

政府开放数据的国家安全风险评估模型研究

王标^{1,2}, 刘兴洋², 许卡^{1,3}, 刘汪洋^{1,3}, 王克楠², 夏宇清²

(1. 提升政府治理能力大数据应用技术国家工程实验室, 贵州 贵阳 550022;

2. 国际关系学院, 北京 100091;

3. 中电科大数据研究院有限公司, 贵州 贵阳 550022)

摘要: 政府开放数据作为国家和社会发展重要战略资源, 蕴含着巨大价值, 但我国在政府开放数据的安全风险评估方面缺乏标准, 国家数据安全面临风险。借鉴信息安全风险评估理论, 以国家安全资产、开放数据脆弱性和安全威胁作为主要安全风险要素, 构建政府开放数据的安全风险评估模型, 利用层次分析法和模糊综合评价法对政府开放数据的安全风险进行量化评估, 并通过实例验证模型的有效性。

关键词: 政府开放数据; 风险评估模型; 层次分析法; 模糊综合评价法

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020077

Research on national security risk assessment model of open government data

WANG Biao^{1,2}, LIU Xingyang², XU Ka^{1,3}, LIU Wangyang^{1,3}, WANG Kenan², XIA Yuqing²

1. Big Data Application on Improving Government Governance Capabilities National Engineering Laboratory, Guiyang 550022, China

2. University of International Relations, Beijing 100091, China

3. CETC Big Data Research Institute CO., LTD., Guiyang 550022, China

Abstract: As an important strategic resource of national and social development, the government open data is of great value. But China lack standards in the security risk assessment of government open data, especially the security of national data is at risk. Based on the theory of information security risk assessment, a government open data security risk assessment model was constructed with national security assets, open data vulnerability and security threat as the main security risk elements. Analytic hierarchy process (AHP) and fuzzy comprehensive evaluation methods were used to quantify and evaluate the security risks of government open data, and the validity of the model is verified by example.

Key words: government open data, risk assessment model, AHP, fuzzy comprehensive evaluation method

收稿日期: 2020-07-14; 修回日期: 2020-09-23

通信作者: 王克楠, wkn@uir.edu.cn

基金项目: 提升政府治理能力大数据应用技术国家工程实验室开放基金项目 (W-2018013)

Foundation Item: Big Data Application on Improving Government Governance Capabilities National Engineering Laboratory (W-2018013)

论文引用格式: 王标, 刘兴洋, 许卡, 等. 政府开放数据的国家安全风险评估模型研究[J]. 网络与信息安全学报, 2020, 6(6): 80-87.

WANG B, LIU X Y, XU K, et al. Research on national security risk assessment model of open government data[J]. Chinese Journal of Network and Information Security, 2020, 6(6): 80-87.

1 引言

当前我国政府数据开放形势较为迫切，政府数据开放理念逐渐成熟，政府数据开放已成为政府机构合作的重要内容，“开放数据晴雨表”“开放数据指数”已成为衡量开放政府的重要指标，在数据开放领域，我国面临较大压力。促进政府信息再利用，提升政府公共服务质量、强化协作，服务于政府施政进而实现“人民对美好生活的向往”，都对我国政府数据开放提出了新要求。

政府开放数据具有巨大的经济价值、社会价值和政治价值，是重要的国家基础战略资源^[1]。如果政府开放数据被恶意分析利用，可能威胁到国家安全，可以说政府开放数据的安全直接影响国家安全和社会稳定。目前，我国在政府数据开放工作方面已有一定成效，但仍不完善，政府数据开放在开放内容、开放范围、数据使用门槛和数据安全风险评估方面缺乏相应标准，存在安全隐患，甚至直接威胁国家安全。因此，有必要开展政府数据开放流程梳理、国家安全风险评估等工作。

本文借鉴信息安全风险评估理论，构建政府开放数据的国家安全风险评估模型，对政府开放数据的国家安全风险进行量化评估，为政府数据开放工作提供前置风险评估，具有现实意义。最后，以上海市交通委员会公开的“上海市桥梁点数据”进行实例分析，对风险评估结果进行有效性检验。

