第 29 卷第 3 期
2021 年 6 月

安 徽 建 筑 大 学 学 报
Journal of Anhui Jianzhu University

Vol.29 No.3
Jun.2021

DOI：10.11921/j.issn.2095-8382.20210305

新型智慧城市“非传统安全”评价及对策研究

潘和平，许雨晗，魏偲琦

（安徽建筑大学　经济与管理学院，安徽　合肥　230601）

摘　要：新型智慧城市是新一代信息通讯技术与城市发展深度融合的高级社会形态，建设新型智慧城市利于提高城市治理效率，同时也暴露出网络信息安全隐患，“非传统安全”难以掌控。为识别我国新型智慧城市建设背景下的“非传统安全”危机，故选取 50 所新型智慧城市，纵向通过灰色关联度分析，从个人、政府、企业三个维度进行研究，表明我国新型智慧城市网络安全在三个维度相对建设水平较高；横向通过聚类分析，对选取的 50 个城市进行分层，综合分析各类城市网络安全建设情况。通过二者结合分析，找出我国新型智慧城市网络安全中存在的不足之处，为企业、政府提供对策建议。

关键词：新型智慧城市；非传统安全；网络安全建设；灰色关联分析；聚类分析

中图分类号：F49　　**文献标识码：**A　　**文章编号：**2095-8382（2021）03-032-08

Evaluation and Countermeasure Research on "Unconventional Security" in New Smart Cities

Pan Heping，Xu Yuhan，Wei Siqi

（School of Economics and Management，Anhui Jianzhu University，Hefei　230601，China）

Abstract：New smart cities are advanced social forms with the deep integration of new-generation information and communication technologies and urban development，and the construction of new smart cities is conducive to improving the efficiency of urban governance，but at the same time，it also reveals that there are hidden dangers in network information security and "non-traditional security" is difficult to control.In order to identify the "non-traditional security" crisis in the context of the construction of new smart cities in China，50 new smart cities are selected and studied vertically through gray correlation analysis in three dimensions：personal，government and enterprise，which shows that the relative construction level of network security in new smart cities in China is high in the three dimensions；horizontally through cluster analysis The horizontal analysis is conducted by cluster analysis，which stratifies the selected 50 cities and comprehensively analyzes the construction of network security in various cities.Through the combination of the two analyses，the shortcomings in the network security of China's new smart cities are identified，and countermeasure suggestions are provided for enterprises and governments.

Key words：New Smart City；Non-traditional Security；Cyber Security Construction；Gray Correlation Analysis；Cluster Analysis

“智慧城市”这一概念最早于 2008 年由 IBM 提出[1]，旨在高效运用各种先进信息与通讯技术，通过感测和整合城市运行体系对城市内的人类需求做出智能响应。我国此时处于以信息技术为主导的智慧城市导入期及摸索期，衍生出“信息孤岛”效应，“非传统安全危机”在我国境内开始蔓

收稿日期：2021-03-24

基金项目：安徽省人文社科重点研究项目（SK2020A0262）

作者简介：潘和平（1974-），男，教授，主要研究方向：技术经济与企业管理。

许雨晗（1996-），女，硕士研究生，主要研究方向：信息经济；科学管理研究。

延，智慧城市建设中产生的“非传统安全危机”主要指的是由信息的共享和使用中产生的不安全性引发的信息危机[2]。因此，2012 年住建部出台《关于国家智慧城市试点暂行管理办法》，开始着手建设智慧化城市，由中央牵头建设基础信息网络通信基础设施，逐渐将信息网络安全等十一类非传统安全问题上升到了国家战略层次。此时我国智慧城市建设开始进入探索期，智慧城市发展逐步走上正轨。2016 年以来，5G、大数据、区块链、人工智能等信息技术推动智慧城市建设走向网络化、智能化、数字化等新方向，《中华人民共和国国民经济和社会发展第十三个五年规划纲要》中提出，“以基础设施智能化、公共服务便利化、社会治理精细化为重点，充分运用现代信息技术和大数据，建设一批新型示范型智慧城市”[3]，首次明确“建设新型智慧城市”这一理念，着重强调“新型”是“以人为本”的新的核心特征，建设惠民服务、城市治理、信息资源共融共享三大城市体系，为形成智慧智能、广泛覆盖、精准治理、高效便民、安全有序、生态环保的智慧城市发展新模式指明了发展方向，将新型智慧城市建设与信息网络融合新模式作为未来城市发展的重心。

自我国开展智慧城市建设以来，智慧城市相关政策红利逐步释放，吸引大批社会资本注入，依据 IDC《2019H1 全球半年度智慧城市支出指南》估计，2019 年，我国智慧城市的技术相关投资达到 228.79 亿美元，新型智慧城市建设技术投资同比增长了 14.09%，预估 2020 年同比增长达到 16.26%。在新型智慧城市建设规模扩大的同时，对信息技术的依赖性亦逐步增强[4]，信息的使用与共享加剧了非传统安全的风险问题。

