项寅．基于改进神经网络的恐怖袭击风险预警系统[J]．灾害学，2018，33(1)：183－189.[XIANG Yin. Warning System of Terrorist Attacks based on Improved Neural Network[J]. Journal of Catastrophology，2018，33(1)：183－189. doi：10.3969/j. issn. 1000－811X. 2018. 01. 032.]

基于改进神经网络的恐怖袭击风险预警系统*

项 寅

(上海财经大学 国际工商管理学院，上海 200433)

摘 要：为提高恐怖袭击应急管理的效率，设计了恐怖袭击的风险评估和预测系统。评估模型通过因子分析方法计算各类目标的相对风险指数，评估指标包含“威胁”、“脆弱性”、“后果”三大因素，具体数据从全球恐怖主义数据库(GTD)中进行采集。预测模型通过神经网络实现风险指数的预测，由于 BP 神经网络的梯度下降算法收敛较慢且易陷入局部最优点，因此利用遗传算法对神经网络的初始权值阈值进行优化，并提高预测精度。最后，对 GTD 数据库中的 21 类主要袭击目标进行算例分析，验证了该模型的可行性和准确性，同时还根据这些目标的风险指数进行原因分析和策略建议。

关键词：恐怖袭击；风险评估；风险预测；因子分析；神经网络

中图分类号：N949；X45　　**文献标志码**：A　　**文章编号**：1000－811X(2018)01－0183－07

doi：10.3969/j. issn. 1000－811X. 2018. 01. 032

当前，恐怖主义正成为影响国际社会安全的重要风险源，恐怖袭击在世界各地频频发生，愈演愈烈。根据全球恐怖主义数据库(GTD)的记录，2001－2015 年期间，全球共发生恐怖袭击 85 196 起，累计死亡人数 203 943 人。近几年的重大恶性恐怖袭击事件包括“3·1”中国昆明火车站暴恐事件、“8·17”泰国四面佛爆炸事件、“11·3”法国巴黎系列恐怖袭击事件、“7·14”法国尼斯恐怖袭击事件等。

因此，如何评估和预测恐怖袭击风险成为反恐研究的重要课题。随着恐怖袭击目标的不断泛华和软化，通过对恐怖袭击的风险进行评估和预测，可以锁定关键目标并发现新目标[1]，进而提高反恐资源管理效率，并减少袭击损失。

很多学者针对恐怖袭击风险评估进行研究，现有文献主要利用影响图[2]、贝叶斯网络[3]、决策树[4]、事件树[5－6]、云模型[7]等概率论方法以及博弈论方法[8]针对军事要地、危险品运输道路、地铁站、民航机场等具体场所进行风险评估。然而，恐怖袭击预测方面的研究则相对较少。例如，Petroff 等[9]提出了关于具体恐怖袭击事件预警的隐马尔可夫模型，并将其应用于伊拉克和阿富汗战场。Popp 等[10]以及战兵等[11]利用隐马尔可夫模型与贝叶斯网络方法，通过分析一些先前发生的事件来预测近期可能发生的相关恐怖袭击事件，实现对相关情报的侦测，预防可能发生的恐怖事件。傅子洋等[12]利用国外恐怖袭击样本建立贝叶斯网络模型，并利用我国数据对网络参数进行修正，最后用于恐怖袭击事件的预警。

通过对文献的归纳与总结发现，现有文献存在一些局限。一方面，事件树、决策树、贝叶斯网络、马尔科夫模型、影响图等概率论方法存在大量的先验概率信息不易获取、分布函数难以确定等技术难度和缺陷[13－14]，因而较难应用于实际。另一方面，现有的风险评估和预测研究主要集中于例如机场、公路、军事等某类目标、某类系统的局部性风险评估，缺乏整体层面的研究，例如全球范围内不同国家、区域、袭击方式、袭击目标、袭击武器的风险指数评估和预测。

基于以上不足，本文从整体性层面出发，设计以数据驱动的全球恐怖袭击风险指数评估和预测系统，系统建立在 GTD 数据库的大数据样本之上，克服了风险评估中先验概率难以获取的难题。该系统包含两部分，首先，对选取的评估指标进行因子分析，计算出不同袭击对象的风险指数并进行排名；其次，在预测指标的基础上，利用 BP 神经网络实现未来风险指数的预测，并结合遗传算法优化神经网络的初始权值和阈值，提高算法精度。

* 收稿日期：2017－05－13　　修回日期：2017－07－23
基金项目：国家自然科学基金项目“不对称信息下随机反恐阻止网络设计与资源分配研究”(71571114)
作者简介：项寅(1987－)，男，江苏苏州人，博士研究生，研究方向为应急管理．E-mail：xiang19872728@126. com

