广东省数字政府网络安全评估体系与实践

Practice of digital government network security index evaluation system in Guangdong Province

高尚省（1977- ），男，广东省政务服务数据管理局副局长，主要研究方向为政务信息化、数字政府网络安全。

郭勇（1977- ），男，就职于广东省政务服务数据管理局安全管理处，主要研究方向为数字政府网络安全、密码应用及安全。

高智伟（1981- ），男，博士，广州赛宝认证中心服务有限公司高级工程师，主要研究方向为网络安全、云计算安全、数据安全与治理等。

钟世敏（1979- ），男，就职于数字广东网络建设有限公司，主要研究方向为数字政府网络安全、云计算安全。

中图分类号：D668 文献标识码：A doi: 10.11959/j.issn.2096-0271.20210021

刘丕群（1989- ），男，广州赛宝认证中心服务有限公司高级工程师，主要研究方向为网络安全防护与管理、云计算安全、数据治理等。

刘婷（1989- ），女，广州赛宝认证中心服务有限公司工程师，主要研究方向为政务信息化、网络安全管理等。

1 引言

《2020联合国电子政务调查报告》显示[1]，全球电子政务整体发展水平不断提升，数字政府转型快速推进，在线政务服务水平普遍提高，数据治理框架不断完善。随着数字政府建设的不断推进和深化应用，网络安全面临的风险和挑战不断增加。世界各国纷纷在国家战略的要求和指导下制定了与互联网相关的法律或命令，互联网发展越早、越成熟的国家，对网络安全的治理越关注，例如美国、日本已经发布了国家级网络安全战略等[2]。

政府数字化转型的本质是推进政务数据的整合、开放和共享[3]，然而政务业务和数据的融合加大了网络安全防护的难度[4]，网络安全治理成为我国数字政府建设的重点[5]。为了防范和化解广东省数字政府网络安全风险，提高风险预见、预判能力，有必要对数字政府网络安全防护现状进行评估，促进全省各地市迭代建设网络安全防护体系，提升整体安全防护能力。

2 数字政府面临的网络安全风险分析

随着信息技术的快速发展、国际形势的日趋复杂，网络安全已成为我国面临的极度复杂、极度现实、极度严峻的非传统安全问题。数字政府在网络安全方面也随之暴露出愈来愈多的风险隐患，其网络平台和信息系统中存有大量关于国家和政府机密的相关数据文件信息，存在系统破坏、数据窃取、信息泄露等安全风险。

从网络安全管理的角度来看，数字政府存在内部威胁和外部威胁[6]。如果地方政府没有意识到网络安全的重要性，就极容易在日常工作中忽视网络安全管理的作用，出现员工操作失误、机构及服务提供商责任不清等很多非技术性的安全问题。另外，病毒、黑客等外部网络攻击也占据了相当大的比例，当前，全国已有多个重要部门遭到勒索病毒的攻击，损失严重，影响

十分巨大。

从建设与运营的角度来看，数字政府网络安全风险体现在以下多个方面：一是部分地方政府和相关部门的系统平台建设仅停留在功能层面，缺乏网络安全顶层设计和防护规划，存在被非法入侵的隐患；二是对关键信息基础设施概念的理解不准确，未能建立资产档案，未落实强化核心人员管理、整体防护、监测预警等重点保护措施，难以开展有针对性的安全建设工作；三是对大数据安全、云计算环境下“政企合作，管运分离”的管理安全、数据上云后的“分确三权”等问题关注不够，导致大数据安全治理能力低下，这极大地威胁了政务数据安全[7]；四是监控和监测的全面性和及时性不到位，具体表现为安全监测不成体系、监测数据未能及时报送、数据备份与恢复测试不足、难以快速有效地做好应急响应以保障业务连续性；五是多采用被动的网络安全防御机制，对政务系统平台遭受网络攻击的预测和风险分析缺乏实时、定量的数据计算分析手段。

3 数字政府网络安全指数评估

“十三五”期间，广东省率先开展数字政府建设，连续两年在省级政府网上政务服务能力指数评估中位列全国第一。与此同时，广东省政务外网时刻面临着安全威胁，这对数字政府网络安全工作提出了更高的要求。为了实现数字政府网络安全工作由“看不见、摸不着”向“可量化、可评估”转变，由广东省政务服务数据管理局牵头组织、工业和信息化部电子第五研究所负责、华为技术有限公司等多个单位共同参与，设计并构建了数字政府网络安全指数评估指标体系，针对广东省21个地市开展第三方评估。

