Modern Management 现代管理, 2025, 15(1), 71-75
Published Online January 2025 in Hans. https://www.hanspub.org/journal/mm
https://doi.org/10.12677/mm.2025.151011

Hans汉斯

“以分析为中心”的情报分析方法在数据安全风险评估中的应用研究

范　晓，于海燕

扬州大学社会发展学院，江苏　扬州

收稿日期：2024年11月11日；录用日期：2024年12月3日；发布日期：2025年1月10日

摘　要

有效的风险评估高度依赖于对风险信息的准确判断与分析，文章通过对“以分析为中心”的情报分析方法的概述，从明确数据安全风险、数据的脆弱性分析和风险影响分析评估三个维度探讨其应用在数据安全风险评估中的优势与价值。采用“分析为中心”的情报方法对数据安全风险信息进行多维度全过程综合研判，有助于提高数据风险评估的准确性和可靠性，将该方法应用于数据安全研究具有指导意义，但其具体效用仍需在实践中加以检验。

关键词

分析为中心，情报分析，数据安全，风险评估

Research on the Application of “Analysis Centered” Intelligence Analysis Method in Data Security Risk Assessment

Xiao Fan, Haiyan Yu

The College of Social Sciences, Yangzhou University, Yangzhou Jiangsu

Received: Nov. 11th, 2024; accepted: Dec. 3rd, 2024; published: Jan. 10th, 2025

Abstract

Effective risk assessment is highly dependent on the accurate judgment and analysis of risk information. Through the overview of the “analysis-centered” intelligence analysis method, the advantages and values of this analysis method in data security risk assessment are discussed from the three dimensions of defining data security risks, data vulnerability analysis and risk impact

文章引用: 范晓, 于海燕. “以分析为中心”的情报分析方法在数据安全风险评估中的应用研究[J]. 现代管理, 2025, 15(1): 71-75. DOI: 10.12677/mm.2025.151011

analysis and assessment. The "analysis-centered" intelligence analysis method improves the accuracy and reliability of data risk assessment through multi-dimensional and whole-process comprehensive research and judgment of data security risk information. The application of this method to data security research is of guiding significance, but its specific utility still needs to be tested in practice.

Keywords

Analysis-Centered, Intelligence Analysis, Data Security, Risk Assessment

1. 引言

随着数据共享热潮和大数据时代的到来，数据面对的安全风险愈发多元、复杂，能否始终确保数据作为助力经济社会发展的正面因素，规避因为全世界信息安全环境变化带来的数据风险隐患，是国家数据安全保障情报工作的重要关切。个人、组织或者社会面对数据安全风险所做出的不同决策或行动的直接原因在于其对风险信息的分析、评估与判断。在有限的信息情报中如何科学、准确、有效地评估数据安全风险，风险情报信息的来源、内容和分析方法至关重要。本文将基于“分析为中心”的情报分析方法探讨分析其对于数据安全风险评估的意义。

2. “以分析为中心”的情报分析方法概述

情报收集和分析是国家信息安全决策的基础，其本质是通过强化扩大事物发展的积极面同时最大程度上遏制住消极倾向，进而为决策者做出最优选择、规划未来走向提供方案和指南。一般而言，“分析为中心”的情报方法是“‘情报周期’或‘情报过程’(Intelligence Circle/Intelligence Process)在情报分析中的实践，可以视为将信息转化为真正的‘情报’的过程”[1]。

一方面，“以分析为中心”的情报分析方法是一套系统化流程，与情报活动的不同要素之间是相互关联、紧密联系的，只是着重强调“分析”的重要性，对应到传统的“方向、收集、处理和传递”的情报周期中，其注重的是情报收集与处理的过程；另一方面，这种情报方法“将协同的方法整合到情报过程诸方面，即与情报议题相关主体的协同参与：搜集全源情报(All-Source Intelligence)之间的协同获取、情报分析人员之间的情报沟通、情报使用者同分析者之间的反馈”[2]，强调所有利益相关者(用户、分析和搜集人员等)都是情报分析过程的组成部分。在多元参与协同的框架之中，通过不同领域不同学科的知识整合与共享，确保团队获得对风险有全面理解和认知，形成统一的行动方案，共同应对复杂的风险挑战。

3. “以分析为中心”的情报分析方法在数据安全风险评估中的适用性

“以分析为中心”的情报分析方法之所以可以应用在数据安全风险评估中，主要基于以下几个方面的原因：

首先，“以分析为中心”的情报分析方法强调对信息的深入剖析和解读，这与数据安全风险评估的核心理念相契合，数据安全风险评估的本质是对数据资产可能面临的威胁和风险进行系统性评估，而分析则是实现这一目标的关键手段。其次，在“以分析为中心”的情报分析方法中，数据处理与分析技术扮演着重要角色，同样地，在数据安全风险评估中，也需要运用先进的数据分析技术来解读和处理海量

数据资产，以帮助评估人员快速识别出潜在的风险点，提高评估效率和准确性。最后，情报分析中的多元参与协同对于数据安全风险评估也不可或缺，通过多元协同体系下的预测分析与情景构建，模拟不同的数据安全事件场景并制定具有针对性的防护策略，有助于提升数据安全风险评估的实用性和可操作性。