表 1 恐怖袭击风险评估指标

威胁	脆弱性	后果			
袭击发生概率	袭击成功率	死亡人数	受伤人数	死亡人数 3 人或以上的袭击次数	受伤人数 10 人或以上的袭击次数

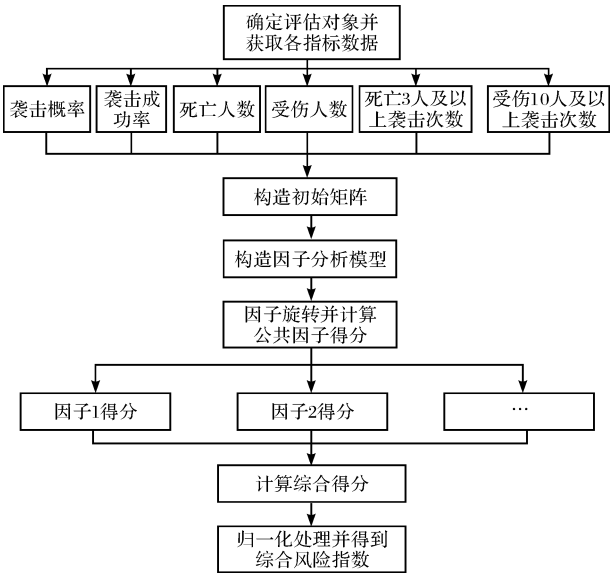

图 1 恐怖袭击风险评估模型流程图

1 风险指数的评估模型

1.1 风险评估指标选取

对于恐怖袭击风险评估指标的选取，兰德公司认为其应当由“威胁”、“脆弱性”、“后果”三部分组成[1]，分别代表“袭击发生的概率”、“袭击发生前提下产生损失的条件概率”以及“产生损失前提下的期望损失值”，三者的乘积即为具体的风险值，且在后来的研究中，该评估指标得到了广泛应用[15-16]，说明具有可行性和准确性。

因此，选取 GTD 数据库中的 6 个变量构成风险评估的具体指标，具体为：“袭击发生概率”、“袭击成功率”、“死亡人数”、“受伤人数”、“死亡人数 3 人或以上的袭击次数”、“受伤人数 10 人或以上的袭击次数”。前两个指标变量代表“威胁”和“脆弱性”，通过 GTD 数据库中“单个对象的袭击次数/所有对象的袭击次数”和“袭击成功次数/总袭击次数”的简单运算获得。后四个指标则反映“后果”，其中，“死亡人数 3 人或以上”及“受伤人数 10 人或以上”参考了《生产安全事故报告和调查处理条例规定》[17]中较大事故伤亡人数的评定标准。此外，由于 GTD 中“财产损失”的样本数据缺失值高达 64%，出于评估精度考虑，予以剔除，因此，该评估指标仅评估恐怖袭击人生伤亡的风险指数。

1.2 风险评估模型

利用因子分析得到袭击对象中不同样本的综合风险指数，该指数仅反映各样本间的相对风险水平。具体风险评估流程如图 1 所示，主要包括 6 个步骤。

步骤一：确定评估对象并获取各指标数据。GTD 数据库按照不同的袭击对象进行归类，包括 12 个不同区域、220 个不同国家、各国的省份和城市、8 类袭击方式、21 种主要袭击目标、110 种细分袭击目标、12 种主要袭击武器和 28 种细分袭击武器。选取任意袭击对象进行评估，并根据六个评估指标收集数据。

步骤二：构造初始矩阵。数据收集完后得到一个矩阵，为消除各指标不同量纲的影响，进行标准化处理并得到初始矩阵 $X=(X_1\cdots X_p)$，X_p 为关于指标 p 的数据向量。

步骤三：构造因子分析模型。模型如下：

$$X=AF+\varepsilon。\tag{1}$$

式中：$F=(F_1, F_2, \cdots, F_m)$为公共因子矩阵，$A$ 为因子载荷矩阵。初始变量矩阵 X 用 $m(m<p)$个公共因子向量 F_1，F_2，…，F_m 的线性组合表示，通过略去公共因子外的特殊因子矩阵 ε 实现降维。m 和 A 通常采用主成分分析方法计算。

