IT 基础设施。作为应对措施的增强安全协议虽然可能会导致服务中断和工作速度变慢的后果，但它会确保数据安全。因此在类似攻击事件发生时，应急响应人员可以采取增强安全协议，并迅速启动针对基础设施攻击及其后果的应急响应流程，将资源优先投入到基础设施设备的维护与防御中，确保相关基础设施的运营稳定，从而降低或避免可能的造成的损失。此外，还可以针对增强安全协议可能带来的负面影响进行维护和优化。由此可见，事理图谱能为应急响应提供一定的决策支持。

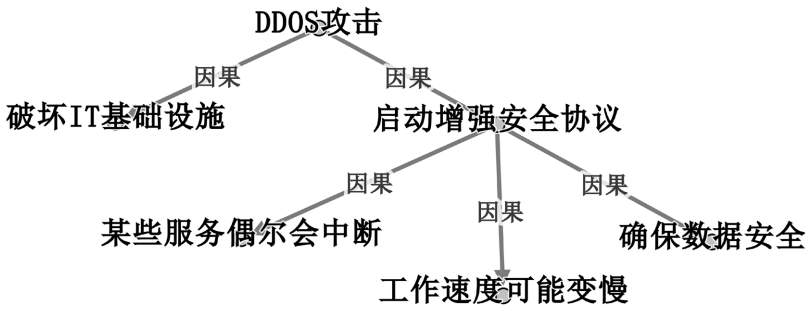

Figure 8. An example of a cyber-attack in the cybersecurity overall event evolutionary graph
图 8. 网络安全总事理图谱中的某一网络攻击事例

4. 结束语

本文提出了一种网络安全事件本体模型和面向网络安全事件的事理图谱构建方法。以采集到的网络安全事件文本为例，经过事件分类、规则模板匹配、依存句法分析、计算余弦相似度等过程获取网络安全事件总事理图谱，并使用 Gephi 进行可视化处理。

网络安全子事理图谱展示了某特定网络安全事件集的具体论元要素，呈现了事件之间的逻辑关系，有助于决策人员了解事件发生的原因与结果。同时网络安全总事理图谱展示了网络安全事件发生的可能路径与演化，有助于相关网络安全管理人员根据网络安全事件发生的相关节点判断态势、预测路径与响应决策。本文的研究结果为网络安全事件应急响应与治理研究提出了一种新的思路，对于事理图谱在不同领域的应用拓展进行了有益的探索，同时进一步深化了事理图谱的理论内涵和实践方法。

本研究仍存在需要完善的地方，比如研究的数据主要为网络安全资讯文本，具有一定局限性。后续将对事理图谱与多源数据集的融合和决策分析进行研究，以期为网络安全管理提供更多决策支持。

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] 中国网络安全产业联盟. 中国网络安全产业分析报告[R]. 中国网络安全产业联盟, 2023.

[3] 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]. 工程(英文), 2018, 4(1): 117-133.

[4] 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.

[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] 刘如, 周京艳, 李佳娱, 等. 基于数据科学思维的情报事理逻辑揭示与科学解读[J]. 情报理论与实践, 2018, 41(8): 22-27.

[8] 杨纪星, 杨波, 朱剑林, 等. 金融领域事件因果关系发现及事理图谱构建与应用[J]. 中文信息学报, 2023, 37(7): 131-142.

[9] 单晓红, 庞世红, 刘晓燕, 等. 基于事理图谱的政策影响分析方法及实证研究[J]. 复杂系统与复杂性科学, 2019, 16(1): 74-82.

[10] 朱福勇, 刘雅迪, 高帆, 等. 基于图谱融合的人工智能司法数据库构建研究[J]. 扬州大学学报(人文社会科学版), 2019, 23(6): 89-96.

[11] 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.

[12] 王翊臻, 云红艳, 李正民. 旅游顺承事理图谱的构建及应用研究[J]. 青岛大学学报(自然科学版), 2022, 35(1): 34-39+47.

[13] 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.

[14] 全国网络安全标准化技术委员会. 信息安全技术网络安全事件分类分级指南: GB/T 20986-2023 [S]. 北京: 中国标准出版社, 2023: 2-6.

[15] 朱艺娜, 曹阳, 钟靖越, 等. 事件抽取技术研究综述[J]. 计算机科学, 2022, 49(12): 264-273.

[16] 马春明, 李秀红, 李哲, 等. 事件抽取综述[J]. 计算机应用, 2022, 42(10): 2975-2989.

[17] Chieu, H.L. and Ng, H.T. (2002) A Maximum Entropy Approach to Information Extraction from Semi-Structured and Free Text. American Association for Artificial Intelligence, 786-791.

[18] Fu, J., Liu, Z., Zhong, Z. and Shan, J. (2009) Chinese Event Extraction Based on Feature Weighting. *Information Technology Journal*, **9**, 184-187. https://doi.org/10.3923/itj.2010.184.187

[19] Chen, Y., Xu, L., Liu, K., Zeng, D. and Zhao, J. (2015) Event Extraction via Dynamic Multi-Pooling Convolutional Neural Networks. *Proceedings of the* 53*rd Annual Meeting of the Association for Computational Linguistics and the* 7*th International Joint Conference on Natural Language Processing*, Volume 1, 167-176. https://doi.org/10.3115/v1/p15-1017

[20] 李旭晖, 程威, 唐小雅, 等. 基于多层卷积神经网络的金融事件联合抽取方法[J]. 图书情报工作, 2021, 65(24): 89-99.

[21] Consortium, L.D. (2005) ACE (Automatic Content Extraction) English Annotation Guidelines for Events.

[22] 刘炜, 王旭, 张雨嘉, 等. 一种面向突发事件的文本语料自动标注方法[J]. 中文信息学报, 2017, 31(2): 76-85.

[23] Satyapanich, T., Ferraro, F. and Finin, T. (2020) CASIE: Extracting Cybersecurity Event Information from Text. *Proceedings of the AAAI Conference on Artificial Intelligence*, **34**, 8749-8757. https://doi.org/10.1609/aaai.v34i05.6401

[24] Trong, H.M.D., Le, D.T., Veyseh, A.P.B., Nguyen, T. and Nguyen, T.H. (2020) Introducing a New Dataset for Event Detection in Cybersecurity Texts. *Proceedings of the* 2020 *Conference on Empirical Methods in Natural Language Processing* (*EMNLP*), November 2020, 5381-5390.