基于 AHP 的威胁情报网站价值评估方法*

张 雷,宋 栋,刘 红
(华北计算机系统工程研究所,北京 100083)

摘 要:威胁情报的采集是情报搜集工作中至关重要的一个环节,威胁情报网站是其重要载体。首先确定了威胁情报的价值特性,然后讨论了利用层次分析法确定诸多模糊聚类因子的权重,并且应用模糊综合评价方法建立了模糊综合评价方法的两级模型,从而得到对威胁情报网站的客观评估,方便用户在搜集信息时进行权衡。与其他方法相比该方法评价结果更具准确性,具有较大的现实意义和应用前景。

关键词:威胁情报;层次分析法;评估
中图分类号:TP391.1 文献标识码:A DOI:10.19358/j.issn.2096-5133.2020.11.013
引用格式:张雷,宋栋,刘红. 基于 AHP 的威胁情报网站价值评估方法[J].信息技术与网络安全,2020,39(11):79-83.

Threat intelligence website value assessment method based on AHP

Zhang Lei, Song Dong, Liu Hong
(National Computer System Engineering Research Institute of China, Beijing 100083, China)

Abstract: The collection of threat intelligence is a crucial link in the intelligence collection work, and the threat intelligence website is its important carrier. This paper firstly determines the value characteristics of threat intelligence, and then discusses the use of analytic hierarchy process to determine the weights of many fuzzy clustering factors, and uses the fuzzy comprehensive evaluation method to establish a two-level model of the fuzzy comprehensive evaluation method, thus the objective evaluation of threat intelligence website is obtained, which is convenient for users to make a trade-off when collecting information. The evaluation results are more accurate and has greater practical significance and application prospects compared with other methods.

Key words: threat intelligence; AHP; assessment

0 引言

随着网络技术的飞速发展,现在网络上充斥着各种各样的威胁情报网站,威胁情报是对搜集到的各种公开的、泄露的素材进行综合分析整理的成果,是协助和指导作战的重要依据。威胁情报网站都有各自的特点和侧重项,对各网站的综合性能很难做出一个评估,要从这些网站中获取对自己有价值的信息比较困难,需要对不同的网站进行筛选比较,找出对自己价值最大的网站来。基于此,研究一种合适的方法,比较客观地评价一个威胁情报网站的价值[1],将不但有利于用户的使用,而且有利于调动情报搜集人员的积极性和主观能动性,更有助于辅助决策,使针对敌方的各类决策趋于科学化、合理化,最终提高军事行动效能,同时也有利于网站本身的改进和发展。

本文首先确定了威胁情报的价值特性,主要将相关性、准确性、全面性、及时性四部分作为准则层进行分析阐述,各部分共分化出 12 个指标作为措施层;然后运用层次分析法建立综合评价模型,对威胁情报类网站价值进行综合评价;最后选取一个威胁情报网站的评价实例进行实际评测,在保证客观性和准确性的基础上实现了主观和客观、定性与定量的有机结合,结果更具科学性和参考性。

1 层次分析法

由运筹学家莎迪(SAATY T L)于 20 世纪 70 年代首次提出的层次分析法(Analytic Hierarchy Process,

*基金项目:国家重点研发计划(2018YFB0803502)

AHP)[2]，是一种多目标多层次的决策分析方法，它实现了定量和定性分析的结合，具有非常简洁的特性，且逻辑性很强，还有很高的实用性。该方法对待选方案进行精确的评价，有一个基本的前提，即系统与全面的指标体系必须首先建立起来。全面系统只是指标体系的一个基本方面，内在结构组成的科学性也是尤其需要关注的。有一些基本原则，如可操作性和导向性，科学性与目的性等都是在设计评价指标体系时需要考虑遵照的。本文在对威胁情报类网站评价指标进行选取时遵循了以上准则，并且在相应部分有所侧重。

2 价值模型的构造

在对威胁情报网站进行分层构建模型前，首先需要明确威胁情报的价值特性，这样才能确定评价指标，构建评价准则。

2.1 威胁情报价值特性的确立

威胁情报是运用于军事领域的一种特殊信息，因此威胁情报价值具备信息价值的一般特性，同时根据军事斗争的激烈对抗性和不可预测性以及威胁情报工作的特殊性和内幕性，归纳起来，威胁情报价值主要有以下 4 个方面的特性。

