中文引用格式:王渊洁,王秉,李燕峰,等. 安全情报视域下的安全事件致因模型构建[J]. 中国安全科学学报,2024,34(2):15-21.
英文引用格式:WANG Yuanjie, WANG Bing, LI Yanfeng, et al. Construction of safety and security incident causation model from a safety and security intelligence perspective [J]. China Safety Science Journal, 2024,34(2):15-21.

安全情报视域下的安全事件致因模型构建*

王渊洁[1,2,3], 王 秉[1,2,3]教授, 李燕峰**[4]讲师, 史志勇[1,2,3]
(1 中南大学 资源与安全工程学院,湖南 长沙 410083;2 中南大学 安全理论创新与促进研究中心,湖南 长沙 410083; 3 中南大学 安全科学与应急管理研究中心,湖南 长沙 410083;
4 中南大学 学科建设办公室,湖南 长沙 410083)

中图分类号:X915.2 **文献标志码**:A **DOI**: 10.16265/j.cnki.issn1003-3033.2024.02.0107
基金项目:国家社会科学基金重大项目资助(22ZDA121)。

【摘 要】 为明晰安全情报视域下的安全事件致因机制,夯实安全情报视域下安全事件调查分析与防控理论基础,开展安全情报视域下的安全事件致因模型研究。首先,根据安全情报-安全行为双循环模型,分析安全情报视域下的安全事件成因;其次,构建并解析安全情报视域下的安全事件致因模型;最后,以某市地铁X号线安全事件为例,应用分析安全情报视域下的安全事件致因模型。结果表明:安全情报视域下的安全事件致因模型是由安全情报循环与安全行为循环构成的一个安全事件致因系统。根据该模型,安全情报循环过程中出现的安全情报失误问题会引发系统的安全行为循环紊乱和崩溃,从而导致系统内发生安全事件。

【关键词】 安全情报; 安全事件; 致因模型; 安全行为; 安全情报失误

Construction of safety and security incident causation model from a safety and security intelligence perspective

WANG Yuanjie[1,2,3], **WANG Bing**[1,2,3], **LI Yanfeng**[4], **SHI Zhiyong**[1,2,3]
(1 School of Resources and Safety Engineering, Central South University, Changsha Hunan 410083, China; 2 Safety and Security Theory Innovation and Promotion Center (STIPC), Central South University, Changsha Hunan 410083, China; 3 Safety and Security Science and Emergency Management Center, Central South University, Changsha Hunan 410083, China; 4 Office of Discipline Management, Central South University, Changsha Hunan 410083, China)

Abstract: In order to clarify the mechanism of safety and security incident causation from a safety and security intelligence perspective, and to consolidate the theoretical foundation for the investigation, analysis and prevention, and control of safety and security incidents from a safety and security intelligence perspective, research on safety and security incident causation model from a safety and security intelligence perspective was conducted. Firstly, according to the model for safety and security intelligence-safety and security behavior double loops, this paper analyzed the causes of safety and security incidents from a safety and security intelligence perspective. Secondly, the safety and security incident causation model from a safety and security intelligence perspective was constructed and explained. Finally, this paper analyzed the application of the safety and security incident causation model from a safety and security intelligence

* 文章编号:1003-3033(2024)02-0015-07; 收稿日期:2023-08-14; 修稿日期:2023-11-12
** 通信作者:李燕峰(1979—),男,河南郑州人,博士,讲师,主要从事数据安全与学科数据系统管理等方面的研究。E-mail:liyanfeng@csu.edu.cn。

perspective with a safety and security incident on Line X of a city metro. The research shows that the safety and security incident causation model from a safety and security intelligence perspective is a safety and security incident causation system consisting of a safety and security intelligence loop and a safety and security behavior loop. According to this model, safety and security intelligence failures in the safety and security intelligence loop can lead to the disruption and collapse of the safety and security behavior loop of the system, resulting in a safety and security incident in the system.