2 构建政府开放数据的安全风险评估指标体系

2.1 风险评估步骤

信息安全风险评估是信息系统安全的基础性工作，合理的安全风险评估能够帮助用户了解信息系统的安全现状，认清信息系统面临的安全威胁，从而提出科学有效的安全维护策略。目前国内对于信息安全风险评估已有比较成熟的研究，风险评估的方法和流程已经有了相对完善的框架，能够使风险评估工作有效地发挥作用^[2]。

借鉴信息安全风险评估理论^[3]，政府开放数

据的国家安全风险评估主要步骤包括：风险评估准备、风险因素评估、风险确定、风险评价及风险控制等。

2.2 风险评估流程

针对政府开放数据本身的国家安全风险评估，与信息系统的的社会安全风险不同，将不考虑数据的载体——信息系统的安全状况，只根据政府开放数据特点，对数据本身进行国家安全风险评估，评估流程如图1所示。

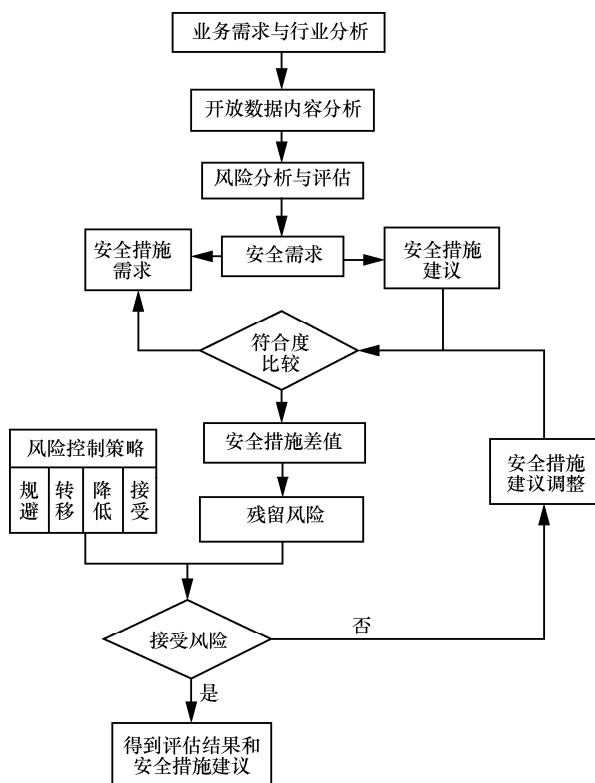


图1 政府开放数据国家安全风险评估流程
Figure 1 The national security risk assessment process of government open data

(1) 业务需求与行业分析

在对不同的开放数据进行风险评估时，要考虑数据开放部门的业务需求以及数据涉及的行业，一般认为，不同的部门安全需求的侧重点不同。例如，交通部门公布的道路、桥梁等信息多和国家的基础设施建设相关，对带来的国家安全风险比较重视；审计部门公布的从业资格名单、企业经营许可证信息等，多与个人和企业的权益相关，风险评估重点应为个人和其他组织合法权益损失的风险。

(2) 风险分析与评估

针对开放数据本身存在的弱点, 开放数据面临的危险主要有篡改、挖掘分析和关联分析。对开放数据进行篡改, 改变数据原有信息, 可能带来更大的安全风险; 对开放数据进行挖掘分析, 可能会挖掘到更有价值的信息从而对国家安全资源造成损害; 对数据进行关联分析, 将多个不同数据源数据的相关属性组合后, 由于数据间的关联性可能得到损害国家安全资产的敏感信息。

(3) 安全措施

安全措施的制定应该充分考虑开放数据面临的安全威胁和数据本身的脆弱性。数据的脆弱性来源于数据内容的重要度、完整度和保密程度。重要度体现了开放数据的影响程度和经济价值, 完整度指开放数据中包含信息的完整程度, 保密程度体现了开放数据的保密等级。安全措施应降低因数据弱点被利用而产生的安全风险。

