目　录

前言

前 言

2021 年，赛迪顾问针对国内城市数字化转型过程中网络安全的建设和运营情况，设计了城市数字化网络安全评价指标体系，并且调研了近百个城市的网络安全状况，在对相关资料进行收集分析后，结合指标体系对中国各城市进行科学评估，得出 2021 城市数字化网络安全指数榜单 TOP30，并在此基础上形成了《城市数字化网络安全评价指数白皮书（2021）》。

今年，百年变局和世纪疫情交织叠加，国际环境日趋复杂，全球产业链供应链遭受冲击，网络空间安全面临的形势持续复杂多变。此外，随着数字化、网络化进程加快，城市资产暴露面不断扩大，安全漏洞、数据泄露、网络诈骗等风险持续增加。在此背景下，数字城市建设、运营和治理等方面的工作重心发生了哪些变化？数字城市网络安全建设是否有了新的进展？是否满足城市自身数字化转型对网络安全保障的要求？又有哪些城市的网络安全建设与运营经验值得我们借鉴？这些都是我们进一步提升数字城市网络安全能力应该关注的重点。

因此，赛迪顾问在调整优化了部分指标后再次启动了《数字城市网络安全评价指数白皮书（2022）》的研究和撰写工作。期望借助此次研究进一步全方位评估数字城市网络安全的体系化管理、建设及运营能力，寻找优秀的建设理念和经验，为我国城市数字化转型过程中的网络安全建设提供方向指引。

数字城市网络安全发展背景

- 数字城市建设不断加快，运营与安全成为新的关注焦点
- 数字城市网络安全建设仍处于初级阶段

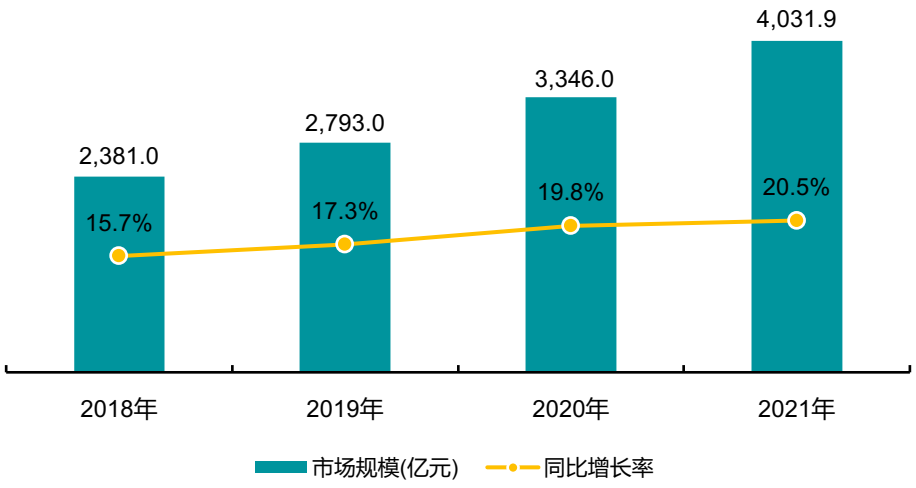
一 数字城市网络安全发展背景

（一）数字城市建设不断加快，运营与安全成为新的关注焦点

1、数字城市建设步伐不断加快

经过改革开放四十多年的发展，我国城市基础设施建设不断完善，城市发展重心逐步从建设向治理转移。智慧城市建设作为推动治理体系和治理能力现代化的重要抓手，受到各级政府广泛关注与高度重视。2021 年，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》发布，明确提出“加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革”。中国各地政府亦加快数字化建设步伐，提升城市数字化水平。全国多地发布“十四五”新型智慧城市、数字政府、数字经济等发展规划，引发数字城市建设“新浪潮”。2021 年，中国数字城市市场投入规模达到 4031.9 万亿，同比增长 20.5%，四年内增长率持续上升。

图 1　2019-2021 年中国数字城市市场规模及增长率



数据来源：赛迪顾问，2022.06

2、数字城市建设迈向集约化、融合化与一体化

从 2016 年新型智慧城市概念的提出之后，中国智慧城市建设正式有序开展，这个阶段的重点是推动大数据中心、通信网络、智慧交通等基础设施建设；2018 年以后，智慧城市在技术上开始朝着平台化方向发展，推动城市变革原来各部门分散建设分散管理的信息化发展模式。此外，政府推进公共服务的智慧化建设应用，智慧电力、智慧医疗、智慧交通、智慧金融等智慧应用遍地开花。2020 年新冠肺炎疫情开始蔓延，智能化、数字化手段加快赋能，城市治理水平更加高效精准。当前，我国智慧城市建设已进入全面提升新阶段，以组织扁平化、数据共享化、业务协同化为切入点，向着集约化、融合化、一体化加速迈进。

3、泛城市安全及数据安全在数字城市建设中放到突出的位置

智慧城市的深入推进，使得城市发展方式发生了深刻变化，城市运行系统日益复杂，信息资源高度集中、共享，安全风险也随之不断增大，“城市公共安全”“生产安全”“应急安全”“数据泄露溯源”“个人信息及隐私保护”等成为关注焦点。2022 年，随着《网络安全法》《数据安全法》《个人信息保护法》的深入实施，城市运行安全的重要性将进一步凸显，包括生产安全、公共安全、信息安全等在内的泛城市安全将备受关注。做好与基础设施、数据资源、信息系统等相关的网络安全监测预警、应急处置以及灾难恢复保障，提升应对网络安全、风险管理和运营保障的能力，将成为数字城市建设的重中之重。

（二）数字城市网络安全建设仍处于初级阶段

1、网络攻击行为不断攀升，智慧城市网络安全事件愈演愈烈

随着“智慧城市”“新基建”等战略的持续推进，5G、工业互联网、边缘计算等技术的快速发展，物联网与关键信息基础设施深度融合，在提高行业运行效率和便捷性的同时，也面临严峻的网络安全和数据安全挑战。近年来，全国范围内针对智慧城市，特别是城市关键信息基础设施的网络攻击行为不断攀升，涉及金融、医疗卫生、交通、电力、能源、工业控制等多个领域，影响范围广泛、程度严峻。针对智慧城市的网络攻击一般通过入侵和感染联网设备、重要系统，造成设备破坏、系统崩溃、敏感数据丢失等后果，以实现对城市关键信息基础设施的破坏性打击。

表 1　2021 年中国主要智慧城市安全事件

序号	时间	安全事件
1	2021 年 1 月	国内多家安全厂商检测到蠕虫病毒 incaseformat 在国内大范围爆发，涉及政府、医疗、教育、运营商等多个行业，且感染主机多为财务管理相关应用系统，表现为所有非系统分区文件均被删除。
2	2021 年 3 月	中国台湾 PC 制造厂商宏碁遭黑客入侵被勒索赎金 5000 万美元，赎金约合人民币 3.25 亿元。
3	2021 年 5 月	澳门卫生局电脑系统遭恶意攻击，影响健康码、医疗券、新冠病毒疫苗和核酸检测等系统的正常运作。
4	2021 年 5 月	西安某医院网络系统持续出现故障，导医台、诊室系统等网络设备无法正常联网，医院诊疗秩序受到破坏。经院方网络工程师初步排查，医院网络系统重要文件疑似被人为更改，诊疗系统全面瘫痪。
5	2021 年 8 月	中国台湾电脑巨头技嘉遭勒索软件攻击，上百 GB 数据失窃，导致技嘉公司的系统被迫关闭，多个网站受到影响。