Keywords: safety and security intelligence; safety and security incident; causation model; safety and security behavior; safety and security intelligence failure

0 引　言

安全事件致因是安全科学的重要研究内容。安全情报是对安全事件防控有用的安全信息,安全事件防控离不开安全情报的支持[1]。例如:在网络和数据安全领域,网络和数据安全情报视角下的网络和数据安全事件防控研究和实践极为普遍。可见:安全情报是分析安全事件致因的重要视角之一。因此,开展安全情报视域下的安全事件致因研究意义重大。

在安全领域,安全事件包括 Safety 事件(即事故,它一般指因无意因素引发的安全事件)与 Security 事件(一般指因蓄意因素引发的安全事件)2 类[2]。现代安全科学认为,任何系统安全问题均是 Safety 与 Security 一体化的安全问题,系统安全事件同时涉及 Safety 事件和 Security 事件[2]。就数据系统安全而言,既要防控因自然灾害和质量设计等无意因素引发的 Safety 事件,又要防控因黑客攻击和间谍软件等蓄意因素引发的 Security 事件。因此,从系统安全角度看,应同时关注涵盖 Safety 事件和 Security 事件具有普适性的安全事件致因研究[2]。但是,已有安全事件致因研究主要集中在 Safety 事件致因研究层面[3],尚未过渡至同时面向 Safety 事件和 Security 事件的具有普适性的安全事件致因研究。同时,从安全信息链(安全事实→安全数据→安全信息→安全情报→安全智慧)[4]角度看,实现安全事件智慧防控需明晰安全情报视域下的安全事件致因,但目前安全事件致因研究主要停留在安全信息层面,如基于安全信息流的事故致因模型[5]和多级安全信息不对称模型[6]等,尚未过渡至安全情报层面。综上,亟需开展安全情报视域下的安全事件(包括 Safety 事件和 Security 事件)致因研究。

鉴于此,笔者拟从安全情报视域出发,分析安全情报视域下的安全事件成因,构建安全情报视域下的安全事件致因模型,以期丰富安全情报视域下的安全事件致因理论,从而为安全事件调查分析和防控提供相关理论依据。

1 安全情报视域下的安全事件成因

从安全情报角度看,安全事件防控是一个基于安全情报支持的多种安全行为不断循环的过程。根据安全情报循环(包括安全情报搜集、安全情报分析、安全情报生产和安全情报应用)[7]与安全行为循环(包括安全感知、安全判断、安全决策和安全执行),构建安全情报-安全行为双循环模型,如图 1 所示。图 1 中,外环的安全情报循环与内环的安全行为循环之间呈相互对应关系,即安全情报搜集对应安全感知、安全情报分析对应安全判断、安全情报生产对应安全决策,以及安全情报应用对应安全执行,具体解释见表 1,内环的安全行为循环需依靠外环的安全情报循环开展。需说明的是,在当今数智时代,安全情报工作离不开数智技术的支撑,为确保安全情报本身的安全,在安全情报循环中应尽可能使用安全性高的数智技术(如区块链被认为是一种安全可信度高的数智技术[8])。

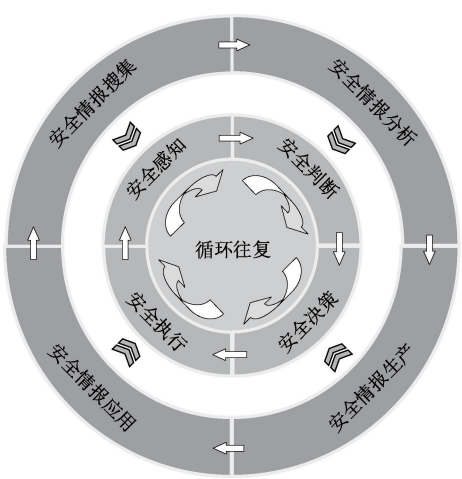


图 1 “安全情报-安全行为”双循环模型

Fig. 1 Model for "safety and security intelligence-safety and security behavior" double loops