2.3 政府开放数据国家安全风险评估的安全要素分析

在信息安全评估相关标准中, 以资产、威胁及脆弱性评估为核心, 安全风险与信息系统的资产、面临的威胁、自身的脆弱性有关, 因此可以说信息安全风险是关于资产、威胁与脆弱性的函数, 可以表示为 $R(A, T, V)$, 其中, R 代表风险计算函数, A 代表资产, T 代表威胁, V 代表脆弱性。

每个要素有各自的属性, 资产的属性是资产价值, 脆弱性的属性是资产弱点的严重程度, 威胁的属性是威胁主体、威胁方法、影响对象、动机等^[4]。要素之间的关系是威胁利用系统的脆弱性使安全事件的发生变为可能, 系统中存在脆弱性使资产具有损失的风险, 因此风险分析原理如图2所示。

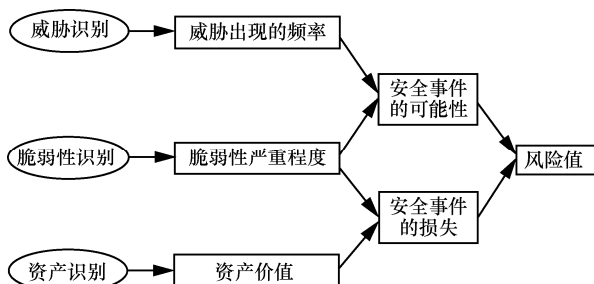


图2 风险分析原理

Figure 2 Schematic diagram of risk analysis

对于政府开放数据的国家安全风险评估来说, 需要评估的是政府开放数据本身给国家安全带来的风险, 借鉴信息安全风险评估理论, 即评估的是政府开放数据本身面临的威胁和漏洞会给国家安全资产带来的损失程度。可以认为, 对于政府数据而言, 资产的价值就是国家安全资产, 由此, 以国家安全资产、开放数据脆弱性和开放数据面临的安全威胁为主要安全风险要素, 构建政府开放数据国家安全风险评估要素模型。政府开放数据面临的国家安全风险是关于国家安全资产, 开放数据脆弱性和安全威胁的基本函数, 可以表示为

$$R(S, T, V) \quad (1)$$

其中, R 表示风险计算函数; S 表示国家安全资产; T 表示安全威胁; V 表示开放数据脆弱性。构建的政府开放数据国家安全风险评估要素模型如图3所示。

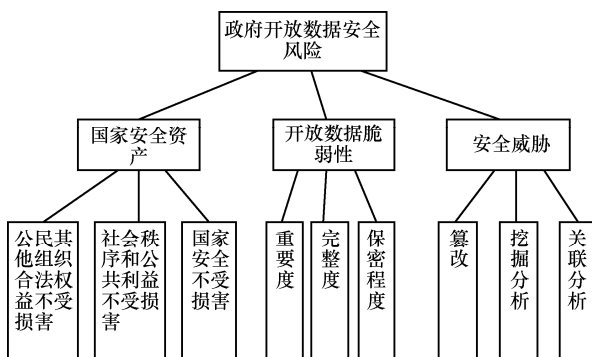


图3 政府开放数据国家安全风险评估要素模型

Figure 3 The model of government open data national security risk assessment elements

(1) 国家安全资产

国家安全资产是国家的基本利益, 借鉴《信息安全等级保护管理办法》, 为国家安全资产包括: 公民和其他组织合法权益不受损害, 社会秩序和公共利益不受损害, 国家安全不受损害。

(2) 开放数据脆弱性

脆弱性是指政府开放数据本身能够被安全威胁利用的漏洞或弱点, 脆弱性本身不会带来国家安全资产的损失, 只是为安全事件的发生提供了条件。

对于政府开放数据本身来说, 数据的脆弱性来源于数据内容的重要度、完整度和保密程度。

重要度体现了开放数据的影响程度和经济价值，完整度指开放数据中包含信息的完整程度，保密程度体现了开放数据的保密等级。

(3) 安全威胁

在政府开放数据国家安全风险评估模型中，安全威胁利用开放数据的脆弱性给国家安全资产造成损失，对于开放数据本身面临的安全威胁，包括篡改、挖掘分析和关联分析。对数据进行篡改，改变数据原有信息，可能带来安全风险；对数据进行分析，可能得到更有价值的信息，从而损害国家安全资源；对数据进行关联挖掘，将多个不同数据源数据的相关属性组合起来后，由于数据间的关联性可能会得到损害国家安全资产的敏感信息。