步骤四：因子旋转并计算公共因子得分。旋转过程如下：

$$F_j=\beta_{j1}X_1+\cdots+\beta_{jp}X_p,\ (j=1\cdots m)。\tag{2}$$

式中：F_j 为公共因子 j 的得分向量，β_{jp}表示 X_p 对公共因子 j 的相关程度，通常采用正交旋转最大方差法计算。

步骤五：计算综合得分。计算过程如下：

$$\mathbf{Score}=\sum_{j=1}^{m}W_jF_j。\tag{3}$$

式中：**Score** 为包含每个样本的综合得分向量，W_j 为公共因子向量 F_j 的权重向量，通过公共因子 j 的方差贡献率占总方差贡献率的比重来计算。

步骤六：归一化处理并得到综合风险指数。把 **Score** 归一化到$[0,1]$之间，具体过程如下：

$$s_k'=(s_k-s_{\min})/(s_{\max}-s_{\min})。\tag{4}$$

s_k' 和 s_k 分别为归一化后和归一化前的样本 k 的风险值，$s_{\max}$和 $s_{\min}$分别为归一化前所有样本中最大和最小的风险值。

2 风险指数的预测模型

2.1 风险预测系统框架

传统预测方法分为因果预测法和时间序列预测法，由于恐怖袭击风险指数根据评估指标计算而得，因此，利用因果预测法更具合理性。然而，因果分析预测法的缺点是无法预测未来，即通过当年的风险指标仅能预测当年的风险指数，而不能实现未来的预测，这显然不能满足国家安全部

门进行长期反恐战略部署的要求。有学者把 100 多年来的恐怖主义总结为四次浪潮[18]，并认为每次浪潮中恐怖袭击的特征和主要对象不会发生重大变化，这是因为其意识形态所决定的，但是却可能因为军事、政治、经济等影响因素发生中小范围的变动。根据这一特点，可以利用当年的评估指标来预测当年及未来几年的平均风险指数，实现预测作用，预测系统的框架如图 2 所示。

图 2 中 y_i 表示第 i 年，根据 y_1 的风险预测指标预测 y_1 到 y_3 的平均风险指数并用于 y_2 和 y_3 的反恐战略部署；再用 y_3 的风险预测指标预测 y_3 到 y_5 的平均风险指数并用于 y_4 和 y_5 的反恐战略部署……因为预测年份过多或过少分别会影响预测精度或压缩反恐战略部署时间，因此，经过专家的讨论，最终确定为每两年进行一次预测来实现整个预测系统的循环。此外，全球恐怖袭击日益频繁，导致风险评估指标中的“后果”呈现不断上升趋势，而评估出的袭击对象的相对风险指数始终归一化于[0，1]之间，因此，为消除“后果”的这种上升趋势所产生的影响，需要把“后果”部分的指标设置为百分比形式。最终的预测指标如表 2 所示。例如“死亡人数占比”反映为某个时段内单个样本的死亡人数占总体死亡人数的比率。

2.2　基于 GA－BP 的风险预测模型

关于 BP 神经网络，Kosmogorov 定理说明在有合理的结构和恰当的权值的条件下，三层前馈网络可以逼近任意的非线性连续函数，但定理中没给出如何确定合理结构和恰当的权值的方法[19]。通过遗传算法可以实现初始权值和阈值的优化，从而提高 BP 神经网络的预测精度。具体的预测模型如图 3 所示，共包括 9 个步骤。

步骤一：创建神经网络。首先，选择网络层数为 3 层；其次，通常隐含层的节点个数范围为 $n=\sqrt{n_i+n_0}+a$（其中 n_i，n_0，a 分别代表输入节点数、输出节点数和任意[1,10]之间的整数）[20]，经过反复试验选取最佳节点数为 10 个，整个网络的结构为（6－10－1）；接着，由于输入值和输出值的范围均在[0,1]范围内，选择“logsig”函数作为传递函数；最后设置迭代步长 0.3，迭代次数 20 000。

步骤二：输入训练数据。训练数据用于遗传算法中的初始权值和阈值优化。

步骤三：染色体编码并生成初始种群。采用实数编码方式，编码次序按照先权值再阈值，逐层逐点的顺序进行。其中，$w_k(m,n)$ 为连接第 $k-1$ 层网络中的第 n 个节点到第 k 层网络中第 m 个节点的权重；$b_k(m)$ 为第 k 层网络中第 m 个节点的阈值。

步骤四：杂交、变异。选择单点杂交法，选取杂交率和变异率分别为 0.6 和 0.04。

步骤五：计算适应度并选择最优种群。适应度函数选择均方误差函数（MSE），其中 y_i，$\hat{y}_i$，n 分别代表样本 i 的真实值、样本 i 的预测值和样本个数。