表 1　安全情报循环与安全行为循环的具体内容及相互对应关系

Tab. 1　Specific content and mutual correspondence of safety and security intelligence loop and safety and security behavior loop

序号	安全情报循环	安全行为循环	对应关系
1	安全情报搜集表示安全情报部门利用多种方法获取所需安全数据,并初步清洗和筛选安全数据	安全感知是指通过多渠道感知、记录和存储引起系统安全态势变化的安全要素,并为进一步安全判断提供基础资源	安全情报搜集的内容会影响安全感知的效果
2	安全情报分析表示安全情报部门加工处理搜集的安全数据,并形成安全信息	安全判断表示安全事件防控者依据安全感知过程中获取到的安全要素,结合自身的安全风险认知,研判当前系统安全态势	安全情报分析的结果会影响安全判断的正确性
3	安全情报生产是结合安全信息与专家系统,通过各领域专家评估与审核安全信息,获得成熟的安全情报产品	安全决策是根据安全判断结果,针对系统安全态势的控制与优化方案或措施,快速作出科学、有效且经济的决策,是对安全判断的验证	安全情报生产的安全情报产品对安全决策具有重要支撑作用
4	安全情报应用表示安全情报产品被用于支持安全事件防控的具体活动	安全执行是指根据安全决策指示,通过及时有效地实施安全决策方案,尽可能防控安全事件发生或通过相关应急措施将安全事件的不良影响降至最低,使安全决策结果转化为实际行动	安全情报应用体现在安全执行全过程,影响安全执行的效果

由图 1 可知:安全情报循环对安全行为循环具有支撑作用。然而,在安全情报循环过程中,当出现安全情报失误(安全情报失误是一种客观的存在,会出现在安全情报的搜集、分析、生产和应用环节)时,安全情报循环对安全行为循环的支撑作用就会受到影响,导致安全行为失败,并阻断安全行为循环过程,进而引发安全事件。安全情报视域下的安全事件成因是安全情报循环过程中出现安全情报失误,致使安全行为循环无法获得足够的安全情报支持而紊乱乃至崩溃,最终导致安全事件发生。安全情报视域下的安全事件成因如图 2 所示。

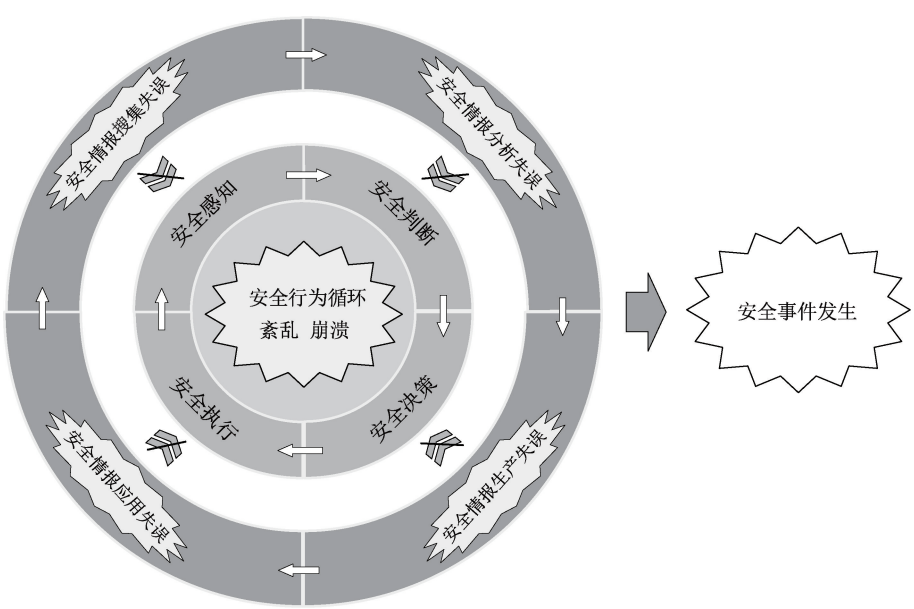


图 2　安全情报视域下的安全事件成因

Fig. 2　Causes of safety and security incidents from a safety and security intelligence perspective