总而言之，将“分析为中心”的情报方法应用于数据安全风险评估，深入分析风险情报信息的来源、内容、业务场景等要素，有利于实现对数据安全风险的科学、全面、准确评估，为数据安全防护提供了新的思路和方法。

4. 运用“以分析为中心”的情报分析方法研判数据安全风险

风险分析的原理主要是“通过资产识别、脆弱性识别及威胁识别，分别计算出威胁造成损失的严重程度以及该安全事件发生的可能性，然后利用损失严重程度与事件发生的可能性得到风险值，最后赋予风险等级”[3]。在数据安全风险分析的框架中，基于可获取的风险情报，“以分析为中心”的情报分析方法以明确数据安全风险、数据的脆弱性分析以及风险影响分析评估作为核心要素展开，试图用一种体系化、综合化的方式识别、定义、量化风险的不确定性，评估所得出的结果用于预防、规避或分担风险。

4.1. 明确数据安全风险

在风险评估中，“明确数据安全风险”是数据安全风险评估的首要步骤，根据“分析为中心”的情报分析流程，安全问题框定要根植于同数据安全风险相关的所有领域的信息搜集，从而基于可获得的情报确定风险的威胁性。首先针对数据的特点对可能会遭受到安全问题的数据目标及其重要性等方面进行分析；其次需要对潜在的风险进行持续监控，定期更新风险信息，全面拓展与潜在威胁源头有关的详细风险情况，包括潜在风险的性质、可能性、规律性、影响范围，以及对各类日常数据与信息活动的存档、对数据安全行为的信息的搜集等；然后在对情报进行筛查、过滤、处理的过程中如果遇到新的问题，可以通过重复上一步的流程开展新一轮的收集与补充信息，或者重新界定目标并对风险评估结果进行重新审视和调整；最后通过有效的信息反馈机制，识别出数据在收集、存储、处理、传输等各个环节中可能存在的风险点，基于对威胁来源、动机、能力等方面的综合分析判断风险与威胁的可能性。

4.2. 数据的脆弱性分析

在界定好“风险”的基础上，数据的脆弱性分析是数据风险评估的核心。在数据安全风险中，所谓脆弱性，不仅包括各类数据攻击对给定目标发生损害，还包括一定时间内由于数据自身特性而导致数据不可用不可读的概率，综合考虑安全技术、法律政策、主体行为等多种因素，更全面地把握风险的全貌。

首先，对于数据脆弱性的分析应当将可搜集到的不同领域的信息进行综合，识别其中涉及的各学科领域的交叉点，进而整合不同领域的专家深入研究；其次在交叉学科的相互协调与合作中，建立定期沟通和反馈机制，在批判性交流中确保合作研究的顺利进行和信息的及时分享，通过历史与当下搜集的全源情报共同研判可能遭受到的数据风险，尽可能对不同风险的种类及时间、空间分布规律进行罗列总结，根据威胁的形式确定用于分析风险影响的参考要素；最后对分析结果进行评估，由于信息自身固有的不确定性，对于缺乏证据的安全威胁要进一步搜集信息进行验证。

4.3. 风险影响分析评估

风险影响评估主要分析的是数据安全风险可能影响的预期程度、主体范围与时空范围以及可能影响的其他事件，是情报分析过程中需关注的焦点。对数据安全风险影响的分析具体包括：评估数据被篡改、删除或泄露的数量、严重性与敏感性，分析数据安全事件对物理设施(如服务器、数据中心等)的破坏程度，计算因此导致的直接和间接经济损失(如罚款、赔偿、业务中断等)，评估数据安全事件发生后的影响所持

续的时间和潜在的长期后果等。

首先，对风险结果的分析建立在明确数据安全事件类型的基础之上，针对外来攻击，其通常具有烈性的影响但可能是短暂的，需要分析攻击手段、攻击来源以及可能的攻击频率；而内在威胁往往具有长期积累的特点，可能来自内部人员、系统漏洞等，需要分析威胁的持续性、隐蔽性以及可能造成的长期损害。其次，评估数据安全事件一旦发生后其影响持续的时间，包括直接影响的持续时间和潜在影响的延迟时间，以及数据安全事件波及扩散的地域范围、系统范围或数据范围。此外，还应该预估对经济活动、政策制定、公众信任、社会稳定、国际关系等其他相关影响，防止其消极影响再度波及数据安全。最后根据明确的损失评估标准，“采用资产价值结合脆弱性严重程度的综合评价方法判断安全事件(风险)影响程度，采用威胁能力结合脆弱性严重程度的综合评价方法判断安全事件发生的可能性，最终根据影响程度和可能性判断风险区间(风险值)”[4]。通过综合不同的损失程度进行权重分析形成风险评估结果报告，帮助决策者更直观地了解数据安全风险的严重性和紧迫性，从而制定高效的应对策略和措施。