2.4 构建政府开放数据国家安全风险评估模型基础

为实现国家安全风险量化计算，将层次分析法(AHP, analytic hierarchy process)和模糊综合评价法(fuzzy comprehensive evaluation method)结合起来，对风险要素进行量化分析。

(1) AHP

AHP 是一种定性与定量相结合的多目标决策分析方法，其特点是判断者依据知识和经验将评价因素量化^[5]。该方法将定性分析和定量分析结合起来处理各评价因素，具有简洁灵活的特点，被广泛应用于尚无统一度量标尺问题的分析方面。其优点在于能充分考虑复杂问题中的各种因素关系。在实际使用过程中，基本思想是所要解决的复杂问题纵向分解为若干个层次，多数情况下是3层。然后按照由下到上的顺序，在较低层上通过各元素之间两两比较的方式，计算出该层的每个元素相对于上一层的权重，最后结合上一层的权重，计算出各因素对最高层的相对权重。

(2) 模糊综合评价法

模糊综合评价法^[6]是一种基于模糊数学的综合评价方法，该方法利用隶属度理论将定性评价转为定量评价。

模糊综合评价法将定性和定量因素相结合，可以对多种因素影响的对象做出一个综合的评价。它具有结果清晰、系统性强等特点，能较好地解决模糊的、难以量化的问题，适合各种非确

定性问题的解决。利用模糊综合评价法，可以在很大程度上弥补层次分析法在量化上的不足。

2.5 政府开放数据的国家安全风险计算模型

利用构建的政府开放数据的国家安全风险评估要素，提出基于 AHP 和模糊综合评价法的政府开放数据国家安全风险评估方法，可以对某一开放的政府数据进行国家安全风险评估，判断数据的国家安全风险等级。

(1) 风险评估指标体系及安全要素权重值确认

政府开放数据安全风险评估指标体系如图4所示。

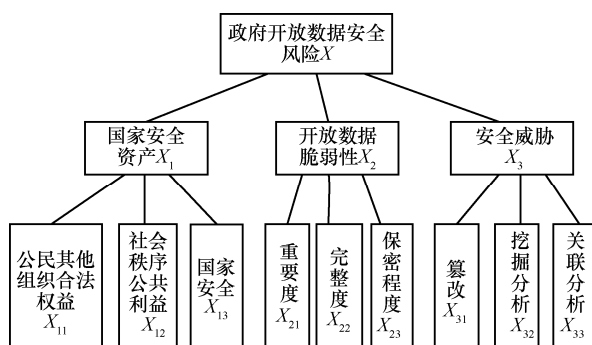


图4 政府开放数据安全风险评估指标体系
Figure 4 The government open data security risk assessment index system

根据评估指标体系，对安全风险因素用1-9比例标度法构造判断矩阵，矩阵的数据由两个评价指标的相对重要性确定，数值来源于咨询专家。在赋值的过程中要考虑到数据的开放部门和涉及的行业。

对于一级风险评价指标集 $\{X_1, X_2, X_3\}$ 构建判断矩阵 A ；

对于二级风险评价指标集 $\{X_{11}, X_{12}, X_{13}\}$ 构建判断矩阵 A_1 ；

对于二级风险评价指标集 $\{X_{21}, X_{22}, X_{23}\}$ 构建判断矩阵 A_2 ；

对于二级风险评价指标集 $\{X_{31}, X_{32}, X_{33}\}$ 构建判断矩阵 A_3 ；

然后，根据 AHP 评价指标权重计算公式，分别计算各个评价指标的权重，其中一级风险评价指标对于 X 的权值为

$$W=\{w_1, w_2, w_3\} \quad (2)$$

二级风险评价指标对于 X_1, X_2, X_3 的权值分

别为

$$\begin{aligned} W_1 &= \{w_{11}, w_{12}, w_{13}\} \\ W_2 &= \{w_{21}, w_{22}, w_{23}\} \\ W_3 &= \{w_{31}, w_{32}, w_{33}\} \end{aligned} \quad (3)$$