2.1.1 相关性

威胁情报网站首先应该采集有针对性的信息，消除不确定的和随机的杂乱信息。决策者要做出正确的决策需要有针对性的大量信息来减少不可预估因素的影响。故而大量的威胁情报信息可以消灭模糊性，使决策者可以精确把握双方当前形势，从而使决策更加科学[3]。从另一个角度看，不一样的威胁情报信息服务于不同的决策对象：高屋建瓴的领导者对战略和总体方面的情报需求更强烈，但局部层面的决策者对战术层次的和具体层面的情报需求非常迫切。不同时间段的威胁情报信息，其价值也不同。相关并切合实际符合特定时间要求的威胁情报信息是决策者正确决策的法宝。

2.1.2 准确性

为体现威胁情报网站的准确性，取以下指标作为判断依据：信息完备详实的程度以及引用数据是否准确。在对某些威胁情报信息的收集整理、鉴别和传递等过程中，一般会使用某些精密的仪器设备，同时还有各类专业人员参与其中。若搜集到的信息与当下特定任务的需求结合不紧密，那么所获取的威胁情报对行动的决策将毫无作用，这样不管看起来多有用，威胁情报的价值也只相当于零。由此而知，准确性对威胁情报的价值而言至关重要。

2.1.3 全面性

威胁情报价值不仅受准确性的影响，全面性也非常重要。一个优秀的决策者必须从各个方面进行考虑才能做出正确的决断。全面准确的威胁情报能够使决策者准确判明敌我状况，及时利用现有资源，制定合适恰当的预案，从而减少不确定情况发生[4]。威胁情报的价值主要取决于使用情报后的效益或成果。本文将是否包含僵尸网络信息、漏洞信息、网络攻防工具信息、攻击技战法信息、病毒信息等作为评价一个威胁情报网站是否全面的重要因素。

2.1.4 及时性

威胁情报的时效性在一定程度上决定了其价值，情报只有实时使用了才有价值。针对威胁情报网站提供信息的及时性，将其从敏感信息更新频率和突发事件发布时间两方面来考量。威胁情报必须及时提供甚至实时提供，及时而准确的威胁情报信息能有效缩短指挥周期，提高决策者的决策效率和准确性。同时，及时的威胁情报信息提供给决策者之后，能够帮助其更精确地对当前态势做出预判，并制定最佳的作战策略。从另一方面来看，若威胁情报信息采集周期超出了决策时间周期，该信息将变得毫无价值和用处，有时甚而有害。

2.2 分析模型的建立

2.2.1 建立层次结构模型

根据威胁情报的价值特性，可以建立一个 3 层的模型，包括：目标层、准则层、措施层。这 3 层中，再细分出不同的评价因素，构成一个整体的架构模型，如图 1 所示。

2.2.2 构造各个层次的判断矩阵

指标之间需要进行两两对比来确定其相对重要程度，这就需要各位专家依据其本人多年的威胁情报经验按照 1~9 比率标度方法(如表 1 所示)来确定，并依次构造出相对应的判断矩阵[5]。

按照图 1，用同层中的不同因素与上面一层的各个因素进行两两对比，这样对每一层中各因素的相对重要性都能给出一定的判断。比如，若 $W_{ij}=1$，$W_{ji}=1$，则认为 W_i 和 W_j 是一样重要的；若认为 W_i 比 W_j 明显重要，则 $W_{ij}=5$，$W_{ji}=1/5$，…。基于此，可以得出一个判断矩阵，该矩阵由某一层次的因素对比于上一层次的某一因素得出[6]：