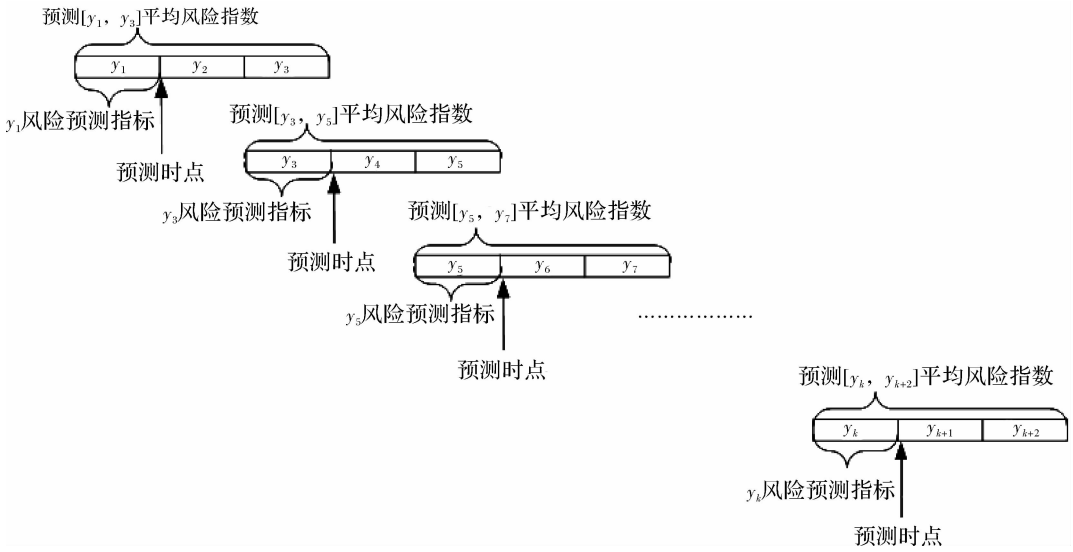

图 2　恐怖袭击风险预测系统框架

表 2　评估指标和预测指标对比

指标类别	指标特征					
	威胁	脆弱性			后果	
评估指标	袭击发生概率	袭击成功率	死亡人数	受伤人数	死亡人数 3 人或以上的袭击次数	受伤人数 10 人或以上的袭击次数
预测指标	袭击发生概率	袭击成功率	死亡人数占比	受伤人数占比	死亡人数 3 人或以上的袭击次数占比	受伤人数 10 人或以上的袭击次数占比