目前，新型智慧城市建设研究主要集中在智慧城市评价体系[1,3,5–9]、智慧城市顶层设计[10–12]、政府开放数据评估[13,14]三个方面的定性研究，而对于新型智慧城市网络信息安全评估方面问题定量研究较少。然而“非传统安全”已成为全球广泛关注的问题，习近平总书记指出：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大群众利益也难以得到保障。”新型智慧城市建设背景下衍生的网络技术失控、信息泄露、网络攻击、信息窃取等“非传统安全”问题日益突出，如何将未知隐患转化为可知问题并对新型智慧城市的网络安全状况进行评估，成为新型智慧城市建设的重要议题。

本文选取 50 个新型智慧城市作为研究对象，从纵向和横向两个角度分别对我国新型智慧城市背景下的“非传统安全”即网络信息安全建设水平进行评估。由于新型智慧城市建设是“以人为本”为核心特点，因此本文采用灰色关联分析从个人、企业、政府三个维度对我国网络安全建设水平的威胁和有效性进行评估；采用聚类分析法通过划分各个城市网络信息安全建设水平的层级，对各层级城市的网络安全建设水平的效用和均衡性进行评估。通过分析各城市网络安全关联度与层级，找出网络安全建设方面面临的重大问题，为未来新型智慧城市建设的网络安全建设提出有益对策。

1　新型智慧城市网络安全评价体系

新型智慧城市的核心特点是以人为本，着重强调人的感觉。新型智慧城市网络安全评价是指导理论和相关实践的一种重要方式，极具应用价值。构建一种代表性强、覆盖面广、典型性好的评估指标体系，关键要保证其可得性、客观性、完整性、科学性。本文研究所采用的研究数据与评价指标选取了由大数据协同安全技术国家工程实验室、提升政府治理能力大数据应用技术国家工程实验室、大数据战略重点实验室、中国赛宝实验室联合发布的《2018 大数据城市网络安全指数报告》，对 50 个新型智慧城市网络安全指数进行评估。上述联合实验室认为城市网络安全建设水平应首先从个人、企业以及政府三个维度进行评估分析，最后再将三者整合为城市的综合安全指数。各指数构成说明如图 1 所示。

（1）个人网络安全指数。主要通过采集和归纳在各城市中的个人用户在移动终端和 PC 终端上所遇见的各主要网络攻击类型，进行综合分析[15]。

（2）企业网络安全指数。在分析我国各城市重点企业整体网络安全性过程中，对所有重点企业使用的信息系统进行全面、多维度的动态监控难以实现，因此选择将重要机构的官方网站公布数据作为一种重要参考，并以官方网站的安全性代表相关企业信息系统的整体安全性[15]。

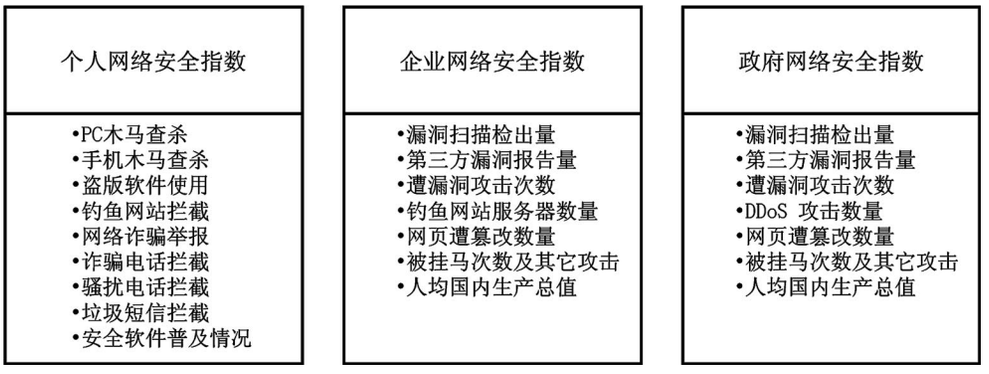

图 1　个人、企业、政府网络安全指数构成图

（3）政府网络安全指数。与企业网络安全指数的确定方法近似，在各城市中，选择具有行使行政管理职能的政府机构网站作为动态监测对象，对遭到网络攻击的多种状况进行分析，并由此形成政府网络安全指数[15]。

2　新型智慧城市网络安全评价及成因分析

2.1　样本选取

本文选取常州、保定、无锡、中山、苏州、杭州、上海、南京、济南、嘉兴、广州、北京、珠海、深圳、乌鲁木齐、唐山、烟台、成都、贵阳、合肥、兰州、长沙、青岛、郑州、东莞等 50 个城市作为研究样本，地区覆盖面广，涵盖了东、中、 西部地区，其经济基础、基础设施建设、政策实施具有显著差异，故选取其作为研究样本。