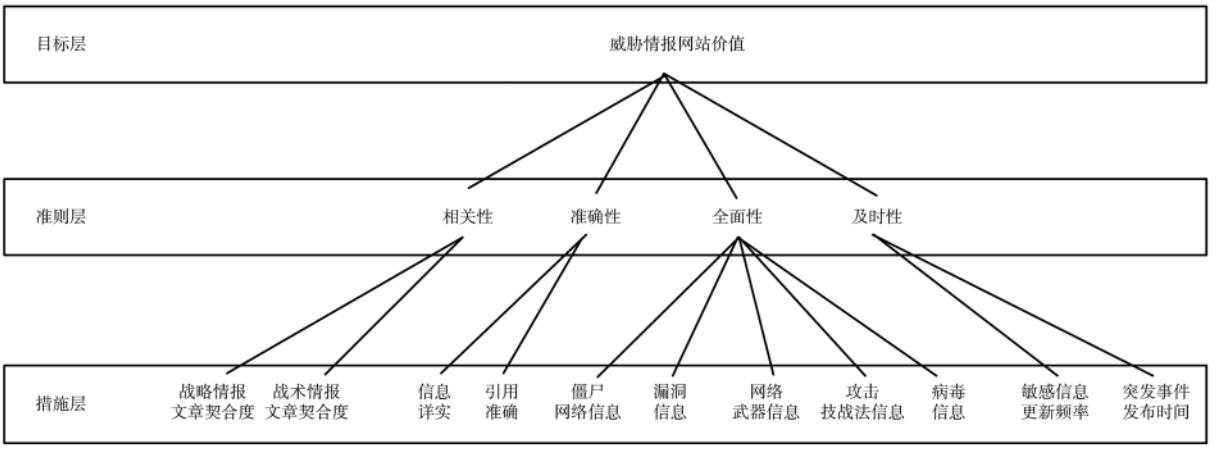

图 1 聚类因子指标体系图

表 1 判断矩阵标度及其含义

标度	含义
1	两因素相比，具有同样重要性
3	两因素相比，一个因素比另一个因素稍微重要
5	两因素相比，一个因素比另一个因素明显重要
7	两因素相比，一个因素比另一个因素强烈重要
9	两因素相比，一个因素比另一个因素极端重要
2，4，6，8	上述两相邻判断的中值
倒数	指标 W_i 与 W_j 相比得判断 W_{ij}，则 W_j 与 W_i 比较得判断 $W_{ji}=1/W_{ij}$

$$A=(W_j)_{n*n}=\begin{bmatrix} W_{11} & W_{12} & \cdots & W_{1n} \\ W_{21} & W_{22} & \cdots & W_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ W_{n1} & W_{n2} & \cdots & W_{nn} \end{bmatrix} \quad (1)$$

在判断矩阵 A 中，其元素 W_{ij} 满足以下关系：

$$W_{ij}>0(i,j=1,2,\cdots,n) \quad (2)$$

$$W_{ii}=1(i=1,2,\cdots,n) \quad (3)$$

$$W_{ji}=1/W_{ij} \quad (4)$$

2.2.3 一致性检验

一般而言，专家会根据自己多年的经验来确定判断矩阵，但是经验有时候也会有误差。为了减小误差，避免前后不一致的情况发生，就需要对判断矩阵进行一致性检验。一般而言，判断矩阵大部分是正互反矩阵[2]，它的最大特征值 $\lambda_{max}\geqslant n$，只有当判断矩阵具有完全一致性时，$\lambda_{max}=n$；λ_{max} 与 n 的差别可以作为指标，来验证判断矩阵的不一致性。判断矩阵的一致性检验的步骤如下：

(1)计算一致性指标 CI

$$CI=\frac{\lambda_{max}-n}{n-1} \quad (5)$$

(2)查找相应的平均随机一致性指标 RI

对 $n=1,\cdots,9$，为了降低判断思维的不一致而引起的偏差，SAATY T L 教授提出了 1~9 比率标准，并且列出了 RI 的值，如表 2 所示。

表 2 平均随机一致性指标 RI

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.51	0.89	1.12	1.25	1.35	1.42	1.46

当 CI=0 时，判断矩阵具有完全一致性；相反地，随着 CI 的增大，判断矩阵的一致性会变得越来越差。

在检查判断矩阵的一致性时需要将 CI 与平均随机一致性指标 RI 进行比较。一般而言，1 阶和 2 阶判断矩阵总是具有完全一致性的。对于 2 阶以上的判断矩阵，其一致性指标 CI 与同阶的平均随机一致性指标 RI 之比，称为判断矩阵的随机一致性比率 CR(Consistency Ratio)。

(3)计算一致性比率

$$CR=\frac{CI}{RI} \quad (6)$$

当 CR<0.10 时，判断矩阵的一致性可以被认可，若 CR $\geqslant$ 0.10，则认为判断矩阵设计不合适，需要提请各位专家重新思考，认真选择并重新赋值，一直到通过检验时为止。到此时所得的判断矩阵的特征向量才可以用做权向量。

2.2.4 综合评估

利用各准则对目标的权向量 X 及各方案对每一准则的权向量 W_k，在经过计算后，就可以得到各方案对总目标的权向量 W，这就是综合权向量[7]。

将准则层对目标层的权向量表示为 $X=(x_1,x_2,\cdots,x_k)^T$，措施层对准则层的权向量表示为 $W_k=(w_{k1},w_{k2},\cdots,w_{kn})^T$。以 W_k 为列向量构成组合矩阵，则措施层对目标层的综合权向量为：