对计算出的结构进行一致性检验, 如果通过检验, 利用下式计算二级风险评价指标对 X 的权值。

$$X_{ij} = w_i \cdot w_{ij} \quad (4)$$

计算结果表示各风险安全因素对政府开放数据安全的相对影响力。

(2) 安全风险因素等级判定

利用模糊综合评价法, 根据需要评估的政府开放数据, 对构建的二级风险评价指标进行评判, 不同的开放数据的评判结果并不相同, 评判结果分为 5 个安全风险等级, 请多名专家分别进行评判, 评判等级如表 1 所示。

表 1 安全风险等级
Table 1 Security risk level

等级	风险程度	描述
5	高	安全风险严重, 数据不宜开放
4	较高	安全风险较为严重, 数据需要有条件开放
3	中	安全风险适中, 数据处理后开放
2	较低	安全风险较低, 对数据部分处理后开放
1	低	安全风险低, 为可接受风险, 可以直接开放

根据专家的评判结果, 分别对安全风险因素 X_1, X_2, X_3 构建模糊关系矩阵 R_i ($i=1, 2, 3$), 并利用上一步计算出的各指标权重 W_i ($i=1, 2, 3$), 使用式(5), 计算单层次评判结果。

$$B_i = W_i \circ R_i \quad (5)$$

把得到的单层次评估结果, 利用式(6)得到总的模糊关系矩阵 R 。

$$R = \begin{bmatrix} B_1 \\ \vdots \\ B_n \end{bmatrix} = \begin{bmatrix} W_1 R_1 \\ \vdots \\ W_n R_n \end{bmatrix} \quad (6)$$

利用式(7)计算总的综合模糊评价结果。

$$B = W \circ R \quad (7)$$

最后计算得到的 B 值是一个数据集, 本文采用最大隶属度原则来判断评估的政府开放数据的安全风险等级。

(3) 安全策略制定

经前面两步计算, 可以分析出要素的相对风险程度和政府开放数据的安全风险等级。通过确认风险等级, 可以提高对政府开放数据安全风险的认识, 并采取相应的处理措施; 确定风险要素的相对风险程度, 可以更加有针对性地提出改进的安全策略, 降低政府开放数据的安全风险。

如果计算结果显示, 个人的合法权益相对重要, 那么就可以对开放的政府数据进行一定程度上的脱敏处理, 如去掉姓名、身份证号等敏感字段; 如果计算结果显示遭到篡改的影响力较大, 则可以对数据进行数字水印等加密处理; 如果计算结果显示数据的保密程度影响较大, 那么就需要对开放数据进行脱密处理, 降低数据的保密程度。

3 实例分析

以上海市交通委员会提供的“上海市桥梁点数据”作为风险评估对象进行实例分析, 依据提出的政府开放数据国家安全风险评估过程和风险评估模型, 对该数据进行国家安全风险评估。由于在不同时期、不同国家安全环境下有不同的安全风险评估标准, 为了更好地体现评估效果, 本次评估设定上海市面临的国家安全环境为中等国家安全风险, 面临恐怖袭击威胁和其他国家较为频繁的间谍活动。

3.1 数据安全风险评估流程

(1) 确认评估对象

对象是“上海市桥梁点数据”, 数据中包含桥梁名称、航道名称、离河口距离、总孔数、总长度、总宽度、通航孔数、通航孔净宽、梁底标高(米)、结构类型、类别、高水位净空等字段数据, 属于上海市的交通运输信息。

(2) 建立风险评估指标体系并计算影响因素权重

分别针对一级风险评价指标和二级风险评估指标构建判断矩阵 A 、 A_1 、 A_2 、 A_3 。

针对一级风险评价指标(国家安全资源 X_1 、数据弱点 X_2 、安全威胁 X_3)构建判断矩阵 A 。

$$A = \begin{bmatrix} 1 & 2 & \frac{3}{2} \\ \frac{1}{2} & 1 & \frac{2}{3} \\ \frac{2}{3} & \frac{3}{2} & 1 \end{bmatrix} \quad (8)$$