3.1 评估原则

● 客观性。本次评估依托网络安全监管部门掌握的与数字政府安全相关的监管数据、网络安全厂商及互联网公司掌握的地区安全大数据、“粤盾”数字政府实战攻防演练结果数据，采用定量和定性相结合的分析方法，对全省各地市数字政府的网络安全管理、安全建设、安全运营、安全效果等方面进行评价，客观科学地反映各地市数字政府网络安全的整体防护水平。

● 导向性。本次评估以“责任明确、保障有力、安全合规、重点到位、协同有效”为导向，通过建立指标体系，全面评价各地市数字政府的网络安全水平，引导、鼓励各地市持续加强网络安全体系建设，推动全省数字政府网络安全建设迈向新阶段、实现新跃升。

● 实效性。本次评估按照“以评促管、以评促建、以评促改”的原则，注重数字政府网络安全管理、建设、运营的实际成效，帮助各地市全面掌握当前数字政府安全现状，发现存在的问题，找到解决方案，快速提升网络安全整体水平，形成“执行-评估-反馈-改进”的管理模式。

3.2 评估指标体系

数字政府网络安全指数评估指标体系从安全管理、安全建设、安全运营、安全效果4个方面进行评价[8-9]，包含24个二级指标，三级指标为具体评估要点，共70项。前两级指标体系如**图1**所示。

（1）安全管理

安全管理方面包含安全战略规划、安全政策规范、安全意识、安全投入、安全管理组织、安全管理人员、供应链安全管理，涉及战略、政策、意识、投入、组织、人员

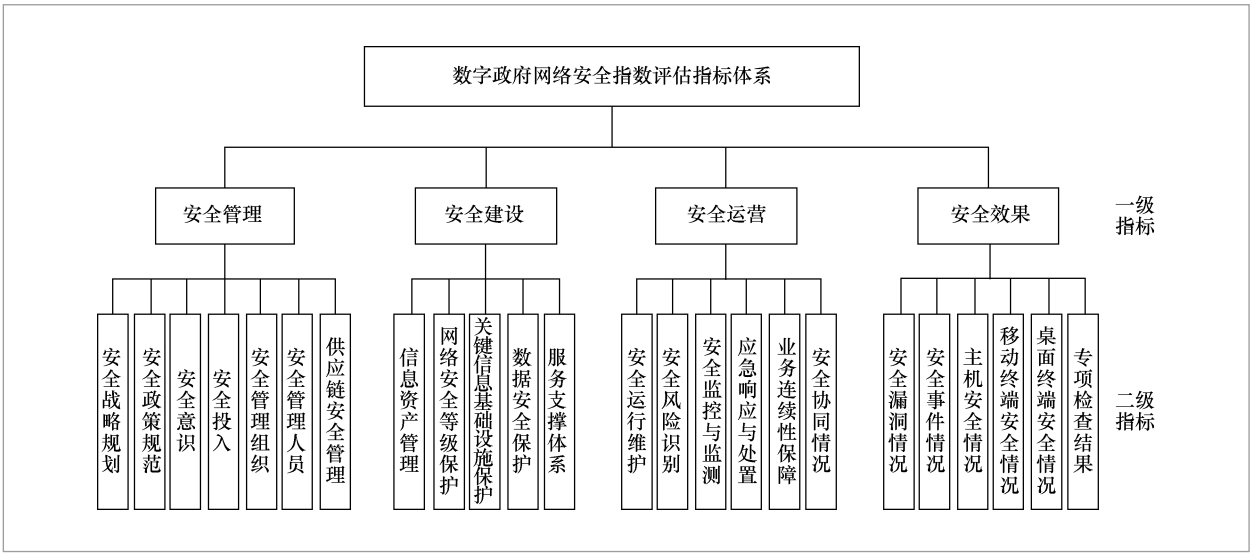

图1 数字政府网络安全指数评估指标体系

等管理工作的众多要素。

(2)安全建设

安全建设方面包含信息资产管理、网络安全等级保护、关键信息基础设施保护、数据安全保护、服务支撑体系，重点是摸底，有针对性地开展安全建设工作。

(3)安全运营

安全运营方面包含安全运行维护、安全风险识别、安全监控与监测、应急响应与处置、业务连续性保障、安全协同情况，重点是及时、全面地了解安全事件，控制安全风险，做好应急响应。

(4)安全效果

安全效果方面包含安全漏洞情况、安全事件情况、主机安全情况、移动终端安全情况、桌面终端安全情况、专项检查结果，侧重从结果的角度进行评价，反映数字政府在安全管理、安全建设及安全运营等方面实施的效果和价值。