2.2　灰色关联分析法

新型智慧城市网络安全评价是对一个灰色系统的综合评价[16]，可用灰色关联分析法进行系统分析。灰色关联分析是基于灰色系统理论的一种多因素分析方法，其基本思想是通过对系统参考数列（理想对象）与比较因素数列（实际评价对象）曲线的几何形状相似程度来判断其联系是否紧密，度量各数列因素间关联程度。二者曲线形状越相似，则联系越紧密，其关联性也越大；反之，越不紧密，其关联性也就越小[17]。

在本研究中由于样本量较小且无规律，难以对评价指标关系进行定量化、数字化描述，故采用灰色关联分析法度量新型智慧城市的网络安全评价指标数列与理想指标数列之间的灰色关联系数，进而计算出各数列间的关联度，具体描述各指标间的关联顺序。依据个人、企业、政府网络安全指数三个基本维度，综合分析和评判我国新型智慧城市的网络安全水平，建模设计基本步骤及相应结果分析如下：

（1）确定数列特征值矩阵 X。设 m 个待评价对象，n 个评价指标构成的指标特征值矩阵为 $X=\begin{Bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{Bmatrix}$ 其中，m=1,2,3, …,50；n=1,2,3。

（2）数据的预处理。由于各数列间单位、量级、范围等方面存在差异，为了消除差异进行无量纲化处理以及缩小各变量范围简化计算。即计算出各评价指标均值，用各指标中的元素除以该指标对应的均值得到预处理后的矩阵 $Z_{m\times n}=(z_{ij})_{m\times n}$。

（3）确定系统参考数列 x_0 与比较因素数列 x_i。系统参考序列是反映一个系统行为特征的母序列，选取样本数据各评价指标的最大值构成系统参考序列，记为 $x_0=(x_0(k))^{\mathrm{T}}$（$i$=1,2,3,…,50），比较因素数列是影响一个系统的系统行为因素所构成的子序列，可记为 $x_i=(x_i(k))^{\mathrm{T}}$（$i$=1,2,3;$k$=1,2,3,…,50）。

由于灰色关联分析法的系统参考序列选取是由所有城市的各维度中的最大值所构成，灰色关联度能明确新型智慧城市网络安全在各维度上的发展水平和最优水平间的差距大小。

（4）计算灰色关联系数 $\gamma(x_0(k),x_i(k))$。关联系数（1）（2）计算公式如下。通过计算，得出我国新型智慧城市的网络安全评价指标的灰色关联系数如表 1 所示。

表 1　新型智慧城市网络安全指数评价指标的灰色关联系数

城市	编号	个人	企业	政府	城市	编号	个人	企业	政府
常州市	1	1.000 0	0.615 1	0.553 3	宁波市	26	0.823 4	1.000 0	0.999 0
保定市	2	1.000 0	0.853 2	0.803 2	沈阳市	27	1.000 0	0.6683	0.671 7
无锡市	3	0.678 2	0.981 2	1.000 0	昆明市	28	1.000 0	0.6315	0.621 4
中山市	4	1.000 0	0.756 0	0.723 7	天津市	29	0.499 4	0.6763	1.000 0
苏州市	5	0.530 1	0.913 2	1.000 0	太原市	30	0.934 6	0.6733	1.000 0
杭州市	6	1.000 0	0.631 0	0.590 7	武汉市	31	1.000 0	0.7602	0.628 5
上海市	7	1.000 0	0.818 0	0.866 4	厦门市	32	0.656 4	1.0000	0.968 7
南京市	8	1.000 0	0.733 6	0.885 1	长春市	33	0.535 7	0.8183	1.000 0
济南市	9	1.000 0	0.558 0	0.613 3	石家庄市	34	1.000 0	0.7030	0.576 0
嘉兴市	10	0.922 8	0.729 2	1.000 0	温州市	35	0.712 4	1.0000	0.895 0
广州市	11	1.000 0	0.562 2	0.628 0	廊坊市	36	1.000 0	0.5737	0.554 1
北京市	12	1.000 0	0.519 1	0.486 7	哈尔滨市	37	1.000 0	0.7456	0.773 1
珠海市	13	0.456 0	0.915 1	1.000 0	大连市	38	0.538 0	1.0000	0.636 0
深圳市	14	0.723 1	0.985 5	1.000 0	银川市	39	1.000 0	0.7001	0.753 6
乌鲁木齐	15	1.000 0	0.692 8	0.704 3	西安市	40	1.000 0	0.7240	0.856 0
唐山市	16	0.745 5	1.000 0	0.530 0	佛山市	41	0.333 3	1.0000	0.700 7
烟台市	17	0.542 9	0.900 5	1.000 0	芜湖市	42	0.448 8	0.9945	1.000 0
成都市	18	1.000 0	0.796 5	0.777 9	福州市	43	0.748 5	1.0000	0.799 3
贵阳市	19	1.000 0	0.539 9	0.653 7	海口市	44	1.000 0	0.4348	0.514 9
合肥市	20	0.960 6	0.972 8	1.000 0	惠州市	45	0.360 2	0.9583	1.000 0
兰州市	21	1.000 0	0.526 5	0.512 9	张家口市	46	0.549 9	0.8450	1.000 0
长沙市	22	1.000 0	0.741 3	0.840 7	临沂市	47	0.574 0	1.0000	0.911 0
青岛市	23	0.856 7	1.000 0	0.948 3	重庆市	48	0.480 3	1.0000	0.996 5
郑州市	24	1.000 0	0.659 3	0.665 6	南宁市	49	1.000 0	0.6488	0.577 9
东莞市	25	1.000 0	0.776 6	0.739 9	南昌市	50	1.000 0	0.8070	0.779 4