通过计算，得到 $W = \{w_1, w_2, w_3\} = \{0.460, 0.221, 0.319\}$ 。

针对二级风险评价指标（公民即其他组织合法权益 X_{11} 、社会秩序和公共利益 X_{12} 、国家安全 X_{13} ）构建判断矩阵 A_1 。

$$A_1 = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{4} \\ 2 & 1 & \frac{1}{2} \\ 4 & 2 & 1 \end{bmatrix} \quad (9)$$

通过计算，得到 $W_1 = \{w_{11}, w_{12}, w_{13}\} = \{0.143, 0.286, 0.571\}$ 。

针对二级风险评价指标（重要度 X_{21} 、完整度 X_{22} 、保密程度 X_{23} ）构建判断矩阵 A_2 。

$$A_2 = \begin{bmatrix} 1 & 1 & \frac{3}{2} \\ 1 & 1 & \frac{3}{2} \\ \frac{3}{2} & \frac{3}{2} & 1 \end{bmatrix} \quad (10)$$

通过计算，得到 $W_2 = \{w_{21}, w_{22}, w_{23}\} = \{0.375, 0.375, 0.250\}$ 。

针对二级风险评价指标（篡改 X_{31} 、挖掘分析 X_{32} 、关联分析 X_{33} ）构建判断矩阵 A_3 。

$$A_3 = \begin{bmatrix} 1 & \frac{1}{2} & \frac{2}{3} \\ 2 & 1 & \frac{3}{2} \\ \frac{3}{2} & \frac{2}{3} & 1 \end{bmatrix} \quad (11)$$

通过计算，得到 $W_3 = \{w_{31}, w_{32}, w_{33}\} = \{0.221, 0.460, 0.319\}$ 。

以上结果都可以满足一致性检验。

(3) 计算二级指标相对于 X 的相对权重并排序

利用下式计算各二级指标相对于 X 的相对权重。

$$x_{ij} = w_i \cdot w_{ij} \quad (12)$$

计算后对结果排序，二级指标权重及排序如表 2 所示。

表 2 二级指标权重及排序
Table 2 Weights and rankings of secondary indicators

二级指标	风险值权重	排序
X_{11}	0.065 78	8
X_{12}	0.131 56	3
X_{13}	0.262 66	1
X_{21}	0.082 875	5
X_{22}	0.082 875	5
X_{23}	0.055 25	9
X_{31}	0.070 499	7
X_{32}	0.146 74	2
X_{33}	0.101 761	4

(4) 安全风险因素等级判定

首先，分别对每一个二级风险因素的安全风险等级进行单独判定，为保证判定结果的科学性和准确性，邀请 20 位具有国家安全风险意识的风险评估领域、数据安全以及大数据领域具有丰富经验的专家进行评判。经过整理的评判结果如表 3 所示。

表 3 专家评判结果
Table 3 Expert evaluation results

二级指标	高	较高	中	较低	低
X_{11}				3	17
X_{12}				9	11
X_{13}			12	7	1
X_{21}			6	7	7
X_{22}			11	7	2
X_{23}				11	9
X_{31}				9	11
X_{32}			12	7	1
X_{33}			11	7	2

针对专家评判结果表中 X_{11} , X_{12} , X_{13} 的数据，可以得到针对这 3 项的模糊关系 R_1 ，对其构造模糊关系矩阵 R_1 。

$$R_1 = \begin{bmatrix} 0 & 0 & 0 & 3 & 17 \\ 0 & 0 & 0 & 9 & 11 \\ 0 & 0 & 12 & 7 & 1 \end{bmatrix} \quad (13)$$

对矩阵 R_1 进行归一化处理。

$$R_1 = \begin{bmatrix} 0 & 0 & 0 & 0.15 & 0.85 \\ 0 & 0 & 0 & 0.45 & 0.55 \\ 0 & 0 & 0.6 & 0.35 & 0.05 \end{bmatrix} \quad (14)$$