$$W=W_kX \tag{7}$$

由此计算得出方案层各指标的权重。

2.2.5 建立综合评判模型

模糊综合评价涉及到如下 3 个因素：

(1)因素集 $U=\{u_1,u_2,\cdots,u_n\}$。

(2)评价集 $V=\{v_1,v_2,\cdots,v_m\}$，例如{优，良，中，差，劣}。

(3)单因素评价，它是 U 到 V 的一个模糊映射 $f:U\to V$，即：

$$u_i\to f(u_i)=(r_{i1},r_{i2},\cdots,r_{im})\in F(V) \tag{8}$$

模糊映射 f 可确定一个模糊关系 $R_f\in F(U\times V)$，即：

$$R_f(u_i,v_i)=f(u_i)(v_j)=r_{ij} \tag{9}$$

因此 R_f 可由模糊矩阵 $R\in M_{n\times m}$ 表示：

$$R=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix} \tag{10}$$

于是(U,V,R)构成一个综合评判模型。

将因素集 U 分成若干组，$U_i=(U_{i1},U_{i2},\cdots,U_{ini})$，于是：

$$U=\bigcup_{i=1}^{p}U_i(U_i\cap U_j=H,i\neq j) \tag{11}$$

$$U=\{u_{11},u_{12},\cdots,u_{1n1},u_{21},u_{22},\cdots,u_{2n2},\cdots,u_{p1},u_{p2},\cdots,u_{pnp}\}$$

令 $\underline{U}=\{U_1,U_2,\cdots,U_p\}$，称 $\underline{U}$ 为 2 层因素集，其元素 U_i 为一层因素集 U 的子集[7]。

对 $U_i=(U_{i1},U_{i2},\cdots,U_{ini})$中的各因素进行评价，即建立模糊映射：

$$f_i\bullet U_i\to F(V) \tag{12}$$

$$f_i(u_{ik})=(r_{k1},r_{k2},\cdots,r_{km})\in F(V) \tag{13}$$

得评判矩阵 R_i，以(U_i,V,R_i)为原始模型，在 U_i 中通过 AHP 法求出各因素的权重值 $A_i=(a_{i1},a_{i2},\cdots,a_{imi})$，求得综合评价：

$$B_i=A_i\bullet R_i\in F(V)\quad(i=1,2,\cdots,p) \tag{14}$$

考虑 2 层因素 $\underline{U}=\{U_1,U_2,\cdots,U_p\}$，以 B_i 作为 U_i 的单因素判断，建立模糊映射$f:\underline{U}\to F(V)$，$U_i\to f(U_i)=B_i$，得 2 层评价矩阵：

$$R=\begin{bmatrix} B_1 \\ B_2 \\ \cdots \\ B_p \end{bmatrix}=\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ b_{p1} & b_{p2} & \cdots & b_{pm} \end{bmatrix} \tag{15}$$

以$(\underline{U},V,R)$作为原始模型，利用 AHP 法可以求出 $\underline{U}$ 中各因素的权重[8]：

$$A=(a_1,a_2,\cdots,a_p) \tag{16}$$

求出综合评价：

$$B=A\bullet R\in F(V) \tag{17}$$

上面给出的就是综合评判 2 层模型。

3 评价实例

以对威胁情报网站(如卡巴斯基)的模糊评价为例，指标体系及评分分别列于表 3，邀请 15 名评价专家对其进行评分，并形成列表。

表 3 威胁情报网站的模糊评价指标体系及评分表

一级指标	二级指标	网站价值评估				
		优	良	中	差	劣
相关性	方法类文章契合度	6	5	2	1	1
	工具类文章契合度	5	4	5	1	0
	其他情报文章契合度	5	5	5	0	0
准确性	信息完备详实	6	5	1	3	0
	引用数据准确	8	4	1	1	1
全面性	包含僵尸网络信息	5	5	2	1	2
	包含漏洞信息	2	2	4	4	3
	包含网络攻防工具信息	8	6	1	0	0
	包含攻击技战法信息	7	4	1	2	1
	包含病毒信息	9	1	3	0	2
及时性	敏感信息更新频率	2	2	4	3	4
	突发事件发布时间	4	1	4	2	4

本例中经专家综合及利用层次分析法得出各层因子的权重为：

$$A_1=(0.425,0.355,0.22);$$

$$A_2=(0.395,0.605);$$

$$A_3=(0.205,0.188,0.205,0.213,0.189);$$

$$A_4=(0.35,0.65);$$

$$A=(0.255,0.35,0.185,0.21)$$

$$R_1=A_1R_1(C_1)=(0.425,0.355,0.22)\times\begin{bmatrix} 0.400\,0 & 0.333\,3 & 0.133\,3 & 0.066\,7 & 0.066\,7 \\ 0.333\,3 & 0.266\,7 & 0.333\,3 & 0.066\,7 & 0 \\ 0.333\,3 & 0.333\,3 & 0.333\,3 & 0 & 0 \end{bmatrix}$$