$$\gamma\left(x_0(k),x_i(k)\right)=\frac{a+\eta b}{\left|x_0(k)-x_i(k)\right|+\eta b} \tag{1}$$

$$\begin{cases} a=\min\limits_i \min\limits_k \left|x_0(k)-x_i(k)\right| \\ b=\max\limits_i \max\limits_k \left|x_0(k)-x_i(k)\right| \end{cases} \tag{2}$$

其中，a，b 分别是两极最小差和两极最大差；η 为分辨系数，$\eta \in (0,1)$，取值一般为 0.5。

（5）计算 x_0 与 x_i 之间的灰色关联度 并评价。通过对关联度的计算和分析，定量化描述系统间各因素的影响程度或各因素对系统主行为的贡献程度[18]。其按照公式（3）计算：

$$\gamma\left(x_0,x_i\right)=\frac{1}{n}\sum_{k=1}^{50}\gamma\left(x_0(k)\quad x_i(k)\right) \tag{3}$$

依据计算出的灰色关联度进行排序，关联度越大，比较因素对系统参考数列的影响越大，反之则越小。其灰色关联度计算结果及排序结果：第一名是个人网络安全指数的关联度，度数为 0.832 2；第二名是政府网络安全指数的关联度，度数为 0.794 7；第三名是企业网络安全指数的关联度，度数为 0.790 8。

当 η 取 0.5 时，计算出的关联度大于 0.6 即认为其关联性显著[13]。通过分析上述各关联度的计算结果可知，在选取的 50 个新型智慧城市网络安全评价指标的关联度范围为 0.790 8~0.832 2，关联度较高，说明我国新型智慧城市在网络安全建设过程中个人、企业、政府等都采取了一系列有效措施。虽然目前我国新型智慧城市网络安全建设仍处于初级阶段，但是无论是从政府层面还是个人层面，都充分重视网络安全建设并开始积极探索。

个人网络安全指数的灰色关联度最高，达到了 0.832 2。该数据说明我国在建设新型智慧城市中个人所使用的网络安全防护取得较大成效，个人网络安全意识有所提升。用户目前普遍通过移动终端与外部社会进行交流，部分用户缺乏信息安全保护意识，个人信息在网络中易被非法搜集、保存、窃听从而导致信息泄露、交易等安全隐患。信息泄露又分为主动泄露和被动泄露。主动泄露是指用户在无意识的状态下泄露信息；被动泄露则是指用户信息被企业和机构收集、使用和售卖。由于新型智慧城市的应用服务商在经济利益驱动下可能会非法采集个人信息同时利益、出售相应信息[19]，商家利用计算机等相关技术对个人网上行为进行分析并依据个人数据精准投放广告，发送垃圾短信和欺诈信息，这种营销手段仅通过目前的网络拦截技术难以全面防范，其面临的安全威胁仍较严重。因此，

个人信息主动泄露仅需通过提升网络安全意识即可效避免，而被动泄露必须依靠技术手段进行防范。各大城市通过综合分析该城市个人用户受到网络攻击状况，采取一系列富有成效的试点措施，例如进行网上教育活动、网络安全线下宣传活动、建立个人信息管理模式等。但主要是从加强个人信息保护意识的角度解决个人网络安全建设问题，网络安全技术机制仍不够完善。