同理可得

$$R_2 = \begin{bmatrix} 0 & 0 & 0.30 & 0.35 & 0.35 \\ 0 & 0 & 0.55 & 0.35 & 0.10 \\ 0 & 0 & 0 & 0.55 & 0.45 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} 0 & 0 & 0 & 0.45 & 0.55 \\ 0 & 0 & 0.6 & 0.35 & 0.05 \\ 0 & 0 & 0.55 & 0.35 & 0.1 \end{bmatrix} \quad (15)$$

由式 $B_i = W_i \circ R_i$ 可计算出单层次的评价结果。

$$B_1 = W_1 \circ R_1 = [0, 0, 0.343, 0.35, 0.307]$$

$$B_2 = W_2 \circ R_2 = [0, 0, 0.319, 0.4, 0.281] \quad (16)$$

$$B_3 = W_3 \circ R_3 = [0, 0, 0.451, 0.372, 0.177]$$

将以上单层次评估结果综合起来, 可得到总的模糊关系矩阵 R 。

$$R = \begin{bmatrix} B_1 \\ \vdots \\ B_n \end{bmatrix} = \begin{bmatrix} W_1 \circ R_1 \\ \vdots \\ W_n \circ R_n \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0.343 & 0.350 & 0.307 \\ 0 & 0 & 0.319 & 0.400 & 0.281 \\ 0 & 0 & 0.451 & 0.372 & 0.177 \end{bmatrix} \quad (17)$$

最后计算得到总的模糊综合评价结果。

$$B = W \circ R = [0, 0, 0.372, 0.368, 0.260] \quad (18)$$

根据计算结果, 可以看到结果中的最大值“0.372”属于安全风险等级“中”, 因此, 根据最大隶属度原则, 认为该数据的安全风险评估等级为“中”。

(5) 国家安全风险分析及安全策略制定

1) 分析上面步骤计算得到的结果

首先, 由二级指标相对影响度排名可以看出, 排在前 3 位分别的是: 损失国家安全、挖掘分析威胁、社会秩序及公共利益损害, 说明这 3 个风险因子对此数据的安全影响最大。

其次, 由综合评价结果得知, 数据的安全风

险评估等级为“中”, 因此该数据需要经过部分处理后再进行开放。

2) 安全策略建议

根据得到的评估结果可知, 该数据的安全需求是降低数据对国家安全的损害、减少由于挖掘分析产生的安全威胁、减少数据对社会秩序及公共利益的损害。因此需要对该数据的某几个字段进行处理。

如果对该数据进行挖掘分析, 可以得到每个桥梁详细的建筑结构, 这属于公共基础设施信息; “航道名称”这个属性, 可以和“上海市航道信息”这一数据进行关联分析, 从而得到上海市包含航道和对应桥梁节点详细位置的战略地图。如果上述两个重要信息被恶意利用, 就会威胁我国国家和社会秩序。由此可得安全策略建议: 去掉“航道名称字段”避免由关联分析产生的威胁, 对桥梁的结构位置信息等不完全开放。

3.2 结果有效性检验

为检验通过政府开放数据安全风险评估模型进行评估后得到结果的有效性, 采取定性的分析方法对该数据进行分析, 将评估结果进行比较。通过对“上海市桥梁点”数据内容的分析, 数据记录了上海市所有桥梁节点的详细信息。

数据包含的内容属于交通信息和基础设施信息, 这些信息如果被恶意人员利用, 对数据信息深入挖掘分析和关联分析, 那么就有可能得到上海市关键桥梁节点的交通图, 并清楚掌握桥梁的结构、用途等, 如果根据得到的信息, 对上海市关键桥梁节点进行有针对、有目的性的恐怖袭击, 那么就会危害国家和社会稳定。另外, 上述分析具有发生的可能性, 若社会稳定, 其发生可能性并不高, 因此评价等级“中”在合理范围内。需要指出的是, 假设上海市当前恐怖袭击指数较高, 这一类数据的开放和使用是需要引起注意的。