数据来源：赛迪顾问整理，2022.06

2、我国智慧城市网络安全投入占比仍旧较低

近年来，我国智慧城市建设在经过概念普及、政策推动、试点示

范后已进入爆发式增长阶段。智慧城市、信息惠民、宽带中国等智慧城市相关试点已超过 700 个，开展新型智慧城市顶层设计的省会城市及计划单列市、地级市已分别达 94%、71%，2021 年全国智慧城市投资总规模超过 2 万亿元，占全国固定资产投资比例为 3.7%。然而，相对于智慧城市投入规模和日渐成熟的建设思路，与之相适应的网络安全建设还非常不充分，2021 年全国智慧城市网络安全投入占智慧城市整体投入的比例还不足 8%。大多数城市只考虑数字化助力城市发展的巨大作用，而忽略安全保障没跟上所带来的巨大风险，仅采用“先建设、后安全补课”的思路来建设，导致当前网络安全建设投入和建设思路已无法保障智慧城市的平稳运行。不过近年来也有越来越多的城市意识到智慧城市安全建设的重要性，重庆、天津、珠海、青岛、苏州、郑州、上海、鹤壁、成都等城市都先后将网络安全建设纳入到智慧城市的整体建设思路中去。

3、数据泄露、入侵攻击成为智慧城市面临的主要安全风险

智慧城市中涉及大量的城市公共数据及市民个人信息数据的共享使用，因此，在数据集中存储和边界互联互通等场景下，存在较大的数据泄露风险，以及由于企业重要信息和个人隐私信息管理不严带来的隐私数据泄露和滥用风险。在城市关键信息基础设施方面，可能存在由于自身安全性不足或受外部入侵攻击等影响带来的应用/服务不可用风险。此外，智慧城市的网络和物联网设备也是极易被攻击的对象，一旦网络或物联网设备遭受攻击，将造成大规模网络服务不可用及物联网设备失效或瘫痪风险。

表 2　智慧城市各层级面临的主要安全风险

智慧城市各层级	主要面临的安全风险
智慧应用层	✓ 应用不可用风险 ✓ 隐私泄露风险 ✓ 网络欺诈风险
数据及服务层	✓ 数据泄露风险
平台及管理层	✓ 平台被入侵风险
网络及感知层	✓ 网络被攻击风险 ✓ 网络失效或不可用风险 ✓ 终端设备被盗用风险 ✓ 设备被入侵/攻击风险 ✓ 设备被仿冒/干扰风险

数据来源：赛迪顾问整理，2022.06

数字城市网络安全保障体系

- 保障目标
- 保障对象
- 数字城市网络安全整体架构

二 数字城市网络安全保障体系

（一）保障目标

数字城市网络安全保障的目标就是要保证城市在数字化转型过程中各类数字基础设施和重要业务系统的正常运行，确保智慧城市重要数字资源的保密性、完整性、可用性、真实性、可控性、不可抵赖性，使个人信息得到保护，满足国家对新型智慧城市网络安全保障工作的要求。

（二）保障对象

数字城市网络安全保障对象包括城市数字化转型过程中的数字基础设施、重要业务系统以及重要数据资源。

智慧城市的数字基础设施主要包括承担公共通信、广播电视传输的物联网、电信网、互联网、广播电视网、卫星通信网等信息网络。重要业务系统包括关系国家安全、城市安全、经济命脉、社会稳定的信息系统。对智慧城市数字基础设施和重要业务系统的保障主要是让其具有更强的感知能力、更高的通信处理能力和更快的响应速度，使智慧城市的网络运行更加安全和高效。

智慧城市的重要数据资源是关系到国家安全、城市安全、经济命脉、社会稳定的数据与信息，包括涉密数据与信息、敏感数据与信息，是可衡量价值的数据。智慧城市重要数据资源是智慧城市网络安全保障的重要对象，只有保护好这些重要的数据资源，智慧城市才能在保障和改善民生服务、创新社会管理方面发挥出更大的作用。

（三）数字城市网络安全整体架构

数字城市网络安全整体架构以安全保障为视角，从数字城市网络安全战略保障、数字城市网络安全管理机制保障、数字城市网络安全技术保障和数字城市网络安全运营保障四个方面给出数字城市网络安全要素。

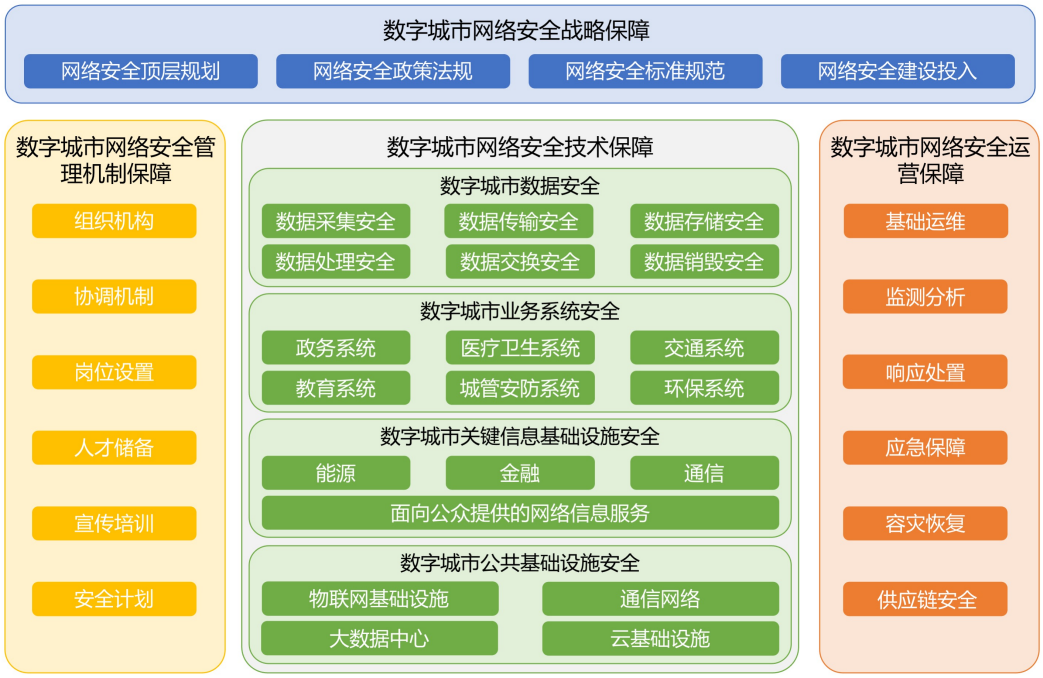
1、数字城市网络安全战略保障包括网络安全顶层规划、政策法规和标准规范等方面，通过该项保障来指导和约束城市数字化转型过程中安全管理与建设运营等活动。

2、数字城市网络安全管理机制保障是数字城市协调管理、协同运作、信息融合的关键，包括组织机构设立、人才储备和宣传培训等。

3、数字城市网络安全技术保障从城市公共基础设施安全、关键信息基础设施安全、业务系统安全、数据安全四个层次出发，通过部署多样的网络安全产品，来应对城市数字化转型过程中出现的各类安全风险。

4、数字城市网络安全运营保障是指对城市基础设施、信息资产和业务系统的监测、预警与维护。确保在城市数字化转型过程中基础设施、业务系统等状态发生变化时，可以采取一系列的预警、响应和恢复活动来保障智慧城市的平稳运行。

图 2　数字城市网络安全保障体系



数据来源：赛迪顾问，2022.06

数字城市网络安全评价指标

- 数字城市网络安全评价指标设计原则
- 数字城市网络安全评价指标体系

三 数字城市网络安全评价指标

（一）数字城市网络安全评价指标设计原则

数字城市网络安全评价可验证数字城市网络安全保障的有效性并促进网络安全建设，适用于智慧城市规划、设计、建设、运营管理等各个阶段。数字城市网络安全评价过程是：基于评价目标设计指标体系，从指标中提取具体的评价对象，通过测量模型和测量方法得出测量结果，经过对测量结果的研判，计算得出评价结果。