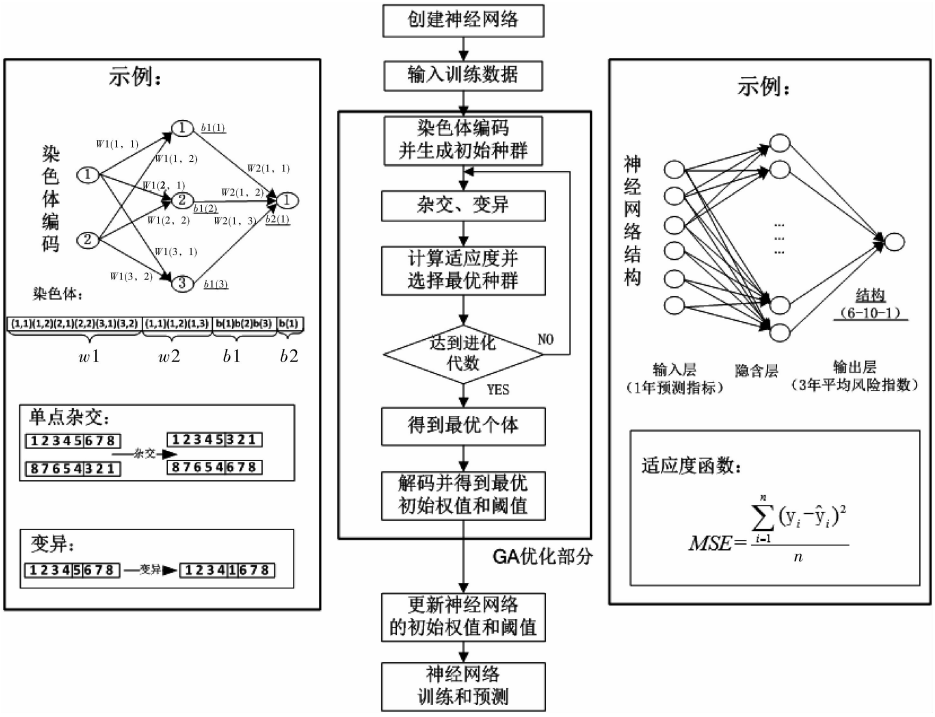

图 3 GA – BP 恐怖袭击风险预测模型

表 3 不同时间段的风险指标值

样本号	目标	2001 – 2003	2003 – 2005	2005 – 2007	2007 – 2009	2009 – 2011	2011 – 2013	2013 – 2015
1	商业	0. 4124	0. 4525	0. 2885	0. 3203	0. 3760	0. 3544	0. 2765
2	政府	0. 2740	0. 4361	0. 2692	0. 3105	0. 3683	0. 3354	0. 2147
3	警察	0. 3475	0. 7672	0. 5742	0. 4132	0. 3223	0. 6804	0. 4618
4	军队	0. 4407	0. 7869	0. 3791	0. 2885	0. 2327	0. 6835	0. 6206
5	医疗场所	0. 1102	0. 1803	0. 0000	0. 0000	0. 1407	0. 0000	0. 0000
6	飞机/机场	0. 0141	0. 0000	0. 0549	0. 0709	0. 0000	0. 0601	0. 0882
7	大使馆	0. 0593	0. 0295	0. 0549	0. 0954	0. 0026	0. 1044	0. 1235
8	教育	0. 0847	0. 1934	0. 1044	0. 1614	0. 1483	0. 1551	0. 1324
9	食品	0. 0000	0. 1869	0. 1071	0. 1222	0. 0716	0. 0918	0. 0941
10	媒体	0. 0876	0. 1607	0. 0962	0. 1247	0. 1125	0. 0949	0. 1059
11	海事	0. 1186	0. 2033	0. 1071	0. 1125	0. 0179	0. 0475	0. 1206
12	非政府组织	0. 0678	0. 1180	0. 1126	0. 1540	0. 1023	0. 1076	0. 1324
13	其他	0. 1130	0. 2000	0. 0852	0. 1540	0. 1483	0. 1044	0. 1265
14	平民	1. 0000	1. 0000	1. 0000	1. 0000	1. 0000	1. 0000	1. 0000
15	宗教	0. 1977	0. 3410	0. 2088	0. 2249	0. 2302	0. 2437	0. 1912
16	通讯	0. 1073	0. 0951	0. 0742	0. 1027	0. 1100	0. 1171	0. 1147
17	恐怖组织	0. 0819	0. 1934	0. 1236	0. 1638	0. 0921	0. 1772	0. 1794
18	旅游场所/游客	0. 0763	0. 1639	0. 0824	0. 1296	0. 1458	0. 0886	0. 0971
19	交通	0. 3107	0. 2689	0. 1896	0. 1980	0. 1560	0. 1551	0. 1471
20	公共设施	0. 0847	0. 1344	0. 1099	0. 1198	0. 0946	0. 1139	0. 1206
21	暴力政党	0. 1045	0. 0787	0. 0659	0. 1443	0. 1509	0. 0728	0. 1000
FA	巴特勒检验	. 00	. 00	. 00	. 00	. 00	. 00	. 00
指	检验值	0. 703	0. 705	0. 736	0. 756	0. 679	0. 706	0. 759
标	累积方差	94. 37%	96. 62%	98. 15%	98. 70%	98. 40%	96. 60%	92. 40%

表 4　训练数据和预测数据分类

训练数据(71%)		测试数据(29%)	
输入部分	输出部分	输入部分	输出部分
2001 年预测指标	2001 – 2003 年平均风险指数	2011 年预测指标	2011 – 2013 年平均风险指数
2003 年预测指标	2003 – 2005 年平均风险指数	2013 年预测指标	2013 – 2015 年平均风险指数
2005 年预测指标	2005 – 2007 年平均风险指数		
2007 年预测指标	2007 – 2009 年平均风险指数		
2009 年预测指标	2009 – 2011 年平均风险指数		

步骤六：得到最优个体。进化到指定代数后，选择种群中适应度值最小的个体作为最优个体。

步骤七：解码并得到最优初始权值和阈值。将编码后的最优个体进行解码并得到遗传算法优化后的神经网络的最优初始权值和阈值。

步骤八：更新神经网络的初始权值和阈值。

步骤九：神经网络训练和预测。

3　恐怖袭击风险评估和预测模型的应用

“9·11”事件后，伊斯兰宗教极端恐怖主义肆虐，在世界各地不断开展恐怖活动，主要针对平民、军队和警察等目标进行炸弹攻击，掀起了一波“宗教恐怖主义”的浪潮，使全球安全形势受到极大威胁和挑战。