政府网络安全指数的灰色关联度为 0.794 7，说明各城市政府在建设新型智慧过程中逐渐重视保障、管理门户网站、电子政务系统安全建设，弥补网络漏洞，抵御恶意网络攻击。据 CNCERT 抽样监测显示，在政府网站安全方面，2018 年内我国政府网站遭植入后门的数量平均减少 46.5%，遭篡改网站的数量平均减少 16.4%，DDOS 攻击活跃控制端的数量同比下降 46%、被控端数量同比下降 37%，显示我国政府网络总体安全状况较好。因云服务平台具有便捷性、高效性、低成本的特点，我国多地政府部门积极将政务、交通、医疗、环境等社会民生问题融入新型智慧城市网络体系中，形成各市 “互联网 +N” 模式的云平台，但云服务平台存储大量个人隐私、企业运营信息和社会民生数据且利于攻击者使用云平台作为跳板发起网络攻击，故成为黑客攻击的重点，亦是网络攻击的重灾区。目前来看，政府门户网站和云服务平台建设已经较为成熟，但对云服务平台的网络安全系统防护重视不足，忽视云的安全性和可控性可能会引起更大的安全风险问题。同时，社会民生对网络的依赖性随着新型智慧城市发展逐渐增强，社会管理、民生保障等系统中存储了大量政府相关信息，信息共享背景下这些信息被滥用的几率呈倍数增长，这要求政府在管理中予以高度关注。

企业网络安全指数的灰色关联度为 0.790 8，这是我国新型智慧城市网络安全建设方面较为落后的一个维度，但与政府网络安全指数（0.794 7）相差不大。监测结果显示，广东、北京、山东、浙江、上海、山东、陕西等地区由于互联网行业较为发达，资源较好，遭到计算机恶意程序攻击严重、黑客、网络间谍组织非法入侵企业网络窃取商业机密、谋取暴利的问题已经变得极为普遍，如何防御黑客入侵网络成为需要解决的首要目标。新型智慧城市建设为各大企业带来了新的发展机遇，利于各行业进行产业升级，绝大部分城市制定产业结构调整规划，将网络安全信息系统、数据安全审查纳入企业网络安全综合管理体系中。同时，商业领域已经开始通过成立互联网企业安全工作组的方式进行联合防护网络入侵。

2.3 聚类分析

聚类分析是一种通过对多个研究样本的研究特征按照关系的远近进行定量分类的一种多元统计分析方法。利用层次聚类方法对我国新型智慧城市网络安全建设水平进行分类 [20]，可以将建设水平相近的城市划分成一类。

本文通过 SPSS23.0 软件，采用 Q 型聚类分析法，组间联接聚类方法，点间距离采用平方欧式距离，对 50 个新型智慧城市进行聚类分析。通过使用 Excel 软件，根据聚类表中的聚合系数 J（Y 轴）和聚类类别数 K（X 轴）做出其之间的对应关系，如图 2 所示。

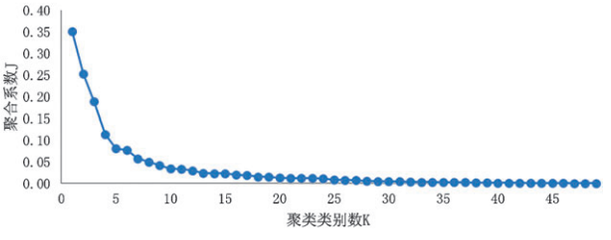

图 2 聚合系数随分类数变化情况

由图可知，当 K=5 时，折线下降趋势趋缓，K 值从 0 到 5 时，畸变程度最大。K 值＞ 5，畸变程度变化显著呈现降低趋势，故可依据 “肘部法则（即依据图 2 大致估计出最优的聚类个数）”，将 50 个新型智慧城市划分为 5 类较为合适。

结合聚类分析树形图（如图 3 所示）可知，将 50 个新型智慧城市划分为 5 类，其聚类结果见表 2。从相应的聚类结果中可以得出，以下五种类型所包含的新型智慧城市数量不同且个数、地域差异较大，相较于人工的划分形式，其表现出不均匀、不整齐的特点。这种特点恰好避免了人为操纵的主观性，保持了聚类分析的客观性。

第 Ⅰ 类城市：常州、中山、杭州、上海、南京、济南、嘉兴、广州、北京、乌鲁木齐、成都、贵阳、兰州、长沙、郑州、东莞、昆明、沈阳、太原、武汉、石家庄、廊坊、哈尔滨、银川、西安、海口二十六个城市。这

表 2　我国新型智慧城市聚类表

类别	Ⅰ类 高水平	Ⅱ类 较高水平	Ⅲ类 一般水平	Ⅳ类 较低水平	Ⅴ类 低水平
城市	常州市、中山市、杭州市、上海市、南京市、济南市、嘉兴市、广州市、北京市、乌鲁木齐、成都市、贵阳市、兰州市、长沙市、郑州市、东莞市、昆明市、沈阳市、太原市、武汉市、石家庄市、廊坊市、哈尔滨市、银川市、西安市、海口市	无锡市、苏州市、珠海市、深圳市、唐山市、烟台市、合肥市、青岛市、宁波市、天津市、厦门市、长春市、温州市、大连市、福州市	保定市、南宁市、南昌市	佛山市、芜湖市、惠州市、重庆市	张家口市、临沂市