2　安全情报视域下的安全事件致因模型

在明晰安全情报视域下安全事件成因的基础上,结合安全情报理论,构建安全情报视域下的安全事件致因模型(简化版),如图 3 所示。该模型中,基于安全情报循环与安全行为循环的相互对应关系,设安全情报搜集-安全感知为 A,安全情报分析-

安全判断为 B,安全情报生产-安全决策为 C,安全情报应用-安全执行为 D。其中,每个阶段都可能引发安全事件,具体解释见表 2。

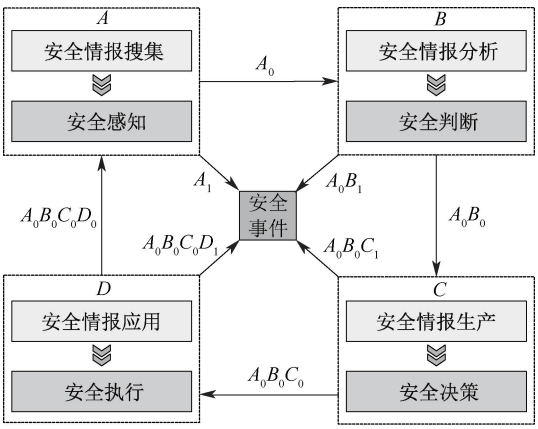


图 3 安全情报视域下的安全事件致因模型(简化版)

Fig. 3 Safety and security incident causation model from a safety and security intelligence perspective (simplified version)

基于安全情报视域下的安全事件致因模型(简化版),面向安全事件防控全过程,结合安全行为循环中的具体安全行为,构建安全情报视域下的安全事件致因模型(详细版),如图 4 所示。

图 4 中,从安全情报循环与安全行为循环的不同阶段出发,具体分析了安全情报视域下的安全事件致因模型(详细版),分别为:

1) 安全情报搜集-安全感知阶段。此阶段中,安全事件防控者在安全情报搜集工作支持下,通过文本感知方式(如安全事件报告、安全法律法规和安全标准政策等)、物联网感知方式(如视频、音频、定位和传感等)和生物感知方式(视觉、嗅觉、听觉和触觉等)等记录与储存引起系统安全态势变化的安全要素。①当安全情报搜集正常时,安全情报为安全感知提供大量获取的安全信息,确保安全感知过程中收集到高质量的安全要素,服务下一阶段(即 A_0);②当安全情报搜集失误时,原有的安全情报搜集工作被迫阻断,致使安全感知能力不足,易出现个人对安全风险的感知偏差和组织安全风险告知的缺失等问题,导致所获安全要素在精准性、全面性与深入性等质量方面有所缺陷,易引发安全事件(即 A_1)。

表 2 安全情报视域下的安全事件致因模型(简化版)的具体解释

Tab. 2 Specific explanation of safety and security incident causation model from a safety and security intelligence perspective (simplified version)

序号	阶段	判定结果	具体解释	结果
1	A	A_0	安全情报搜集未发生失误,安全感知正常	进入下一阶段
		A_1	安全情报搜集失误,安全感知失败	引发安全事件
2	B	A_0B_0	安全情报搜集未发生失误,安全感知正常 安全情报分析未发生失误,安全判断正常	进入下一阶段
		A_0B_1	安全情报搜集未发生失误,安全感知正常 安全情报分析失误,安全判断失败	引发安全事件
3	C	$A_0B_0C_0$	安全情报搜集未发生失误,安全感知正常 安全情报分析未发生失误,安全判断正常 安全情报生产未发生失误,安全决策正常	进入下一阶段
		$A_0B_0C_1$	安全情报搜集未发生失误,安全感知正常 安全情报分析未发生失误,安全判断正常 安全情报生产失误,安全决策失败	引发安全事件
4	D	$A_0B_0C_0D_0$	安全情报搜集未发生失误,安全感知正常 安全情报分析未发生失误,安全判断正常 安全情报生产未发生失误,安全决策正常 安全情报应用未发生失误,安全执行正常	重新进入循环
		$A_0B_0C_0D_1$	安全情报搜集未发生失误,安全感知正常 安全情报分析未发生失误,安全判断正常 安全情报生产未发生失误,安全决策正常 安全情报应用失误,安全执行失败	引发安全事件