这份数据并没有涉及个人和其他组织的利益, 不涉及机密, 那么保密度和损害个人、其他组织合法权益两项评价指标排名较为靠后, 这也验证了本文构建模型的合理性。

通过对两种分析结果的对比, 可验证所建立的政府开放数据国家安全风险评估模型的评估结果合理, 验证了评估模型和方法的客观性和有效性。

4 结束语

本文借鉴信息安全风险评估理论,构建了基于模糊评价法和层次分析法的政府开放数据的国家安全风险评估模型,以上海市交通委员会公开的“上海市桥梁点数据”进行实例分析,分析结果验证了模型的客观性和有效性。对政府开放数据的国家安全风险进行量化评估,为政府数据开放工作提供前置风险评估,对维护我国国家安全具有现实意义。但本文构建的模型中,各指标的选取均参照当前国家安全形势下较为成熟的国家安全体系研究。而国家安全体系并非一成不变,由于国家安全的内涵和外延不断丰富,国家安全的构成要素会不断调整,各要素包含的具体内容也会发生改变,模型中的各项指标应在未来及时调整更新以适应国家安全风险评估的最新需求。此外,信息安全风险评估和大数据领域专家的国家安全意识能力对于评估结果影响较显著。

参考文献:

- [1] 陶希东. 推进政府数据开放的思路与策略[J]. 中国国情国力, 2015, (12): 44-47.
TAO X D. Ideas and strategies for promoting government data opening[J]. China's National Conditions and Strength, 2015, (12): 44-47.
- [2] 张利, 彭建芬, 杜宇鸽, 等. 信息安全风险评估的综合评估方法综述[J]. 清华大学学报(自然科学版), 2012, 52(10): 1364-1369.
ZHANG L, PENG J F, DU Y G, et al. Information security risk assessment survey[J]. Tsinghua Univ (Science and Technology), 2012, 52(10): 1364-1369.
- [3] 王标, 胡勇, 戴宗坤. 风险评估要素关系模型的改进[J]. 四川大学学报(工程科学版), 2005(3): 110-114.
WANG B, HU Y, DAI Z K. Improvement of elements relationship model for risk assessment[J]. Journal of Sichuan University, 2005(3): 110-114.
- [4] 高亚楠, 刘丰, 陈永刚. 信息安全风险管理标准体系研究[J].

信息安全研究, 2018, 4(10): 928-933.

GAO Y N, LIU F, CHEN Y G. Summary of information security risk management standard system[J]. Journal of Information Security Research, 2018, 4(10): 928-933.

- [5] 王铁套, 王国营, 陈越. 基于模糊综合评价法的网络舆情预警模型[J]. 情报杂志, 2012, 31(6): 47-51, 58.

WANG T T, WANG G Y, CHEN Y. A model of online public opinion pre-warning based on fuzzy comprehensive evaluation[J]. Journal of Intelligence, 2012, 31(6): 47-51, 58.

- [6] 郭金玉, 张忠彬, 孙庆云. 层次分析法的研究与应用[J]. 中国安全科学学报, 2008(5): 148-153.

GUO J Y, ZHANG Z B, SUN Q Y. Study and applications of analytic hierarchy process[J]. China Safety Science Journal, 2008(5): 148-153.

[作者简介]



王标(1979—), 男, 浙江丽水人, 博士, 国际关系学院教授, 主要研究方向为信息安全。

刘兴洋(1992—), 男, 河北秦皇岛人, 国际关系学院工程师, 主要研究方向为信息安全。

许卡(1984—), 男, 湖南长沙人, 中电科大数据研究院有限公司高级工程师, 主要研究方向为网络安全与软件工程。

刘汪洋(1987—), 男, 四川德阳人, 博士, 中电科大数据研究院有限公司工程师, 主要研究方向为政府数据共享与开放。

王克楠(1961—), 男, 北京人, 国际关系学院副研究员, 主要研究方向为情报学。

夏宇清(1966—), 女, 北京人, 国际关系学院工程师, 主要研究方向为网络安全。