类城市综合指数在 0.580~0.777 之间，均值达到 0.657，个人、政府、企业网络安全指数均居于前列，属于网络安全高水平的城市，各方面发展较为均衡。大部分城市属于泛珠三角地区，经济水平较为发达，为网络安全建设提供动力支持。政府部门以举行国家网络安全宣传周活动等多种方式，让个人以更直观的方式积极参与到网络安全防护的活动

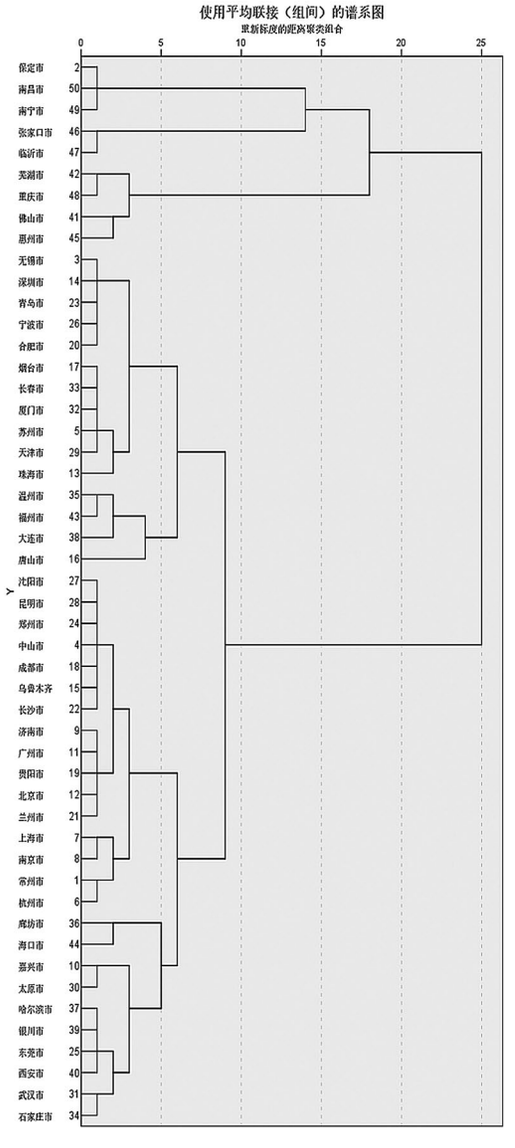

图 3　聚类分析树形图

中去，不仅提升人民网络安全防范意识，同时学习网络安全方面的知识。从效用角度看，个人网络安全意识较高，但被动泄露信息的问题仍未得到解决。我国于 2018 年提出进一步优化网信管理体系，切实保障网络安全建设、促进互联网健康、有序、协调、绿色发展。除廊坊市以外，其余各市由政府、企业、个人、团体以联合组建计算机信息网络安全相关协会的形式，积极宣传政府制定有关网络安全方面的法律法规、推进网络安全建设等，网络安全建设成果显著。绝大部分城市设立了网络安全教育、安全管理、预警平台保障个人用户、企业、政府的上网安全，提供网络监控服务。如：沈阳市于 2016 年致力于构建我国首个大数据互网安全预警平台有望提升智慧城市信息系统及基础设施可控、预测水平。常州市提出 “企业上云”建设，以云计算技术提升企业信息化程度和水平，保障云服务平台的用户信息。上海市在 2017 年 3 月底试运行国内首个区域性网络安全态势感知和应急处理平台，紧接着广州、长沙等城市也开始构建该类平台。与此同时，杭州、成都、郑州、贵阳、长沙、贵阳、东莞、太原、哈尔滨等市编制了该市信息安全产业发展相关规划，以引导该市网络安全产业持续健康发展，保障互联网安全。武汉市建设国家首个网络安全人才与创新基地项目，意味着由中央网信办扶持的 “国家网络安全人才与创新基地” 整体进入实质性建设阶段。以上这些措施在短短近五年的时间内实行，取得成果十分显著，各地之间对网络安全建设所采取措施均衡高，该类城市问题仅在于个人信息被动泄露该如何解决。

第Ⅱ类城市：无锡、苏州、珠海、深圳、唐山、烟台、合肥、青岛、宁波、天津、厦门、长春、温州、大连、福州十五个城市。这类城市综合指数在 0.582~0.736 之间，均值达到 0.651，属于网络安全较高水平的城市。在活动构建方面，网络安全平台类建设和国家网络安全宣传周活动的数量较少，