2) 安全情报分析-安全判断阶段。此阶段中,安全事件防控者在安全情报分析工作支持下,综合自身分析整合安全要素的能力、以往安全事件的经验教训、自身生理心理特征以及安全文化等因素,对

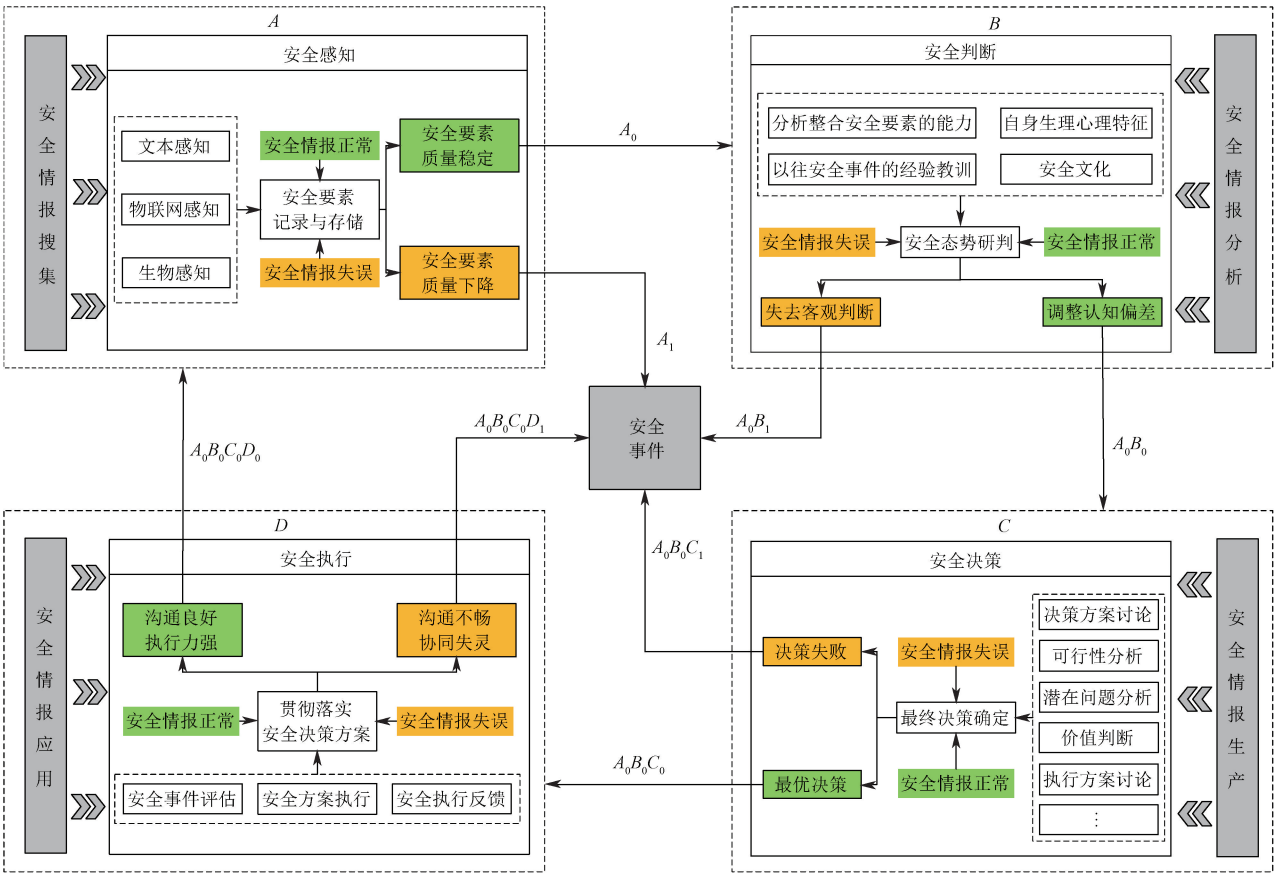


图 4　安全情报视域下的安全事件致因模型(详细版)

Fig. 4　Safety and security incident causation model from a safety and security intelligence perspective(detailed version)

当前安全态势作出判断。①当安全情报分析正常时,安全事件防控者通过安全情报分析结果来调整自身安全风险认知的偏差和局限[9],更科学、客观地进行安全判断并服务下一阶段(即 A_0B_0);②当安全情报分析失误时,原有的安全情报分析工作被迫阻断,安全事件防控者会因上述多个因素的个体差异而产生不同,甚至对立的判断结果,导致安全判断失去对安全决策和安全执行阶段原有的在方向上的引导作用,引发安全事件(即 A_0B_1)。

3) 安全情报生产-安全决策阶段。此阶段中,安全事件防控者在安全情报生产工作的支持下,进行包括确定决策方案、可行性分析、潜在问题分析、价值判断和确定执行方案等安全决策活动。安全决策决定安全态势的最终转变方向。因此,该阶段是安全情报视域下的安全事件致因模型中最关键的一环,也是安全情报最主要的价值体现,反映出安全情报"用于解决安全决策过程中信息不完备问题"的本质作用。