3.3 评估数据来源

本次评估的数据采集对象涵盖全省21个地市政府部门，涉及各地市政务云平台、大数据中心、官方网站及重要政务应用等。数据来源主要为：问卷调研，数字政府安全运营数据，网络安全监管部门的监管数据，网络安全厂商、互联网公司、科研机构掌握的安全大数据。

本次评估对全省21个地市在数字政府网络安全管理、建设、运营、效果等方面进行了调研，采集了21个评估对象涉及的人员、机构、制度、经费、系统，以及安全运行维护、安全大数据监测、安全应急与通报、攻防演练等相关数据约4.4万项。

3.4 评估结果

数字政府网络安全指数评估总分为100分，其中安全管理为25分、安全建设为20分、安全运营为25分、安全效果为30分。为了验证评估指标体系的可行性和有效性，本文选取广东省21个地市开展试点评估。

通过评估，获得了较为完备的试点地市数字政府网络安全状况的数据，各地市

一级指标指数和总体指数得分及排名情况如**图2**所示。

整体来看，全省数字政府网络安全指数平均值为53.81，仍有较大的提升空间。深圳、广州、东莞、佛山、珠海、江门、汕头、惠州8个地市得分高于平均值，占比38.1%。其中，深圳以总体指数得分73.99居全省榜首，广州、东莞、佛山、珠海分列第2~5名，总体指数得分分别为71.01、68.71、66.64、62.59。结合2020年前三季度GDP来看，各地市数字政府网络安全指数排名基本与GDP排名一致，但也存在GDP数据与安全指数得分倒挂的情况。

4 评估发现与展望

4.1 评估发现

2020年，广东省各地市数字政府网络安全指数评估指标体系初步建立，在安全管理、安全建设、安全运营等方面持续推进，并取得了一定成效。但从评估结果来看，当前网络安全工作存在诸多不足，整体安全能力仍需进一步提升。

评估发现，全省大部分地市制定了网络安全总体规划或制度规范，建立了网络安全工作管理机构，但在实际工作中对网络安全重视不足，责任划分不够明确；各地市数字政府网络安全建设高度重视安全合规工作，积极贯彻落实等级保护制度，普遍采购风险评估、等保测评等基础安全服务，但安全建设还不扎实，安全工作仍有不足；大部分地市定期开展网络安全风险评估，持续推进政务系统安全巡检和防护策略升级，初步实现了网络安全运营工作的上下协同，但网络安全运营能力和运行机制还不健全；2020年各地市被监管机构通报的高中危漏洞数量相比2019年明显下降，数字政府未发生较大及以上等级的网络安全事件，但在“粤盾”2020数字政府网络安全攻防演练活动中，各地市暴露了大量安全隐患。