为测试风险评估和预测模型的可行性和预测的准确性，本文选取 GTD 数据库中的 21 个主要袭击目标作为测试对象，利用 2001 年到 2015 年间的恐怖袭击数据进行测试。

首先，对不同目标的袭击风险进行评估。分别收集 2001 – 2003，2003 – 2005，2005 – 2007，2007 – 2009，2009 – 2011，2011 – 2013，2013 – 2015 共 7 个时段的的评估指标数据，用 SPSS21.0 进行因子分析，分别得到这 7 个时段的风险指数，如表 3 所示。

从因子分析指标来看，所有因子分析均通过巴特勒球形检验，且检验值都在 0.65 以上，说明变量间存在相关性，适用因子分析。另外，主因子按照特征根大于 0.9 的选取原则，所选主因子的累积方差都在 90% 以上，说明降维后仍保留了大部分信息。

从风险指数来看，平民在所有时间段中的风险指数均为最高，成为当前恐怖袭击的主要对象；医疗场所在四个时间段中的风险指数均呈现最低，是当前最不易受到袭击的目标。此外，各目标的风险指在不同时间段中未发生较大程度的变化，但是存在中小幅度的波动，说明恐怖袭击的目标偏好比较固定。

其次，利用遗传算法优化后的 BP 神经网络测试系统的预测性能。用 Matlab2014 编译 GA – BP 程序并测试预测效果。如表 4 所示，根据 70% 训练数据和 30% 测试数据的原则，分别收集 2001 年，2003 年，2005 年，2007 年，2009 年各样本的预测指标数据作为训练数据的输入部分，收集 2011 年和 2013 年各样本的预测指标数据作为测试数据的输入部分；把 2001 – 2003 年，2003 – 2005 年，2005 – 2007 年，2007 – 2009 年，2009 – 2011 年各样本的风险指数作为训练数据的输出部分，把 2011 – 2013 年，2013 – 2015 年各样本的风险指数作为测试数据的输出部分。总计 147 个样本，训练样本 105 个，测试样本 42 个。图 4 ~ 图 6 分别为针对测试数据的遗传算法优化前的预测结果、遗传算法优化后的预测结果、优化前后各样本的误差比较。

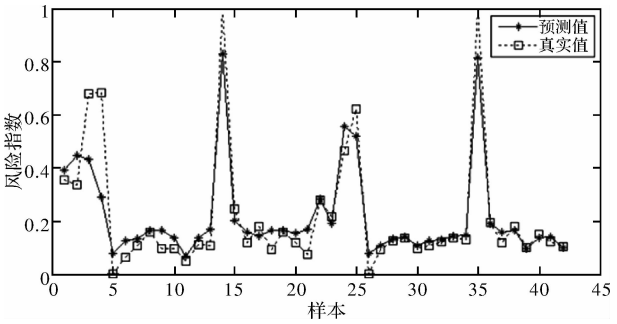

图 4　遗传算法优化前的 42 个测试样本的预测结果

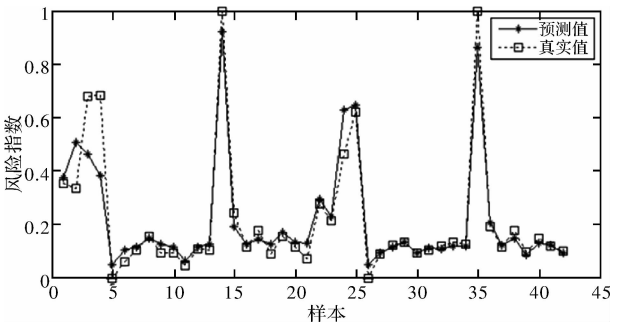

图 5　遗传算法优化后的 42 个测试样本的预测结果

从总体指标来看，如表 5 所示，用 BP 神经网络进行预测，均方误差和测试样本总误差分别为 0.008 和 2.279，用遗传算法优化后的 BP 神经网络进行预测，均方误差和测试样本总误差分别为 0.005 和 1.853，说明优化后预测精度得到了很大提高。根据图 4 和图 5 发现，两种预测方法均能反映出真实风险指数的总体分布情况。但是，在最