在设计数字城市网络安全评价指标体系时，我们遵循的设计原则为：

1、科学性：评价指标选取应能够体现数字城市网络安全的主要内容，反映数字城市发展面临的主要安全风险。

2、导向性：评价指标选取应考虑数字城市建设的循序渐进，应包含体现数字城市发展安全愿景的指标，引导其安全发展。

3、代表性：评价指标选取应能较全面反映城市网络安全建设的总体水平。

4、可采集性：评价指标应具有广泛适用的数据获取来源，并便于采集。

5、可考核性：评价指标应明确每个指标的含义与适用范围。

（二）数字城市网络安全评价指标体系

为探索数字城市网络安全建设特色，总结典型城市在数字化、智能化转型升级过程中的网络安全建设先进经验，赛迪顾问通过对全国多个城市进行深入调研以及数据采集，围绕数字城市网络安全管理保

障、数字城市网络安全技术保障、数字城市网络安全运营保障 3 大方面形成数字城市网络安全评价指标体系，包含 11 个二级指标，48 个三级指标，涵盖数字城市网络安全顶层设计、管理机制、公共基础设施安全、关键信息基础设施安全、业务系统安全、监测预警与应急保障等多方面的内容，以便全方位评价城市在数字化转型过程中的网络安全建设水平。

数字城市网络安全管理保障包括数字城市网络安全战略和数字城市网络安全管理机制两方面。数字城市网络安全战略指由地方制定的网络安全中长期发展规划及政策法规等文件的通称，主要评价数字城市网络安全顶层规划、法规及标准的制定、宣贯和落实情况等；网络安全投入指标是指为了完成城市数字化转型中的网络安全保障，政府财政决算（或预算）中以及相关企业等建设方自筹资金用于网络安全建设方面的资金使用情况。数字城市网络安全管理机制是指为了完成数字城市网络安全保障，建立科学完善的网络安全机构以及组织协调机制，促进多部门联动配合以及重大网络安全事件的责任追究，明确各方安全责任，此外，还包括网络安全人才培养、培训宣传以及网络安全计划的建立。

数字城市网络安全技术保障包括城市公共基础设施安全、关键信息基础设施安全、城市运行关键业务系统安全三方面。城市公共基础设施安全是指支撑城市民生服务、城市治理和产业融合发展最关键的数字化基础设施，重点考察物联网基础设施安全部署、大数据中心安全、政务云安全以及城市大数据平台安全等方面。关键信息基础设施

安全是指对涉及的金融、能源、电信等重要领域的关键信息基础设施开展备案以及安全防护等，此外，还包括数字城市通信网络安全的建设情况。城市运行关键业务系统安全是指保障城市政务、医疗卫生、交通、教育、城管、安防、环保等重要领域业务系统的安全运行。

数字城市网络安全运营保障包括数字城市安全服务支撑能力、数字城市安全监测分析能力、数字城市安全响应处置能力、数字城市安全应急保障能力、数字城市容灾恢复能力、数字城市供应链安全管理能力六方面。数字城市安全服务支撑能力主要从服务机构数量和从业人员数量等方面评价城市整体的网络安全服务支撑能力。数字城市安全监测分析和响应处置能力主要评价城市网络安全运行过程中的隐患发现能力和综合预警、处置能力。数字城市安全应急保障能力主要评价城市对网络安全事件的应急响应能力和对安全事件的追踪溯源能力。数字城市容灾恢复能力主要评价城市对灾难的恢复处置能力。数字城市供应链安全管理能力主要评价城市对供应链安全的评估和管理机制。

表 3　数字城市网络安全评价指标

一级指标	二级指标	三级指标
数字城市网络安全管理保障	数字城市网络安全战略	网络安全战略规划
		网络安全标准规范
		网络安全投入指标
	数字城市网络安全管理机制	网络安全机构及岗位设置
		网络安全组织协调机制
		网络安全人才培养及安全意识教育机制
		网络安全计划建立
数字城市网络安全技术保障	城市公共基础设施安全	物联网基础设施安全部署
		大数据中心安全、政务云安全（含 IDC 和平台）
		通信网络（电子政务网）安全
		云上系统的等保备案率

一级指标	二级指标	三级指标
		城市大数据平台安全
	关键信息基础设施安全	关键信息基础设施备案
		关键信息基础设施安全防护情况
		数字城市通信网络安全
		数字城市数据安全保障
	城市运行关键业务系统安全	政务系统安全指标
		医疗卫生系统安全指标
		交通系统安全指标
		教育系统安全指标
		城市管理系统安全指标
		城市安防系统安全指标
		环保系统安全指标
数字城市网络安全运营保障	数字城市安全服务支撑能力	网络安全服务机构数量
		网络安全从业人员数量
		安全运营实施规范标准化
		安全运营基础能力库建设（包括资产、漏洞、情报、案例库等）
		数字城市安全开发能力
		数字城市基础运维能力（安全设备基础运维机制）
	数字城市安全监测分析能力	网络安全监测范围
		网络安全监测机制
		网络安全监测能力
		风险评估能力
		威胁研判能力
		情报生产与消费能力
	数字城市安全响应处置能力	威胁处置能力
		网络安全风险预警机制
		网络安全发现通报效率
	数字城市安全应急保障能力	安全应急响应机制
		安全应急演练机制
		安全事件应急处置
		安全事件溯源能力
		安全反制能力
	数字城市容灾恢复能力	容灾机制建设（容灾机制、恢复流程）
		关键业务及数据灾难恢复
		其他业务及数据的灾难恢复能力
	数字城市供应链安全管理能力	供应链安全评估机制
		供应链安全评估管理

数据来源：赛迪顾问，2022.06

与去年的评价指标相比，本次指标体系主要有以下两点变化：

1、将城市公共基础设施安全中的大数据中心安全与政务云安全合并，并将云平台安全保障能力明确为云上系统的等保备案率。此外，将数字城市业务系统安全变更为城市运行关键业务系统安全，并在评价指标中提升了政务系统安全的重要性。

2、整体强化了数字城市网络安全运营保障指标的重要性，在二级指标中将监测预警能力、应急保障能力细化为监测分析能力、响应处置能力、应急保障能力、容灾恢复能力和供应链安全管理能力。此外，将服务支撑能力由两条细化为六条，不再简单的关注网络安全机构与人员的数量，而是对实施规范标准化程度、基础能力库建设、安全开发能力与基础运维能力进行了强调。

数字城市网络安全评价结果分析

- 总体评价结果分析
- 数字城市网络安全管理指数
- 数字城市网络安全技术指数
- 数字城市网络安全运营指数

四 数字城市网络安全评价结果分析

（一）总体评价结果分析

赛迪顾问针对上述指标体系设计了详尽的调研问卷，收集到近百份城市的有效问卷，通过调研结果分析与专家打分，结合数字城市网络安全评价指标体系对城市进行科学评估，最后得出 2022 年数字城市网络安全指数榜单 TOP30。

表 4　2022 年数字城市网络安全指数榜单 TOP30

排名	城市	分数
1	北京	88.5
2	上海	87.9
3	杭州	86.8
4	深圳	82.2
5	成都	80.3
6	广州	79.9
7	天津	78.7
8	南京	78.2
9	武汉	76.3
10	西安	75.1
11	重庆	74.2
12	青岛	73.6
13	郑州	73.5
14	长沙	73.0
15	贵阳	72.4
16	厦门	71.7
17	无锡	71.6
18	合肥	71.0
19	昆明	70.7
20	苏州	70.4
21	沈阳	70.1
22	福州	69.9