创新度不高，仅厦门成立了首批“网络安全志愿者队伍”，积极鼓励个人参与到网络安全保护活动中。在平台建设方面，除唐山、烟台、天津、温州市以外，其他城市已建立网络安全类协会，以保障互联网上网安全，维护国家以及个人用户利益。但从成效来看实行效果不太显著，仍有待改进。在该类中一半以上的城市都结合本地优势制定具有当地特色的专业性政策文件。例如，无锡市印发《无锡市推进新型智慧城市建设三年行动计划（2018—2020年）》注重提升无锡市整体网络安全的综合治理，保障重点区域信息资源的安全以及个人用户、企业和政府的信息安全。其他各市政策规划与此类似。苏州市还通过设立该市信息等级安全网，将政府有关部门的工作动态、各行业的行业动态以及网络安全预警分块展示，推行信息系统安全等级保护；大连市首次举办聚焦网络安全人才与创新发展议题的高峰论坛，并于 2017 年 4 月 25 日正式成立信息安全创新中心，推动大连市信息化产业发展。该类城市活动、政策推行时间较晚，特色虽较为鲜明，但仍需加强政策执行力度，提高实施效果。

第Ⅲ类城市：保定市、南宁市、南昌市三个城市。这类城市综合指数 0.483~0.750 之间，均值达到 0.575，属于网络安全一般水平的城市。这类城市综合指数跨度较大，仅保定市达到了 0.750，余下两个城市该值位于 0.488 左右。这三个城市仅只有保定市积极召开网络安全百日攻坚行动推进会，贯彻落实《关于集中开展信访、稳定、安全生产、食品药品安全、网络安全百日攻坚行动的通知》精神，着重解决网络中存在的安全保障问题，该类城市主动性不足。在平台建设方面，仅南宁市于 2017 年通过建设信息安全监测预警平台来保障维护、实时监控并预警网络安全。南昌市并没有提出结合本市特色的政策性规划，其他城市均未提出具体的规划措施。该类城市虽采取一些措施，但有效措施数量略少，各地各方面措施实行均衡度一般，具有当地特色的政策数量较少。

第Ⅳ类城市：佛山市、芜湖市、惠州市、重庆市四个城市。这类城市综合指数在 0.510~0.584 之间，均值达到0.564，属于网络安全较低水平的城市。此四市均成立了网络安全类协会，保障个人、企业、政府三者的信息系统、网站安全。且响应国家号召，国家网络安全宣传周活动除惠州市以外，均开展该项活动。但在平台建设方面，仅只有佛山市成立网络举报平台，该平台功能性较弱，具有一定的局限性，其余城市均未建立与网络安全相关平台。该类城市虽含括互联网企业数量较多，但是个人用户的网络安全意识不足，国家政策推行力度不够，地方政府制定相关政策文件较少，各地各方面措施实行均衡度较低。

第Ⅴ类城市：张家口市、临沂市两个城市。这类城市综合指数在 0.518~0.533 之间，均值达到 0.526，属于网络安全低水平的城市。这两个城市位于我国东部地区，人口众多，社会需求大。但这两个城市仅成立了互联网行业协会对国家互联网有关的政策和规划进行分析、维护个人用户、企业、政府信息安全，这类城市网络安全基础设施建设较为薄弱且缺乏对个人用户、企业、政府信息保护意识，地方政府对于信息安全重视程度低，应变能力较差，各地各方面措施实行均衡度较低。

3 结论与建议

2016 年以来，新型智慧城市建设成为我国城市建设潮流和趋势。对于城市逐渐从智能化转化为智慧化再转化为新型智慧化的发展过程中，我国已经取得了不小的成就。然而，网络安全威胁仍然普遍存在，已经成为制约新型智慧城市发展的最主要因素。

通过上述研究，揭示出我国新型智慧城市网络安全建设水平存在地区不协调性和三个维度的不平衡性两大特征。从灰色关系分析中可得出，三个维度的发展差距并不大，但是企业网络安全建设较为落后，且与个人、政府联系不够紧密。从聚类分析结果可以看出：从高水平、较高水平、一般水平、较低水平和低水平，划分为五类城市，各类城市网络安全建设水平差距较大，发展很不平衡。针对各维度和各类城市网络安全中普遍存在的主要问题，建议从以下方面采取有效措施：

首先，政府应当发挥其主导作用。地方政府需提高对网络安全的重视程度，明确网络安全责任与义务，并依据区域优势制定相应方针、政策，通过鼓励、引导、奖励、协作的方式，联合企业协作建设监测预警、应急指挥、评估审查、安全态势感知的网络

安全平台，打破新型智慧城市建设造成的信息壁垒、“信息孤岛”，实现数据和信息的互通共享。目前，构建新型智慧城市有三种模式：政府负责投资运营，企业参与建设；政府企业合作建设，企业购买服务；政府统筹规划，企业自投自营[21]。企业是新型城市建设的重要参与者，与互联网企业合作是解决网络安全建设问题的最好出路。整合新型智慧城市信息系统中存储的大量信息和数据，形成一套富有成效的监管体系。