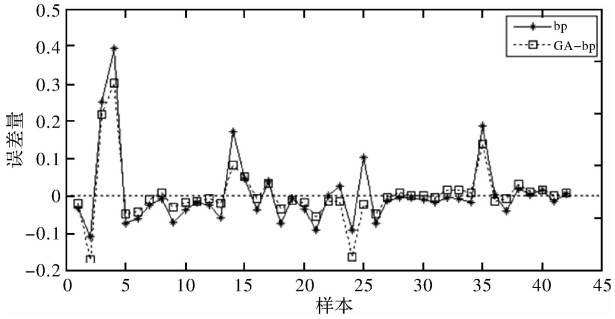

图6 优化前后各样本的误差比较

大风险值和最小风险值两个全局最优点的预测中，BP 神经网络因使用梯度下降算法而极易收敛于局部最优点，预测偏差较大；而优化后的 BP 神经网络虽然仍无法到达全局最优点，但是预测效果有所提高。

表5 优化前后的预测总体指标对比

预测性能指标	BP 神经网络	GA－BP 神经网络	性能优化值
均方误差	0.008	0.005	0.003
总误差	2.279	1.853	0.426

从单个样本的误差来看，由图6可知，除样本2(政府)外，优化后的预测误差均小于或约等于优化前的预测误差，说明遗传算法优化后，预测精度的提高效果比较均衡。在预测结果中，警察(样本3、样本24)和军队(样本4)的预测误差较大，从表2中可以发现其波动幅度较大，因此在预测时需要结合其他数据或定性指标进行单独分析。

4 结论

本文从整体性角度设计了以数据驱动的恐怖袭击风险指数评估和预测系统。首先，在GTI风险评估指标的基础上加入了“威胁”和“脆弱性”因子，并通过因子分析计算各样本的风险指数；其次，利用遗传算法优化过的 BP 神经网络构建了恐怖袭击风险的预测模型；最后，通过对 GTD 中的21类主要目标进行算例分析来验证该系统的可行性和预测的准确性。

算例分析发现：①平民是袭击风险最高的目标，其风险指数远远高于其他目标，一是因为“9·11”事件后各国加大了机场、车站等“硬目标”的安保力度，增加了恐怖袭击的难度，因此恐怖袭击转向防御力低的平民这类“软目标”，二是因为美国发动的大规模反恐战争削弱了恐怖组织的有生力量，恐怖组织结构趋向分散化，类似“9·11”事件的大规模袭击很难组织，而逐渐趋向“独狼式”的平民袭击。②交通类目标的风险指数随时间呈明显下降趋势，非政府组织和恐怖组织目标的风险指数随时间明显上升，其他目标的风险指数则上下波动，其中，军队目标的风险波动最大。说明交通设施和场所的安检措施得到了一定的成效，而不同恐怖组织之间的内斗态势不断加剧，军队目标的风险主要和美国在伊拉克和阿富汗地区的军事战略相关联。

从各类目标的风险指数分布可以得到相应的反恐策略，目前应加强对于平民目标的保护，具体措施包括：加快情报系统建设，对重要时段重要地点重要活动增派安保人员，提高恐怖袭击的应急管理效率等。

最后，此风险评估和预测系统存在一些局限：①因受制于 GTD 数据库中袭击对象的分类，对于数据库以外的新的袭击对象则无数据进行评估和预测。②预测模型的外推年份由专家评估而定，存在一定的主观性。③该评估和预测方法完全依靠数据驱动，避免不了一定的局限性。因此，在实际工作中，可在本模型的分析结果上，再结合社会、经济、政治等因素加以定性分析，从而得到更精确有效的结论。