排名	城市	分数
23	济南	69.7
24	宁波	69.7
25	东莞	69.1
26	兰州	68.8
27	湖州	68.0
28	金华	67.6
29	珠海	67.3
30	徐州	67.1

数据来源：赛迪顾问，2022.06

从整体评价结果看，北京、上海、杭州、深圳综合实力较强，入选第一梯队，成都、广州、天津、南京、武汉、西安、重庆、青岛、郑州、长沙这些城市对网络安全的重视程度较高，入选第二梯队。贵阳、厦门、无锡、合肥、昆明、苏州、沈阳、福州、济南、宁波、东莞、兰州这些城市近些年在网络安全建设方面逐步发力，成效显著，入选第三梯队。

（二）数字城市网络安全管理指数

从数字城市网络安全管理保障方面来看，北京、上海、杭州、深圳等城市的网络安全管理体系较为完善，网络安全投入也相对较多。

表 5　2022 年数字城市网络安全管理指数榜单 TOP30

排名	城市	分数
1	北京	93.1
2	上海	92.3
3	杭州	88.3
4	深圳	86.0
5	广州	84.5
6	南京	84.5
7	天津	83.8
8	武汉	80.3

排名	城市	分数
9	成都	78.8
10	西安	78.3
11	郑州	76.6
12	青岛	75.8
13	重庆	75.3
14	贵阳	75.3
15	沈阳	75.1
16	长沙	73.8
17	合肥	73.8
18	福州	73.8
19	宁波	73.4
20	无锡	73.1
21	东莞	72.8
22	厦门	72.5
23	长春	72.3
24	苏州	72.1
25	珠海	71.8
26	兰州	71.8
27	济南	71.6
28	大连	70.8
29	昆明	70.5
30	徐州	70.5

数据来源：赛迪顾问，2022.06

从详细调研结果来看，国内绝大多数城市已经制定了本地区网络安全建设的总体规划、实施方案、标准规范等政策文件，但其中有近50%的城市制定的政策规范数量在5个以内。从制定政策的进程来看，国内城市网络安全政策制定还集中在顶层设计阶段，缺乏后续更为落地的实施方案和行业指引。

在网络安全建设投入方面，有40%以上城市网络安全占信息化投

入的比例在 6-10%，相较于 2020 年，投入占比有所提升。可以看出，城市对网络安全建设重要性的认知在逐步提升。

从城市网络安全机构设置上来看，94%以上的城市已经设立了网络安全领导小组，并且制定了年度网络安全工作计划，但是大部分城市的网络安全相关部门没有明确内部职责分工，也没有制定专项的管理及考核制度。

从城市举办的网络安全培训及安全意识教育频次来看，有近一半以上城市举办网络安全培训和安全意识教育的次数相对较少，仅在 5 次以内。可以看出，我国城市在网络安全意识教育方面还较为欠缺。

（三）数字城市网络安全技术指数

从数字城市网络安全技术保障方面来看，上海、北京、杭州、深圳的排名较为靠前，城市整体网络安全防护能力相对较强。

表 6　2022 年数字城市网络安全技术指数榜单 TOP30

排名	城市	分数
1	上海	88.7
2	北京	86.3
3	杭州	84.3
4	深圳	79.2
5	成都	77.8
6	天津	77.3
7	广州	76.4
8	南京	76.1
9	重庆	74.2
10	武汉	73.9
11	青岛	73.2
12	长沙	72.7
13	贵阳	72.6

排名	城市	分数
14	昆明	72.6
15	无锡	72.5
16	郑州	72.4
17	厦门	72.1
18	西安	72.0
19	苏州	71.4
20	济南	71.2
21	合肥	70.6
22	福州	70.3
23	宁波	70.3
24	东莞	68.4
25	兰州	67.5
26	湖州	66.9
27	徐州	66.5
28	沈阳	66.2
29	金华	65.2
30	珠海	64.6

数据来源：赛迪顾问，2022.06

从城市政务云安全建设来看，有80%以上城市的政务云平台已经通过了网络安全等级保护三级测评，也有将近56%的城市建立了完善的上云流程与云上安全责任机制划分。

从城市大数据平台的安全建设现状来看，有超过六成的城市建立了数据收集和获取操作规程，规范了数据收集和获取渠道，采取了必要的技术手段保证数据收集和获取过程中个人信息和重要数据不被泄露。也有三成左右的城市对数据收集和获取过程进行了记录和溯源，建立了数据脱敏规范。

在业务承载能力方面，能够承载常住人口万分之五并发访问的城市占比最多，达到34%以上。可以看出，当前城市的业务承载能力还

相对较弱。

在城市关键信息基础设施安全建设方面，九成以上的城市都没有建立完善的关键信息基础设施清单，可以看出，城市关键信息基础设施的认定工作还没有正式开展。

从城市数据安全治理方面来看，大部分城市都已经开展了政务数据分级分类工作，但在数据安全全流程管理方面还较为薄弱。

（四）数字城市网络安全运营指数

从数字城市网络安全运营保障方面来看，杭州、北京、上海、成都在智慧城市安全咨询、安全防御、安全告警、安全处置、安全应急服务等方面的经验较为丰富，能有效解决城市安全运营的各种问题。

表 7　2022 年数字城市网络安全运营指数榜单 TOP30

排名	城市	分数
1	杭州	87.6
2	北京	86.8
3	上海	84.1
4	成都	83.4
5	深圳	81.7
6	广州	79.2
7	天津	76.0
8	武汉	75.2
9	西安	75.1
10	南京	75.1
11	重庆	73.4
12	长沙	72.6
13	青岛	72.3
14	郑州	71.9
15	厦门	70.9
16	贵阳	70.0

排名	城市	分数
17	无锡	69.9
18	昆明	69.5
19	合肥	69.2
20	沈阳	69.2
21	金华	68.6
22	苏州	68.4
23	兰州	67.6
24	湖州	67.6
25	济南	67.2
26	东莞	67.0
27	福州	66.8
28	南昌	66.7
29	宁波	66.5
30	珠海	66.0

数据来源：赛迪顾问，2022.06

从单位网络安全相关从业人数来看，有近七成城市相关单位的网络安全从业人员在 10 人以下，网络安全从业人数相对较少。

在网络安全运营标准规范方面，有 34%的城市相关单位仅安排了信息化部门的日常网络安全运营工作，没有制定自身的考核机制以及与其他部门的协同机制。

在安全开发方面，有 60%以上的城市相关单位能做到在产品规划时考虑安全需求，组织开展安全需求评审和安全设计，并在上线前开展对安全需求的验证工作，但却没有考虑到安全开发流程和安全编码规范方面的问题，也没有通过威胁建模识别开发过程中的安全风险。

在数字化安全运维方面，有五成以上的城市相关单位能够定期组织开展安全巡检，保证安全设备的可用性，并定期对重要信息资产安装补丁文件。但是对重要信息资产并没有定期进行安全脆弱性的核查、

安全加固、安全风险评估与处置。

在数字化信息资产管理方面，有50%左右的城市相关单位采取人工的方式维护信息资产清单，定期通过工具识别和管控互联网侧未知资产带来的安全风险。有30%的城市相关单位可以借助信息化技术平台管理全量信息资产。只有不到20%的城市相关单位可以通过流量分析或主动探测等技术自动化发现新增资产或未知资产，实时监测发现和自动预警资产变动带来的安全风险。

在IT供应链安全管理方面，有近六成的城市相关单位在与IT供应链商及其上游供应链建立关系的同时，可以充分识别和评估供应链安全问题，重点审查许可风险、生态安全和信息安全问题。仅有15%的城市相关单位能充分识别IT供应链成分构成，定期开展供应链安全演练，建立IT供应链安全风险常态化监测机制和快速响应机制。