①当安全情报生产正常时,所生产的安全情报产品能够以支撑工具(包括方法、技术和技能)的形式来辅助安全决策,从而对安全态势的发展产生重要影响,并服务下一阶段(即 $A_0B_0C_0$);②当安全情报生产失误时,原有的安全情报生产工作被迫阻断,安全决策会缺失最重要的支撑内容(即安全情报产品),极易导致安全决策失败,造成安全事件发生等局面(即 $A_0B_0C_1$)。

4) 安全情报应用-安全执行阶段。此阶段中,安全事件防控者在安全情报应用工作的支持下贯彻落实安全决策方案,进行安全事件评估、安全方案执行以及安全执行反馈等具体安全执行活动。安全情报应用会对安全执行起到积极作用,安全执行也是安全情报应用的重要体现。①当安全情报应用正常时,安全情报促进安全执行过程中指令的传递与流通,有利于上层管理者对一线人员的指挥以及相关部门之间的沟通与协同,并完成"安全情报-安全行为"双循环(即 $A_0B_0C_0D_0$);②当安全情报应用失误时,原有的安全情报应用工作被迫阻断,相关指令无法在恰当的情景中及时传递给对口的接收者,降低一线人员的执行效果。同时,安全情报失误也会使各部门之间的信息沟通不畅,严重阻碍安全执行过程中各部门间的交流、合作与协同,易引发安全事件

(即 $A_0B_0C_0D_1$)。

3 模型的应用分析

以某市地铁 X 号线安全事件为例,分析应用安全情报视域下的安全事件致因模型,如图 5 所示。地铁 X 号线安全事件是一起由极端暴雨引发严重城市内涝,涝水冲毁停车场挡水围墙、灌入地铁隧道,某市地铁集团有限公司和有关方面应对处置不力、行车指挥调度失误,违规变更停车场设计、对挡水围墙建设质量把关不严,造成重大人员伤亡的责任事件。从安全情报视角出发,该事件出现多环节安全情报失误与安全行为失败致使自然灾害后果加重的现象,是安全情报失误导致安全事件防控失败的典型案例。