参考文献：

[1] Willis H H. Guiding resource allocations based on terrorism risk [J]. Risk Analysis, 2007, 27(3): 597－606.
[2] Pat－Cornell E, Guikema S . Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures [J]. Military Operations Research, 2002, 7(4): 5－23.
[3] Hudson L, Ware B, Laskey B, et al. An application of Bayesian networks to antiterrorism risk management for military planners [D]. Georgy Mason University, 2001: 19－35.
[4] Winterfeldt D V, Sullivan TM. Should We Protect Commercial Airplanes Against Surface－to－Air Missile Attacks by Terrorists [J]. Decision Analysis, 2006, 3: 63－75.
[5] 王振，刘茂．定量风险分析在恐怖袭击风险评估中的应用[J]．中国公共安全(学术版)，2006(4)：18－22.
[6] 郭璇，吴文辉，肖治庭．基于事件树和 PRA 的民航机场恐怖袭击风险评估模型[J]．计算机应用研究，2016(33)：22－28.
[7] 种鹏云，帅斌．恐怖袭击下危险品运输网络节点风险评估方法[J]．中国安全科学学报，2012，22(8)：105－110.
[8] 赵国敏，刘茂，张青松，等．基于博弈论的地铁车站恐怖袭击风险定量研究[J]．安全与环境学报，2006，6(3)：47－50.
[9] Petroff V B, Bond J H, Bond D H. Using Hidden Markov Models to Predict Terror Before it Hits[M]. New York: Springer, 2013: 163－180.
[10] Popp R, Yen J. Hidden Markov Models and Bayesian Networks for Counter－Terrorism[M]. IEEE Xplore, 2005: 1－29.
[11] 战兵，韩锐．基于隐马尔可夫的恐怖事件预测模型[J]．解放军理工大学学报(自然科学版)，2015，16(4)：386－393.
[12] 傅子洋，徐荣贞，刘文强．基于贝叶斯网络的恐怖袭击预警模型研究[J]．灾害学，2016，31(3)：184－189.
[13] Barry C E, Bennett S P, Winterfeldt D V, et al. Probabilistic risk analysis and terrorism risk[J]. Risk Analysis, 2010 , 30(4): 575－588.
[14] 姜江，李璇，邢立宁，等．基于模糊证据推理的系统风险分析与评价[J]．系统工程理论与实践，2013，33(2)：529－537.
[15] McGill W L, Ayyub B M, Kaminskiy M. Risk analysis for critical asset protection[J]. Risk Analysis, 2007, 27(5): 1265－81.

[16] Chatterjee S, Abkowitz D. A methodology for modeling regional terrorism risk[J]. Risk Analysis, 2011, 31(7): 1133 - 1140.
[17] 中华人民共和国国务院. 生产安全事故报告和调查处理条例[Z]. 2007 - 04 - 09.
[18] 张家栋. 现代恐怖主义的四次浪潮[J]. 国际观察, 2007, 6: 62 - 68.
[19] 李敏强, 徐博艺, 寇纪淞. 遗传算法与神经网络的结合[J]. 系统工程理论与实践, 1999, 19(2): 1 - 7.
[20] 周开利, 康耀红. 神经网络模型及其 MATLAB 仿真程序设计[M]. 北京清华大学出版社, 2005: 89 - 100.

Warning System of Terrorist Attacks Based on Improved Neural Network

XIANG Yin
(*School of International Business Administration*, *Shanghai University of Finance & Economics*, *Shanghai* 200433, *China*)

Abstract: An evaluating and predicting system of terrorist attacks is designed to improve the efficiency of emergency management. In evaluating model, factor analysis (FA) is used to calculate the risk index among different attack subjects. The evaluating index contains 3 factors as threat, vulnerability and consequence, the related data are all collected from GTD database. In predicting model, neural network is applied to predict the risk index. However, as there are some flaws of BP neural network, such as slow convergence and easy of falling into local optimal, a genetic algorithm (GA) is applied to improve prediction accuracy through optimizing neural network's initial weights and thresholds. Finally, this model is applied to evaluate and predict the risk of 21 types of main targets recorded in GTD, the numerical example proves feasibility and accuracy of the model, also policy recommendations are provided at last.

Key words: terrorist attack; risk evaluation; risk prediction; factor analysis; neural network

(上接第 182 页)

Development Strategy of the Knowledge System of Emergency Science and Engineering under the Concept of STEM Education

——A Preliminary Study on Emergency Science

QIAN Hongwei[1, 2, 3]
(1. *Safety and Emergency Management Research Center*, *Henan Polytechnic University*, *Jiaozuo* 454000, *China*; 2. *Emergency Management Institute*, *Jiaozuo* 454000, *China*; 3. *Emergency Rescue Research Institute*, *Henan Polytechnic University*, *Emergency Volunteer Management Research Center*, *Jiaozuo* 454000, *China*)

Abstract: The concept of boundary problems involving multiple disciplines of emergency safety science, disaster management, fire science, public crisis management and public security. We put forward the construction of fusion and integration of emergency science and engineering discipline involving multiple disciplines in emergency, and the emergency of science and engineering subject of study, research the purpose and analyze subject the characteristics; at the same time the we in out the feasibility and significance of the discipline construction. Based on several kinds of STEM become educational philosophy, philosophy of science and technology department of philosophy and reality based on the theory of emergency management, emergency comprehensive design science and engineering discipline knowledge system and discipline direction, science and technology, including emergency and emergency engineering, industrial management, and give each branch direction and preliminary exploration design ideas. Finally, based on the emergency situation, several key problems in the construction of emergency science and engineering discipline are analyzed systematically. This research is of great practical value for the promotion of emergency work in our country, and also has important theoretical significance to improve the subject knowledge structure of our country.

Key words: emergency science; STEM education; subject; knowledge system