$$=(0.361\,6,0.309\,7,0.248\,3,0.052,0.028\,3)$$

同理得：

$\boldsymbol{R}_2=(0.480\ 6, 0.293\ 1, 0.066\ 7, 0.119\ 4, 0.040\ 4)$

$\boldsymbol{R}_3=(0.415\ 5, 0.244\ 8, 0.388\ 8, 0.092\ 2, 0.104\ 3)$

$\boldsymbol{R}_4=(0.220\ 1, 0.090\ 1, 0.266\ 7, 0.156\ 6, 0.266\ 7)$

合并成 $\boldsymbol{R}$，作归一化处理得：

$$\boldsymbol{R}=\begin{bmatrix}0.361\ 6 & 0.309\ 7 & 0.248\ 3 & 0.052 & 0.028\ 3\\ 0.480\ 6 & 0.293\ 1 & 0.066\ 7 & 0.119\ 4 & 0.040\ 4\\ 0.333\ 6 & 0.196\ 5 & 0.312\ 1 & 0.074\ 0 & 0.083\ 7\\ 0.220\ 1 & 0.090\ 1 & 0.266\ 7 & 0.156\ 6 & 0.266\ 7\end{bmatrix}$$

模糊综合评价结果为：

$\boldsymbol{B}=\boldsymbol{A}*\boldsymbol{R}=$

$(0.255, 0.35, 0.185, 0.21)\times$

$$\begin{bmatrix}0.361\ 6 & 0.309\ 7 & 0.248\ 3 & 0.052 & 0.028\ 3\\ 0.480\ 6 & 0.293\ 1 & 0.066\ 7 & 0.119\ 4 & 0.040\ 4\\ 0.333\ 6 & 0.196\ 5 & 0.312\ 1 & 0.074\ 0 & 0.083\ 7\\ 0.220\ 1 & 0.090\ 1 & 0.266\ 7 & 0.156\ 6 & 0.266\ 7\end{bmatrix}$$

$=(0.368\ 3, 0.236\ 9, 0.200\ 3, 0.101\ 7, 0.092\ 8)$

该网站利用层次分析法及专家综和评价，经计算后比例依次为：优(0.368 3)、良(0.236 9)、中(0.200 3)、差(0.101 7)、劣(0.092 8)，根据最大隶属度原则，“优”的隶属度最高，可以得出该威胁情报网站评估水平为优秀。

4 结论

本文研究了威胁情报的价值特性，进而使用层次分析法来确定不同层次指标对各层中不同因素的权重，这是一种科学有效的方法，将它应用于对威胁情报网站的综合评价，得出对威胁情报网站的直观评价，与其他方法相比评价结果更具客观性。未来研究将考虑从网站动态变化的角度进一步开展，根据评价结果，加入反馈，形成动态调整机制。

参考文献

[1] MOHAMED A B, MAI M, FLORENTIN S. An extension of neutrosophic AHP-SWOT analysis for strategic planning and decision-making[J]. Symmetry, 2018, 10(4): 116.

[2] MANI M R, ANKITA M, VETHAMONY P. A new insight to vulnerability of Central Odisha coast, India using analytical hierarchical process(AHP) based approach[J]. Journal of Coastal Conservation, 2018, 22(4): 799-819.

[3] ISHIZAKA A, LABIB A. Review of the main developments in the analytic hierarchy process[J]. Expert Systems With Applications, 2011, 38(11): 14336-14345.

[4] 孙辉，罗双春，李余彪. 大数据技术在信息网络威胁情报中的运用研究[J]. 信息技术与网络安全，2020, 39(5): 28-32.

[5] 许树柏. 实用决策分析——层次分析法原理[M]. 天津：天津大学出版社，1988.

[6] 朱孔来，于祥卿，吴自友，等. 用 AHP 法确定聚类因子的权重[J]. 农业系统科学与综合研究，1990(1): 55-57.

[7] 张跃，邹寿平，宿芬. 模糊数学方法及其应用[M]. 北京：煤炭工业出版社，1992.

[8] 李昱宇，徐蓉. 基于层次分析法的质量安全风险评估[J]. 建筑经济，2007(S1): 54-56.

(收稿日期：2020-06-05)

作者简介：

张雷(1985-)，男，硕士，工程师，主要研究方向：社交网络、自然语言处理、工控安全。

宋栋(1986-)，男，硕士，工程师，主要研究方向：网络测量、工控安全。

刘红(1986-)，女，硕士，工程师，主要研究方向：工控安全测试、网络安全。

版权声明