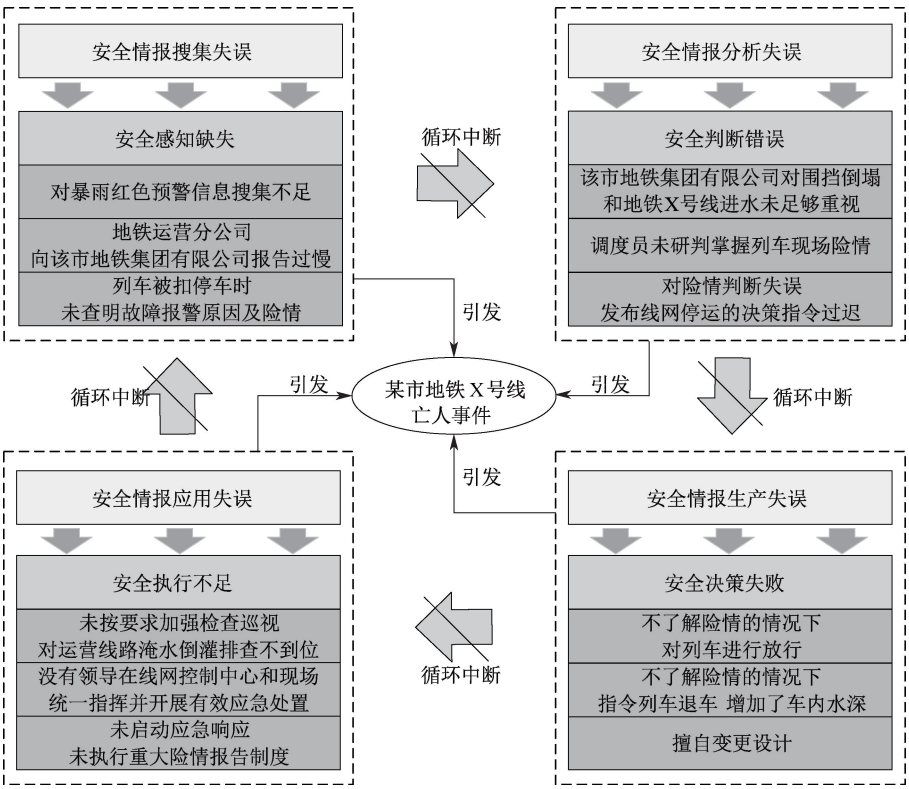


图 5 基于安全情报视域下的安全事件致因模型的某市地铁 X 号线安全事件分析

Fig. 5 Safety and security incident analysis of a city metro line X based on safety and security incident causation model from a safety and security intelligence perspective

4 结 论

1) 安全情报循环与安全行为循环具有对应关系,具体包括安全情报搜集对应安全感知,安全情报分析对应安全判断,安全情报生产对应安全决策,安全情报应用对应安全执行。

2) 在安全情报循环过程中有可能存在安全情报失误问题,主要包括安全情报搜集失误、安全情报分析失误、安全情报生产失误和安全情报应用失误。

3) 安全情报失误会导致安全行为循环失去安全情报的支持,出现安全感知能力降低、安全判断失去客观评价、安全决策缺乏支撑和安全执行效率低下等问题,最终会导致安全事件的发生。

参 考 文 献

[1] 光夏磊,王秉,吴超,等. 大数据环境下情报主导的安全管理模式研究[J]. 情报杂志,2020,39(9):157-162,149.
GUANG Xialei, WANG Bing, WU Chao, et al. Intelligence-led safety & security management (ILSM) model in a big data environment[J]. Journal of Intelligence,2020,39(9):157-162,149.

[2] 王秉. 安全 4.0 时代的重大安全科学问题展望[J]. 灾害学,2022,37(2):6-11.

WANG Bing. Prospect on major issues of safetyandsecurity science in the age of safety & security 4. 0 era[J]. Journal of Catastrophology, 2022,37(2):6-11.