5. 运用“以分析为中心”情报方法研判数据安全风险的实施要略

总的来看，以“分析为中心”的情报方法的应用对数据安全风险评估的意义在于：风险往往并不是相互独立的，一个风险往往会引发不同类型的次生风险[5]，通过对情报信息的共享与全面分析，从“风险链”的角度识别数据流转中的关键环节和薄弱环节、分析各环节之间的因果关系和连锁反应、评估风险链整体对数据安全的影响程度，进而从防与控两个方面提升数据安全风险治理的效能，为深入理解和应对数据安全挑战提供了有效方法。在实践层面，运用“以分析为中心”情报方法分析数据安全风险也需要考量以下几个方面。

5.1. 信息共享与保密相平衡

在数据安全领域，信息共享与保密之间的平衡是一个永恒的议题，数据安全与数据开放已经成为一组对立统一的矛盾[6]。数据安全工作强调的是信息安全保密，而“以分析为中心”的情报分析方法重视共同参与、相互协作和资源共享，将其应用于数据安全领域意味着我们必须在信息共享和安全保密之间找到一个平衡点。在推动信息共享的同时，我们必须建立健全的数据安全治理机制，规范情报机构和分析人员的行为，增强不同学科、不同专业、不同机构人员之间的信任感，及时、公正地解决利益争端或观点冲突，在确保敏感信息不被泄露的前提下，积极推动风险情报信息共享，以实现数据安全风险分析的全面和高效。

5.2. 数据安全高新技术支撑

数据安全风险评估需要大量的数据和信息，不仅风险信息的收集、存储、处理和分析需要依靠强大的信息系统来支撑，情报分析的高效应用、顺畅运作也必须依靠高新信息技术，利用数据挖掘、算法模型等为风险之间的关联和趋势评估提供科学、精准的数据支撑。在数据安全风险分析评估工作中，特别是针对新兴的复杂的不确定的数据安全风险，既要采用先进的技术手段如加密技术、访问控制、审计日志等，确保敏感数据在传输和存储等过程中的安全合规，又要借助具备高效的数据处理能力、强大的存储能力和灵活的扩展能力的信息系统满足情报分析工作的各种需求。

5.3. 情报分析人才智力支持

情报分析人才在构建数据风险评估体系中扮演着非常重要的角色。一方面，他们需要具备全面的专业知识和分析能力，能够准确、迅速地处理和分析各种风险信息；另一方面，风险评估要求其与决策者、监管机构、行动用户、信息搜集人员等各方进行有效沟通，协调各方确保需求的准确传递和反馈，不断

优化分析方法和流程，共同推进风险评估工作的顺利开展。总而言之，建立一支高素质的情报分析团队，对于维持数据安全风险评估周期运行的稳定性、可靠性、连续性具有举足轻重的作用。

5.4. 理论性与实操性相结合

通过风险情报信息分析建立的数据安全风险评估模型不仅要具有理论价值，还要能够在实际操作中发挥作用。在构建评估模型时，首先要以理论为基础，“网络威胁越是复杂，越要对情报分析方法进行融合”[7]，“以分析为中心”的情报分析方法为深入剖析数据安全风险提供了科学的方法论和清晰的框架，与此同时，还要充分考虑实操性，数据的迭代升级增加了风险情报分析的难度，在评估过程中要不断根据实际操作情况持续反复进行风险分析，对评估模型进行迭代优化，保证最终确定的可行性方法必须是直观的、可用的、可操作的，增强评估结果的实用性和影响力。

6. 总结

数据安全正逐步成为未来国际竞争的重要内容，如何应对数据安全风险和由此带来的消极影响，关系到我国经济社会发展的安全与稳定。在复杂的信息环境背景下，引入“以分析为中心”的情报分析方法，对数据安全风险进行系统的、动态的分析和评估，有利于把握其防控重点和策略手段，对未来我国数据安全领域的政策制定、风险应对具有重要的现实意义，未来可通过具体实践对该方法在数据安全风险评估中的适用范围及效用价值进行深入研究与检验。

基金项目

国家社会科学基金项目“档案数据安全治理”(项目编号：21BTQ093)。

参考文献

[1] 张力伟, 赵吉, 李慧杰. “分析为中心”的情报方法及其对恐怖主义风险评估的启示[J]. 情报杂志, 2021, 40(2): 83-89.

[2] Frini, A. and Boury-Brisset, A.C. (2011) An Intelligence Process Model Based on a Collaborative Approach. Defence Research and Development Canada.

[3] 宋璟, 邸丽清, 杨光, 都婧. 新时代下数据安全风险评估工作的思考[J]. 中国信息安全, 2021(9): 62-65.

[4] 杨韬, 刘曦泽, 高红静. 数据安全风险评估方法和实践应用研究[J]. 保密科学技术, 2023(7): 9-15.

[5] Willis, H.H., Morral, A.R., Kelly, T.K., *et al*. (2005) Estimating Terrorism Risk. RAND Corporation, 7-8.

[6] 唐超, 钟灿涛. 数据汇集中的安全风险评估研究[J]. 保密科学技术, 2019(6): 9-15.

[7] 陈明, 汤文峤. 智能化条件下网络威胁情报分析研究[J]. 情报杂志, 2023, 42(3): 17-23+33.