在数字化安全风险监测方面，有26%左右的城市相关单位可以做到实时监测终端设备上病毒爆发的状态，实时监测来自垃圾邮件和恶意邮件的攻击行为，感知安全边界网络攻击的实时状态。有36%以上的城市相关单位可以实时监测网络层及应用层的攻击行为以及数据泄露、数据篡改、数据窃取等安全事件，并能组织开展研判分析和有效处置。还有15%左右的城市相关单位只能做到监测终端设备上病毒爆发的状态，感知不符合安全要求的终端分布以及外部网络攻击行为的实时状态。

在数字化安全预警与处置方面，有40%以上的城市相关单位可以通过第三方通报、基线比对、安全情报、流量分析、漏洞扫描等技术

手段感知和预测安全风险，评估、分析其对全网信息资产的影响面，并借助技术平台进行通报预警和信息流转。有 14%左右的城市相关单位还自建了威胁情报库或订阅第三方情报，结合行业特性自动化关联资产指纹实现精准预警，准确定位受影响的信息资产。

在数字化安全应急保障及容灾恢复方面，有 20%左右的城市相关单位制定了容灾恢复机制，在发生安全事件后，主要依赖于外部资源开展应急响应。有 30%左右的城市相关单位已经制定容灾恢复机制、常见场景安全应急预案，在发生安全事件后，能够按照预案在外部资源协助下开展有效的抑制、加固、消除等措施。也有 20%左右的城市相关单位在发生安全事件后，能独立开展安全事件应急处置、攻击溯源、事件取证等工作。

从上述数字城市网络安全运营的调研结果来看，中国城市在数字化信息资产管理、风险监测、安全预警与处置、应急保障及容灾恢复方面的运营工作开展较好，成熟度较高。而在安全开发、安全运维能力、IT 供应链安全管理等方面还处于较为初级的阶段。

数字城市网络安全建设典型案例

- 上海市
- 金华市
- 湖州市
- 长春市
- 宜兴市
- 宜昌市

五 数字城市网络安全建设典型案例

（一）上海市

1、项目背景

为推动城市治理数字化转型，推进超大城市治理体系和治理能力现代化，上海市委、市政府利用科技手段赋能，推进城市运行“一网统管”，搭建统一平台，促进政府流程再造和体制机制的完善，增强市民的获得感、幸福感和安全感。作为“一网统管”的具象实体，上海市城运中心充分发挥数据赋能、信息调度、趋势研判、综合指挥、应急处置等作用，重点做好拟订城市运行管理智能化管理战略、编制智能化发展规划和专项规划、城市运行状态监测分析和预警预判以及应急事件联动处置等工作。

面对“一网统管”这个复杂巨系统，安全保障非常重要，如何提供创新安全保障平台，如何形成常态化技术保障支撑，探索营造以需求为导向、合规为牵引的城市治理数字安全生态共同体，成为夯实“一网统管”数字安全底座重要研究课题。

2、建设内容

2021 年，上海市政府城运大厅相关大屏定制工作重点推进了“一中心、两平台、两课题”，具体为“一网统管”安全服务中心、数据安全保障平台、市域物联网安全运营平台、安全底座课题、多云管理课题。其中，“一网统管”数据安全保障平台作为适用于城运信息系统数据安全的一站式解决方案，为数据及应用提供一体化的安全保障能力。围绕一网统管业务场景，该平台依托“风险核查-数据梳理-数据

保护-监控预警”模型，建立立体安全防护体系，提供数据流动视角下的安全管控能力，对数据流动场景下的关键节点进行安全监测和防护，并对数据安全风险进行及时预警和通报，形成“多维联动、立体防护”的数据安全管控体系。

针对“一网统管”的安全数据采集、治理、存储、接口服务等安全数据服务支撑，利用相关数据进行建模分析同时提供预警、感知、协调指挥等业务应用支撑能力，探索满足超大城市城市级信息系统开展数据安全管理工作的实际业务需要，为安全服务团队及对接系统安全管理单位提供技术支撑能力。

3、项目成效

从技术上来说，本项目有效保障了“一网统管”的数据安全。通过分析和主动检测相结合的方式对数据安全威胁建模进行实时深度检测、智能分析，为数据安全事件分析和追踪溯源提供支撑。同时支持原有安全基础能力对接能力，对“一网统管”安全基础能力结合等级保护的要求进行补充与完善，遵循等级保护相关要求进行加固，实现数据层面风险发现、威胁分析和关联监测等安全能力。

从业务上来说，本项目实现了安全与业务的深度融合。“一网统管”以数据安全保障平台为基础工具，建立覆盖数据基于业务流转的安全管控措施，实时监控“一网统管”数据调用和数据赋能的安全风险，通过技术手段确保数据来源合法、流向合规、使用正当。助力“一网统管”打通各部门数据壁垒，完善数据归集，优化数据应用，为疫情防控、经济发展、城市治理和民生服务构筑“安全锁”。

从管理上来说，本项目建立了“一网统管”安全服务中心。以“一网统管”数据安全保障平台为依托，探索安全运营服务体系，以安全运营服务、产品、团队、平台相结合的方式为城运云安全运营管理工作提供支撑。

（二）金华市

1、项目背景

随着浙江省数字化改革深入推进，数字化应用不断上线，数据共享力度持续加大，金华市电子政务网面对网络安全攻击手段多样、隐蔽持续且日益严重等网络安全威胁。如何进一步强化金华市电子政务网市县分域监管、部门主体条线体制管理、各技术平台数据整合、防范公共数据泄露风险，切实做好“1612”数字化改革体系中的网络安全保障，对金华市大数据局现有的安全监测体系和安全管理模式都提出了更新、更高的要求。

2、建设内容

通过打通浙政钉用户组织体系，厘清部门安全边界，落实首席安全官职责，完善安全情报共享，安全事件快速联动，金华市大数据局通过制定《金华市一体化全链路网络安全工作规范》，规范金华市域一体化全链路网络安全监测管理的制度体系。

聚焦金华市域“云、网、端、应用、数据”的安全保障，结合安全技术保障体系，实现“云、网、端、应用、数据”五个方面能力的优化集成建设，从场景出发精准掌握风险，实现全方位监测、全要素防护、全流程管理，确保金华市电子政务网络安全环境良性闭环的工

作管理体系。

通过统筹全市技术监测能力建设，开展常态化网络安全运营，实现安全工作业务化、安全管理常态化、安全处置精准化。强化全市电子政务网络安全问题发现、通报、整改的及时性、有效性，进一步压实部门及首席安全官的主体管理责任，立足“多跨协同、数据共享共用、联动处置”，推动市、县各部门安全风险协同处置。同时，又建立“监测、响应、预测、防御”动态自动化闭环流程，将网络空间、地理空间与网安业务有机结合，实现监管有温度，处置有效率。大力推进与市网信、市公安、各部门、信息安全企业、科研院所、专家团队之间的协同联动和情报共享，实现平台的数据贯通和业务协同。发挥大数据局的监督运营作用，充分利用和调动重要行业部门、重点单位和社会技术力量，与多个部门密切配合，大力提升网络空间安全保卫能力，构建全市共建、共享、共管的一体化全链路网络安全监管工作体系。

3、项目成效

通过监测要素全链闭环全方位覆盖、安全防护全链闭环大数据分析、安全管理全链闭环全流程处理创新机制，强化日常应急响应和通报预警工作，不断完善网络安全漏洞和应急处置的全链条闭环管理，金华市一体化全链路网络安全监管平台初步成效。**一是自动化资产梳理，**采用自动化监测手段，围绕“云、网、数、用、端”开展资产全面普查，基于风险漏洞管理技术手段，梳理金华市域资产 87609 个，其中重点保护资产数量 305 个。**二是智能化安全分析，**进一步汇集全