4.2 工作展望

数字政府的高质量发展需要不断优化的安全治理架构和坚实的网络安全防护能力体系支撑。广东省要做好数字政府改革建设工作，必须夯实数字政府网络安全基

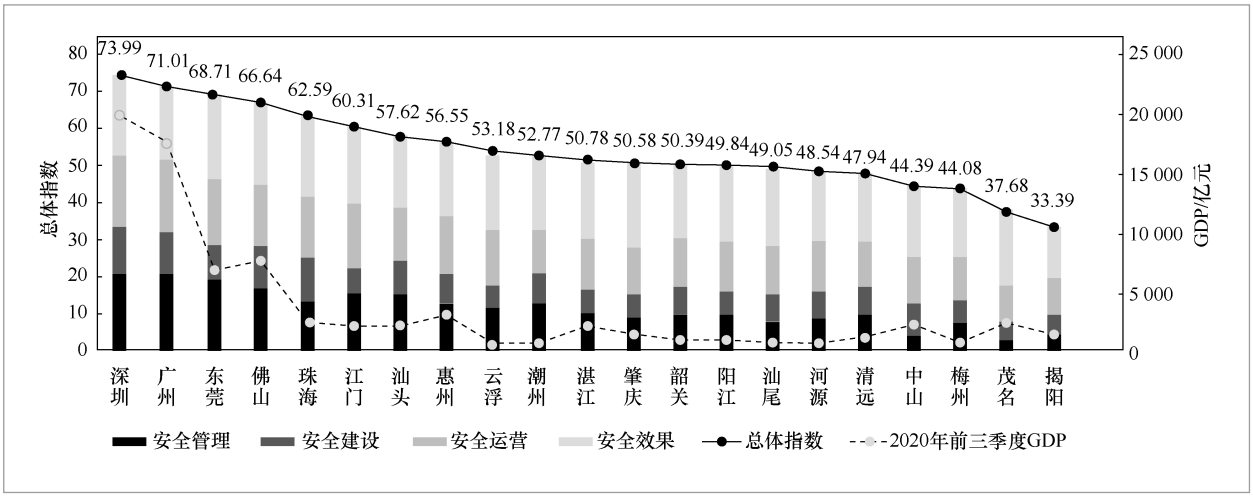

图 2 广东省各地市数字政府网络安全指数排名

础，构建完善的网络安全防护体系，持续提升网络安全防护能力。

建议全省各地各部门重视网络安全规划，加强安全管理，构建高效、协同的安全管理体系；明确安全责任分工，强化安全建设、运营过程监督管理，形成规划设计、建设运行、监督评价和持续改进的良性循环；建立健全数字政府信息资产发现、跟踪、管理机制，加强资产管理，聚焦数据安全，做好数据分类分级及全生命周期安全管理工作；做好安全监测预警，完善预警通报机制，健全安全应急处置机制，确保数字政府安全稳定运行；发展完善数字政府网络安全产业生态，促进技术交流与合作，打造优势互补的网络安全能力体系；加大安全投入，落实资源保障，将安全指数评估纳入绩效考核，形成常态化绩效考核机制。

5 结束语

本文介绍了数字政府网络安全面临的主要风险，提出了数字政府网络安全指数评估指标体系，遵从客观性、导向性、实效性等原则，从安全管理、安全建设、安全运营、安全效果4个方面对广东省21个地市的数字政府网络安全防护工作进行了评估，提出了评估工作中发现的各地市数字政府网络安全防护工作现状，并对未来整体安全防护工作进行了展望，旨在促进各地、各部门不断提升数字政府整体安全防护水平，为相关决策制定提供参考。

本次评估工作是创新性的工作探索，后续将持续优化指数评估工作，完善指标体系和评估方法，增加可信数据来源，提升数据准确性、及时性和全面性，为数字政府安全建设提供有力支撑。

参考文献:

[1] 王益民. 全球电子政务发展前沿与启示——《2020联合国电子政务调查报告》解读[J]. 行政管理改革, 2020(12): 43-49.
WANG Y M. Frontiers and enlightenment of global e-government development: interpretation of the UN e-government survey 2020[J]. Administration Reform, 2020(12): 43-49.

[2] 周丽娜, 陈晴. 国外网络信息安全治理体系现状及启示[J]. 社会治理, 2020(9): 71-78.
ZHOU L N, CHEN Q. Status and enlightenment of foreign network information security management system[J]. Social Governance Review, 2020(9): 71-78.

[3] 金澈清, 陈晋川, 刘威, 等. 政府治理大数据的共享、集成与融合[J]. 大数据, 2020, 6(2): 27-40.
JIN C Q, CHEN J C, LIU W, et al. Sharing, integration and fusion of governmentgovernance big data[J]. Big Data Research, 2020, 6(2): 27-40.

[4] 杨孟辉, 杜小勇. 政府大数据治理：政府管理的新形态[J]. 大数据, 2020, 6(2): 3-18.
YANG M H, DU X Y. Big data governance in governments: a new form of the government administration[J]. Big Data Research, 2020, 6(2): 3-18.

[5] 安徽省数据资源管理局电子政务与应用处. 安徽省智慧政务新模式及典型应用[J]. 大数据, 2020, 6(2): 107-112.
E-Government and Application Office, Anhui Data Resources Administration. New model and typical application of smart government in Anhui Province[J]. Big Data Research, 2020, 6(2): 107-112.

[6] 陈宏, 丛凯, 苏征. 浅谈基于“数字政府”背景下的电子政务网络安全研究[J]. 数字通信世界, 2020(8): 152-153.
CHEN H, CONG K, SU Z. Research of the e-government network security based on the background of “digital government”[J].

Digital Communication World, 2020(8): 152-153.

[7] LUO H N. An emergency management system for government data security based on artificial intelligence[J]. Ingénierie des Systèmes D Information, 2020, 25(2): 207-213.

[8] 全国信息安全标准化技术委员会. 信息安全技术网络安全等级保护基本要求：GB/T 22239-2019[S]. 2019.
National Information Security Standardization Technical Committee. Information security technology-baseline for classified protection of cybersecurity: GB/T 22239-2019[S]. 2019.

[9] 全国信息安全标准化技术委员会. 信息安全技术信息安全保障指标体系及评价方法：GB/T 31495-2015[S]. 2015.
National Information Security Standardization Technical Committee. Information security technology-indicator system of Information security assurance and evaluation methods: GB/T 31495-2015[S]. 2015. □