[3] 李杰,伊宏艳,李乃文. 我国事故致因研究团队与热点主题研究[J]. 中国安全科学学报,2022,32(7):20-27.
LI Jie, YI Hongyan, LI Naiwen. Investigation on research team and hot topics of accident causation in China[J]. China Safety Science Journal,2022,32(7):20-27.

[4] WANG Bing, WU Chao. Safety informatics as a new, promising and sustainable area of safety science in the information age[J]. Journal of Cleaner Production,2020,252:DOI:10. 1016/j. jclepro. 2019. 119852.

[5] WU Chao, HUANG Lang. A new accident causation model based on information flow and its application in Tianjin port fire and explosion accident[J]. Reliability Engineering and System Safety,2019, 182:73-85.

[6] 李思贤,吴超,王秉. 多级安全信息不对称所致事故模式研究[J]. 中国安全科学学报,2017,27(7):18-23.
LI Sixian, WU Chao, WANG Bing. Study on model for accident resulting from multilevel safety information asymmetry[J]. China Safety Science Journal,2017,27(7):18-23.

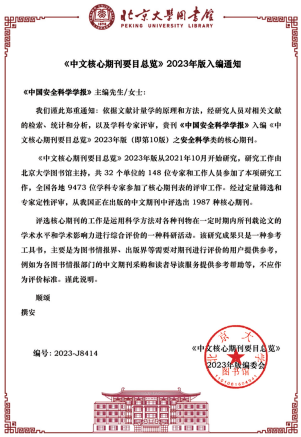
[7] 叶鹰. 情报学基础教程(第 3 版)[M]. 北京:科学出版社, 2018:176-184.

[8] 李燕峰,刘亚男. 高等教育数据治理领域的区块链融合研究[J]. 中国教育信息化,2021,27 (17): 60-66.

[9] 陈彬,高峰. WSR 视域下灾害应急情报失误成因及对策研究[J]. 竞争情报,2022,18(5):14-22.
CHEN Bin, GAO Feng. Research on the causes and countermeasures of disaster emergency intelligence failure from the perspective of WSR[J]. Competitive Intelligence,2022,18(5):14-22.

作者简介: 王渊洁 (1996—),男,陕西渭南人,博士研究生,主要研究方向为安全(应急)情报学、国家安全学与安全科学基础理论。E-mail:jay_wangyj@163. com。

《中国安全科学学报》再次入编“北大中文核心期刊”



《中文核心期刊要目总览》2023年版入编通知

《中国安全科学学报》主编先生/女士:

我们谨此郑重通知:依据文献计量学的原理和方法,经研究人员对相关文献的检索、统计和分析,以及学科专家评审,贵刊《中国安全科学学报》入编《中文核心期刊要目总览》2023年版(即第10版)之安全科学类的核心期刊。

《中文核心期刊要目总览》2023年版从2021年10月开始研究,研究工作由北京大学图书馆主持,共32个单位的148位专家和工作人员参加了本项研究工作,全国各地9473位学科专家参加了核心期刊表的评审工作。经过定量筛选和专家定性评审,从我国正在出版的中文期刊中评选出1987种核心期刊。

评选核心期刊的工作是运用科学方法对各种刊物在一定时期内所刊载论文的学术水平和学术影响力进行综合评价的一种科研活动。该研究成果只是一种参考工具书,主要是为图书馆报界、出版界等需要对期刊进行评价的用户提供参考,例如为各图书馆报部门的中文期刊采购和读者导读服务提供参考帮助等,不应作为评价标准。谨此说明。

顺颂

撰安

编号:2023-J8414

《中文核心期刊要目总览》2023年版编委会

依据文献计量学的原理和方法,经研究人员对相关文献的检索、统计和分析,以及学科专家评审,《中国安全科学学报》入编《中文核心期刊要目总览》2023 年版(即第 10 版)之“安全科学”类的核心期刊。