域安全大数据，将每天系统所产生海量安全事件及告警信息通过层层分析和智能研判后，最终将精准的告警数据进行推送给安全工作人员，为决策、重要时期的网络安全保障工作提供有效支撑，面对网络安全事件、威胁，能够快速组织、高效处置。**三是一体化安全防护，**以“上云是常态，不上云是例外”为原则，采用集约化建设，开展全市业务系统的全方位全天候保护、统一集中安全防护，有效落实全市各部门网络安全主体责任，降低各部门安全产品和服务采购成本。已防护金华市域 1833 个系统，今年共防护 37376 次安全攻击。**四是常态化安全运营，**整合现有碎片化的问题发现机制和预警处置流程，以全链路网络安全监管平台为抓手，实现重大风险隐患实时推送至业务部门安全负责人，重大风险隐患 1 小时内定向通知到指定责任人。经浙政钉通报网络安全警告近 100 余次，协助 40 余个单位处理网站及信息系统的安全问题，安全隐患整改率达到 95%以上。有效提升了金华市域政务网整体安全防护能力，为金华市数字化改革筑牢网络安全底座。

（三）湖州市

1、项目背景

湖州市为了深入贯彻落实浙江省数字化改革中网络安全保障体系的要求，坚持“以安全保发展、以发展促安全”的理念，按照“市域一体化安全保障、安全风险多跨联动协同处置、安全支撑能力集约赋能”的建设思路，以湖州市域网络安全保障工作总体方案为指导、以安全运营中心为支撑、以安全运营中心为抓手，聚力机制创新、制度创新、技术创新、模式创新，打造湖州市域一体化安全保障体系。

2、建设内容

立足“市域一体”，强化理论支撑、构筑顶层设计。针对湖州市数字化改革面临的安全规范不健全、安全责任不清晰、安全能力碎片化等问题。**一是湖州市大数据发展管理局牵头编制“总体工作方案”。**湖州市大数据发展管理局联合浙江省内优秀安全企业，对湖州市域范围内网络与数据安全工作进行深度调研，并编制了《湖州市域一体化网络安全保障工作方案》，工作方案明确了网络安全总体建设目标，提出“云、网、边、数、用、端”全链路安全建设要求，指导各单位落实网络安全防护工作。**二是谋划市域安全运营顶层架构，明确市域一体化安全运营中心定位，**即市域一体化安全运营中心是联动市、区县网络安全工作的总枢纽、是市域各单位获取安全能力的总资源池、是市域一体化安全运营的总工作站。

立足“集约赋能”推动安全能力集约化建设、集中赋能、一城通惠。**一是统筹安全服务能力。**让安全能力集约化、服务化、SaaS 化，形成本地化安全资源与服务目录。对全市单位进行开放，各单位可以自主化、定制化使用安全资源能力。**二是统筹安全服务团队。**整合市场上优秀的安全产品与优秀厂商的安全服务，将不同服务商提供的碎片化的安全服务整合成“政府主导、联合运营”的一体化安全运营服务机制。各厂商安全服务成员统一纳入安全运营中心统一服务团队，将生态服务商整合成一个有机整体，达到持续优化、动态运营的效果。**三是统一安全运营服务机制，建立安全运营服务规范与标准化流程。**各服务商团队采用同一个标准参与、同一个标准考核、同一套流程开

展服务。

立足“多跨协同、联动处置”推动市、县区、委办单位安全风险协同处置。针对目前湖州市安全风险管理流程未闭环困难，市、县区单位风险处置工作协同能力不足等问题。**一是筹建市域一体化安全运营中心，**场地规模 250 平米，驻点专家 10 名。依托市域一体化实体安全运营中心提供湖州全域电子政务系统资产测绘评估、安全巡检加固、安全监测预警、安全事件处置等服务，让安全渗透到应用建设每一个环节。**二是安全风险及问题统一监测与闭环处置。**对现有碎片化的问题发现机制进行整合，利用安全运营平台进行统筹，实现问题同一平台汇总、同一个平台分析、同一个平台处置。**三是强化数据安全监管，**通过安全运营中心，构建市域公共数据“敏感分布地图”。完成三个业务场景的数据梳理，基于业务规则建立监管策略模型，确保数据共享与访问“脉络清晰，流向合规”。

3、项目成效

通过编制《湖州市安全运营中心工作管理规范》，构建湖州市、区县一体化的安全管理组织架构，明确市、区县大数据局及单位和各服务方安全管理职责，形成各级网络安全专职管理机构的工作重点，实现对全市安全风险的有效管理和监督。

湖州市域一体化安全运营中心从技术、管理和运营多方面指导湖州各类重要行政及公共服务系统的安全建设，为公共服务及各单位提供安全工作的指导与赋能，为全市数字化改革护航。目前已经整合安全软硬件资产 18 类、形成 SaaS 化、软件化安全服务能力 24 项。市

域范围内各单位根据安全等级要求通过安全运营中心部署相适应的安全防护产品，IRS 上业务系统备案率达到 70%以上。针对湖州市政务网、政务云平台及云上约 70 多家单位的业务系统、数字大脑上重要业务系统等进行了整体的技术评估，发现存在安全漏洞终端 155 个、服务器 178 个。通过浙政钉在线通报下发网络安全警告 50 余次，协助全市及三县两区 40 余个单位处理网站及信息系统的安全问题。通过自动化手段安全研判与通报预警专项人员由原来的五人减少至 3 人，预警处置效率从原来要 1 周缩短到 3 天就能完成整个处置闭环。

（四）无锡市

1、项目背景

随着无锡市新型智慧城市建设推进，基于数据共享和流程变革的智慧城市管理服务不断投入运营，极大地提升了社会管理服务运行效率，但数据在整合共享过程中也面临众多安全问题。主要体现在一是数据从四面八方汇总在一起，其中不乏大量敏感数据，集中的数据更容易成为攻击的目标；二是缺乏对内部人员业务访问权限的精细化管控，难免出现违规查询、导出，甚至是修改数据行为，给数据泄露造成极大隐患；三是政务数据在各政府部门之间流动、共享和交换，数据存在于数据域、业务域、交换域、终端域，数据交换各环节如果不协调一致，极易造成数据泄露。

目前，无锡市城市大数据中心已汇聚了全市各部门超过 120 亿条数据，为 37 个部门提供数据共享交换服务，加强城市大数据中心数据安全管理是刻不容缓的任务。目前这些数据均存储在政务云环境中，

而政务云计算环境内对于数据安全的防护技术手段有所缺失，缺乏合理的安全域划分，相关服务器和设备混杂在同一个安全域中，无法对数据进行分区分域安全防护，缺少数据存储加解密技术手段，缺少数据脱敏技术手段。

2、建设内容

根据无锡市城市大数据中心安全防护需求，全面梳理城市大数据中心实际数据处理业务场景、传输网络环境、数据处理和存储环境等情况，依据“等级保护 2.0”、数据安全成熟度模型、政务信息共享数据安全技术要求等国家行业标准规范和相关政策法规要求，提升城市大数据中心安全防控能力，最终建立无锡市城市大数据中心安全体系，具体如下：

1）数据安全管理组织建设：建立数据安全管理的组织架构、职责分配和沟通协作机制；

2）数据安全标准规范建设：制定数据安全管理的技术标准和规范，建立数据安全管理制度；

3）数据安全管理平台建设：建设覆盖数据安全管理全链条的数据安全管理平台，根据数据安全管理制度流程，全面归集数据安全管理各环节信息，对数据安全操作进行有效管控，对安全信息进行感知、研判、预警、展示和处置；

4）数据安全技术体系建设：规划调整城市大数据中心所有安全域，建设与制度流程相配套并保证有效执行的采用数据加解密系统、终端防泄露、存储防泄露、数据安全堡垒中心、数据库审计等多种技