其次，从技术层面出发，进行技术优化，完善技术保护机制，配置整体联动的网络安全体系。对敏感、机密信息加密，妥善保存好密钥，可有效防范黑客窃听、拦截及篡改。将个人信息系统和通信系统的认证设置为至少经过账号、密码的认证才能存取[22]，若想进一步提高安全性，提高认证设置等级即可。同时，在网络边界区域设置入侵防御系统，精准针对病毒侵扰、木马后门、漏洞攻击等手段进行监测和防御[23]。对于新型智慧城市广泛应用的云服务平台安全系统构建，云服务商必须提供基础性的网络安全防护措施，承担相应的主体责任，对云用户的信息安全负责。

第三，在新型智慧城市的建设背景下，个人、政府、企业对网络的依赖性提升，加强网络安全意识、增强网络安全宣传力度、提高网络安全素质就变得十分重要，对网络安全和信息安全进行分级保护，注重培养网络安全人才和员工培训，全面构建网络安全观以弥补安全意识不足的缺陷。

最后，围绕构建新型智慧城市网络安全保障体系，重点加大国内新一代信息技术产业资金投入，扶持本土信息产业发展，紧握核心技术以保障城市网络安全。通过综合考量各城市发展条件，采用分级分类制构建各类城市整体保障技术体系，提升我国企业整体运维保障能力，以应对“非传统安全”危机。

参考文献：

[1] 张梓妍，徐晓林，明承瀚 . 智慧城市建设准备度评估指标体系研究 [J]. 电子政务，2019（2）：82–95.

[2] 余潇枫，潘临灵 . 智慧城市建设中“非传统安全危机”识别与应对 [J]. 中国行政管理，2018（10）：127–133.

[3] 任亮，张海涛，魏明珠，等 . 基于熵权 TOPSIS 模型的智慧城市发展水平评价研究 [J]. 情报理论与实践，2019，42（7）：113–118，125.

[4] 毛子骏，梅宏，肖一鸣，等 . 基于贝叶斯网络的智慧城市信息安全风险评估研究 [J]. 现代情报，2020，40（5）：19–26，40.

[5] 胡军燕，修佳钰，潘灏 . 基于面板数据的城市智慧度评价与分类 [J]. 统计与决策，2020，36（7）：76–80.

[6] 崔璐，杨凯瑞 . 智慧城市评价指标体系构建 [J]. 统计与决策，2018，34（6）：33–38.

[7] 郭曦榕，吴险峰 . 智慧城市评估体系的研究与构建 [J]. 计算机工程与科学，2013，35（9）：167–173.

[8] 项勇，任宏 . 基于 ANP–TOPSIS 方法的智慧城市评价研究 [J]. 工业技术经济，2014，33（4）：131–136.

[9] 王振源，段永嘉 . 基于层次分析法的智慧城市建设评价体系研究 [J]. 科技管理研究，2014，34（17）：165–170.

[10] 孙玉婷，王芙蓉，吴掠桅，等 . 智慧城市顶层设计管理与可视化研究实践 [J]. 科技导报，2018，36（18）：55–62.

[11] 房毓菲，单志广 . 智慧城市顶层设计方法研究及启示 [J]. 电子政务，2017（2）：75–85.

[12] 陈德权，王欢，温祖卿 . 我国智慧城市建设中的顶层设计问题研究 [J]. 电子政务，2017（10）：70–78.

[13] 陈伟清，陆恩旋，曾弋戈，等 . 基于灰色关联理论和系统聚类分析的智慧城市政府数据开放水平评价研究 [J]. 数学的实践与认识，2020，50（6）：43–52.

[14] 陈伟清，史丽娜，吕冬妮，等 . 基于灰色关联聚类分析的智慧城市建设领域发展水平实证研究 [J]. 科技管理研究，2017，37（6）：59–64.

[15] 大数据城市网络安全指数报告 [J]. 信息安全与通信保密，2017，（08）：96–118.

[16] 温丽华 . 灰色系统理论及其应用 [D]. 哈尔滨：哈尔滨工程大学，2003.

[17] 金玉石 . 基于灰色关联模型的省域技术创新能力测度 [J]. 统计与决策，2019，35（4）：59–62.

[18] 林卓，郑丽霞，曹玉婷，等 . 福建省创新型城市建设综合评价——基于 AHP– 熵权的灰色关联分析 [J]. 科技管理研究，2019，39（19）：115–123.

[19] 范渊 . 网络安全是智慧城市健康发展的根基 [N]. 中国建设报，2019–05–31（7）.

[20] 任利成，张明柱 . 我国智慧城市发展水平的聚类分析 [J]. 科技管理研究，2014，34（14）：58–62.

[21] 樊婷婷 . 地方政府推动新型智慧城市建设中的问题与对策研究——以河北省衡水市为例 [D]. 石家庄：河北师范大学，2020.

[22] 张晓艺 . 智慧城市的网络安全策略 [J]. 计算机与网络，2019，45（16）：55.

[23] 薛中伟 . 企业内部网络常见安全问题及对策方法 [J]. 网络安全技术与应用，2020（7）：111–112.