术和工具，实现对数据安全各环节的有效管控，全面建立城市大数据中心安全技术体系；

5）数据安全运营体系建设：建立专业的数据安全运营队伍，对数据安全进行管控、评估和咨询，确保城市大数据中心安全体系可靠运行。

3、项目成效

数据安全管理组织方面：组织可分为决策层、管理层和执行层等三层结构。其中，决策层由参与业务发展决策的局领导、业务处室负责人组成，制定数据安全的目标和愿景，在业务发展和数据安全之间做出良好的平衡；管理层是数据业务处室及运维团队管理层组成，负责制定数据安全策略和规划以及具体的管理规范；执行层由数据安全相关运营、技术和各业务部门接口人组成，负责保证数据安全工作推进落地。

数据安全标准规范方面：建设数据安全管理的相关标准规范和管理制度，包括数据安全方针和总纲、数据安全管理规范、数据安全操作指南和作业指导，并监督流程的执行过程，满足了市大数据管理局对数据安全管理业务的需求。

数据安全管理平台方面：建设覆盖数据安全管理全链条的数据安全管理平台，根据数据安全管理制度流程，全面归集数据安全管理各环节信息，对数据安全操作进行有效管控，对安全信息进行感知、研判、预警、展示和处置，把数据安全的管理工作落实到整体技术体系，衔接数据安全运营体系，作为数据安全管理工作的基础支撑平台。

数据安全技术体系方面：规划调整城市大数据中心所有安全域，建设与制度流程相配套并保证有效执行的采用数据加解密系统、终端防泄露、存储防泄露、数据安全堡垒中心、数据库审计等多种技术和工具，实现对数据安全各环节的有效管控，全面建立城市大数据中心安全技术体系。

数据安全运营体系方面：建立专业的数据安全运营队伍，对数据安全进行管控、评估和咨询，确保城市大数据中心安全体系可靠运行，包含人员能力建设和核心能力建设。

（五）长春市

1、项目背景

依托于“业务驱动的数据协同”和“数据推动的业务创新”双轮驱动理念，长春市的新型智慧城市建设将城市智能体作为基础设施、联接中枢和运行载体，实现了城市的智能化管理和运行。长春城市智能体在推动长春城市数字化、网络化、智能化发展的同时，也带来了诸多网络安全隐患和风险。因此亟需开展长春城市智能体安全保障体系规划工作，站在总体安全观的高度规划设计长春城市智能体的安全保障体系，以“安全、合规、可控”为实现目标，构建立体化纵深防御体系，确保长春城市智能体健康发展。

2、建设内容

全面推进落实“等级保护 2.0”标准，加强关键信息基础设施的安全防护工作，深入开展定级备案、测评整改工作，建立集约化安全资源服务平台，以安全能力资源化、安全资源服务化、安全服务目录

化的方式按需申请、按需分配、弹性扩容，并提供不同级别的安全防护能力，满足等保合规建设；提供 SaaS 化云安全防护和密码安全建设，提升智能体各类应用安全保障能力；完善态势感知和监测预警体系，推动各平台互联互通，形成覆盖面广、布局合理、联防联动的监测预警体系，丰富安全数据收集维度，深化信息共享机制建设，强化情报信息研判，落实信息通报机制，实现对长春市网络及数据安全的全方位全天候态势感知，并提高全生命周期安全监测预警能力；同时提供信息安全事件分析处理、智能应急响应、运营流程设计、安全专家决策辅助等服务支撑。

长春城市智能体按照统分结合的模式，构建了科学、高效的系统架构。对“云、网、数、智、安”等基础设施和基础能力进行统筹安全建设，为应用场景和各部门信息化平台建设提供安全赋能，同时保留应用场景的个性化空间，覆盖城市云和 7 大能力平台底座、4 个中枢系统及四个领域 6 大综合应用场景，加快推进政府数字化转型，促进长春数字经济蓬勃发展。

3、项目成效

以城市智能体数据资源管理为基础，以情报和安全业务流程为驱动，以风险管理为核心，以事件管理为主线，辅以有效的运营管理、监控与响应机制，提供专业化安全服务。建立覆盖城市智能体所有用户、平台、设备的常态化安全运营体系，形成由城市智能体安全运营总包方、第三方安全服务商、各委办安全运营团队共同组成联动协同的安全运营组织体系。安全运营基于标准的作业流程，通过技术、流

程、人有机结合完成安全运营，以可视化的形式实现数据之间的连接，完成综合分析，将信息安全服务做到自动化感知、智能分析、应急响应、辅助决策，提供一站式解决方案。安全运营建设具备多种场景适配，并可与态势感知、安全大数据分析系统、SaaS 服务系统、云安全防护系统等形成联动，通过构建纵深立体化网络安全防护体系，实现各业务场景的“可监、可管、可视、可控”安全目标，为长春智能体提供了一个指挥、分析、智能、协调的安全运营服务体系，确保安全无所不在，服务全程全时。

（六）宜兴市

1、项目背景

目前，宜兴市政府信息化基础设施已建设完成宜兴市政府信息化基础设施外网、宜兴市政务云计算平台、宜兴市政务网络安全云平台、宜兴市大数据平台。随着宜兴市部委办局逐步将业务系统迁移至政府信息化基础设施中，政务云信息资源不断丰富，越来越多的云内应用系统投入使用，开放、复杂的业务环境带来了新的安全隐患。为筑牢宜兴数字化的底座，宜兴市打造城市安全大脑运营中心，通过专家持续运营保障宜兴市政务云、政务网业务。

为动态适应数字政府基础设施环境的变化，充分考虑数字政府基础设施的实时风险，宜兴市政府对现有数字政府基础设施风险进行了一番深入调研，发现了风险项、安全差距、安全控制等薄弱环节。宜兴市政府信息化基础设施面临的安全风险以及降低风险可能造成的安全损失，迫切要求其建设持久化安全运营体系。

2、建设内容

本项目坚持贯彻“安全运营闭环管理并基于数据分析为核心”的安全运营理念，结合宜兴市信息化基础设施具体情况和实际需求进行设计，形成威胁预测、威胁防护、持续检测、响应处置的闭环安全运营体系。

本项目打造了安全运营中心，提供安全运营服务，形成了安全管理体系，并且应用了多个核心技术，帮助安全团队实现数据处理、分析、决策和相应的自动化运行，提高运营效率。在筑牢安全防御的基础上，提供的安全运营框架还可以为客户云端情报赋能，利用云端海量安全大数据，如威胁情报、APT 情报、漏洞库、攻防知识库等，与本地安全大脑运营平台实时共享，帮助内部精准研判威胁事件。

此外，本项目还建设了数据安全体系。围绕政务云计算平台、大数据平台，布署了数据库防火墙、数据库防水坝、数据库运行管理平台、业务安全监测系统和防勒索病毒系统，防护宜兴市信息化基础设施。日后，随着政务应用的不断增加以及数据量的不断增长，还将进一步完善设备硬件空间及授权，并增加敏感数据泄露防护能力，实现数据防护的事前敏感数据分级分类，事中细粒度权限控制，事后安全审计。

3、项目成效

首先，实现了安全事件溯源。宜兴某委办单位租用的政务云主机发生过勒索病毒事件，通过本地安全大脑运营平台+人工溯源分析，最终确定攻击路径，确认了包括开发商、系统维护商的安全责任。**其**

次，实现了委办单位业务系统上政务云的申请规范。在系统上线前要求提供漏洞检测报告、源代码审计报告，系统上线后要求定期开展渗透测试，确保上线前后的业务安全。**再次，实现了平台化管理不断增加的业务资产。**在 2021 年重保期间，利用平台对重点资产进行脆弱性分析，发现了某核心业务系统存在弱口令账号和信息泄露。并定时更新新增资产，确保不会有未知资产存在。**最后，实现了本地专业安全服务团队运营。**安全专家定期对核心业务开展安全检查服务，重保期间封禁多个恶意外部 IP。

（七）宜昌市

1、项目背景

宜昌市作为数字化建设的先行者，在数字政府、智慧城市等多方面接连作出显著成绩。“数字公路”“数字公交”“智能交通引导”等一系列数字化应用的落地，不断勾勒出“智慧宜昌”的新面容。然而，伴随着支撑这些数字化场景的 IT 系统越来越开放、复杂，网络风险暴露面也随之增长。“智慧宜昌”的建设与运行，离不开网络安全的全程护航。建设网络安全信息统筹机制，强化关键信息基础设施网络安全保护，提升网络安全态势感知和应急处置能力，才能不断发现宜昌市在数字化转型进程中的痛点与盲点。

作为网络安全监管的政府单位，宜昌市网信办需要对全市等保单位、重要信息基础设施以及辖区重点单位的资产开展安全检测，及时发现监管资产的安全风险。因此，对于宜昌市网信办来说，能够全面摸清全市互联网 IP 资产的具体信息，及时主动认清重要网络和信息

系统中的安全风险，梳理全市风险资产、高危资产、资产属性等风险，督促对应单位进行安全整改，是提升城市全网资产探测和风险管理能力的必然需求。

2、建设内容

本项目针对宜昌市网信办提出的安全建设需求，对当地安全运维、资产分布等状况进行了深入调研，提出了新的资产管理思路：将网络空间、地理空间和社会空间进行相互映射，将虚拟动态的网络空间测绘成一份动态、实时、可靠、有效的网络空间地图，为决策者提供有价值的战略情报信息，降低决策的不确定性，有效帮助宜昌市网信办全面掌握全市互联网资产暴露面分布情况，及时发现网络空间各类安全风险隐患，进一步促进城市各领域的网络安全问题整改。

（1）看见全局：凭借本项目中的空间测绘能力模块，实现对全市互联网资产的资产管理和风险测绘，精准识别资产 IP、开放端口、所用服务、搭载产品、使用域名等多种属性信息和关联信息。

（2）资产梳理：本项目中的数据挖掘探索能力模块，可以提供丰富的基础数据，并将其与各种安全和资产的伴生数据形成关联，有力支持全市网络安全整体水平提升。

（3）防控隐患：本项目中的漏洞感知能力模块，负责将资产与安全性进行直观连接，帮助快速发现、验证、解决资产出现的安全隐患，形成一流的漏洞应急响应闭环流程和机制，同时以攻击者视角分析和监控资产安全状态，发现资产安全漏洞，评估全市漏洞影响面。

此外，根据网络空间测绘 SaaS 服务提供的监测数据，安全专家

还将按照指定的内容和格式进行筛选、分析，汇总为互联网资产测绘分析报告，以便宜昌市网信办能够快速便捷的了解到各类资产数据中可能存在的安全隐患。

3、项目成效

在本项目的持续赋能下，宜昌市网信办挖掘出了“智慧宜昌”在数字化转型过程中的安全新思路。一是通过多维度、大范围、高精准的测绘技术，帮助宜昌市网信办全面掌握了全市 5 个市辖区、3 个县级市、3 个县、2 个自治县互联网中的资产和脆弱性分布情况，同时完成了对资产信息业务类型、端口、协议、产品、服务、自治域和运营商的统计分析。二是依托安全分析专家和安全服务团队的 7*24 小时协同，以及按季度输出的互联网资产测绘报告，构建了常态化的网络空间测绘服务，持续跟踪全市互联网资产脆弱性风险情况，实现了全市互联网资产可视、风险可视、运维可管理、漏洞及时修、通告及时发的崭新局面。

赛迪建议

- 加强数字城市的网络安全顶层设计规划
- 数字城市治理和应用要重视数据安全流转与个人信息保护
- 安全运营是数字城市网络安全建设中的重中之重
- 加快城市网络安全综合防控体系建设

六 赛迪建议

（一）加强数字城市的网络安全顶层设计规划

在将来的数字城市建设过程中，政府建设工程将由项目制转向长期运营制，将更加强调项目的持续性运营能力。因此，在具体建设中要更加注重数字城市的顶层设计，使建设思路、建设行动、后期运营整体一致。数字城市网络安全的建设也要根据区域比较优势、经济水平等因地制宜、因时制宜，整体部署网络安全策略，通过政策驱动以及产业规范的建立，将网络安全纳入智慧城市的顶层架构和设计当中。各城市要建立合理、有效的网络安全组织架构，设立安全决策、管理、执行及监管的机构与责任人。健全与新型智慧城市发展相适应的网络安全运营保障制度，加强日常监督与防护。此外，要强化公众网络安全教育，加快安全专业人才培养，加强网络安全防御意识。

（二）数字城市治理和应用要重视数据安全流转与个人信息保护

在智慧城市建设过程中，政府掌握着 80%左右可开发、可利用的数据，尤其能源、交通、金融、医疗、教育、旅游等领域的数据，是涉足面最广、数量最庞大、价值最高的数据资源。数据开放共享是大数据应用和深入挖掘数据价值的基础，也是推进新型智慧城市建设的重要抓手和核心内容。在数据开放共享过程中，大量的数据及个人隐私信息在网络中暴露，大大加剧了数据泄露及丢失、IP 和身份智慧城市建设保密管理被窃、金融欺诈等数据安全隐患，当其受到攻击，引发数据破坏与灾难时，或将对城市甚至国家的运行管理造成重大且难以恢复的打击。因此，各城市要制定建立健全关键信息基础设施安全

保护、数据安全管理和网络安全审查等网络安全管理制度，建立数据全生命周期的保障体系。在数据资源开放共享、安全保护、数据确权、个人信息保护和数据跨境流动等方面，完善基于数据开放共享的治理策略，加强政策、法律、管理制度、标准规范和技术体系的统筹协调。

（三）安全运营是数字城市网络安全建设中的重中之重

数字城市运行过程是持续性的、不断运转的，智慧城市的网络安全不能只靠建设而忽略运营。因此，数字城市在网络安全方面，在投入安全建设的同时也需要构建网络安全运营体系和运营组织，通过持续的安全运营才能保障数字城市发展的安全底线与持续性运行。为有效应对智慧城市面临的各类新型网络安全威胁与挑战，各城市应当融合安全合规、动态防御、主动防御、综合防控等安全保障体系建设理念，覆盖网络通信安全、物联网感知安全、云平台安全、智慧应用安全、工业互联网安全及城市数据安全等，构建一体化的智慧城市安全运营解决方案。此外，建设专业的安全运营人才团队，结合网络安全企业的专家分析服务，打造数字城市的网络安全运营服务体系，实现动态、主动、持续、闭环的安全运营模式。

（四）加快城市网络安全综合防控体系建设

当政务信息系统上云、数据共享与交换以及物联网等技术广泛应用后，政府单位和信息系统原本孤立的状态发生变化，政务、电力、交通、医疗等跨领域、跨平台的信息单系统被连接起来。但这种跨平台领域的信息整合，给城市的整体性安全防护带来了新的挑战。因此，建立城市网络安全综合防控体系，为数据信息共享提供整体性、体系

化的安全保障尤为重要。通过城市网络安全综合防控体系的建设对智慧城市中的感知层、平台层、数据层及应用层等做到体系化防护，保护物联网终端、网络、云平台、主机和应用等关键要素，形成安全的通信网络、区域边界和计算环境，通过威胁感知、异常检测、风险评估和态势分析等能力，最终为智慧城市中的智慧应用和数据提供纵深防护。