智慧城市安全态势感知体系的研究

Research on Security Situation Awareness System for Smart City

闫 琛,夏俊杰,高 枫,陈奇柏(中国联通智能城市研究院,北京 100048)
Yan Chen,Xia Junjie,Gao Feng,Chen Qibai(China Unicom Smart City Research Institute,Beijing 100048,China)

摘 要:
随着城市智能化建设的推进,海量泛终端接入,智能应用丰富,使得城市级网络安全态势复杂多变,全域网络安全风险管控困难。城市级安全态势感知体系的研究是以城市为单元体,从城市全局着眼建设贯通跨网、跨域的网络威胁、网络病毒、网络攻击的监测能力,旨在融合城市跨行业、跨领域、跨生态、多维的物理和数字城市场景下的全时、全域安全威胁分析和态势感知能力,从城市的整体提升网络威胁感知、监管分析、协同指挥能力、全域对抗网络空间攻击的能力,筑牢城市数字化发展的安全基石,保障智慧城市的高速发展。

关键词:
智慧城市;网络安全态势感知系统;网络安全信息;网络安全事件管理
doi:10.12045/j.issn.1007-3043.2022.05.005
文章编号:1007-3043(2022)05-0022-06
中图分类号:TN919
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
With the advancement of intelligent construction and the access of a large number of terminals, the urban network security situation has become more complex and the security risk control has become more difficult. The research of city level security situational awareness system is to build a network threat monitoring, analysis and disposal capability through cross network and cross domain with the city as the unit. It integrates the global security threat analysis and situational awareness capabilities of cross industry, cross field and cross ecology in the city. City network security situational awareness system improves the ability of network threat awareness, regulatory analysis, collaborative command and anti attack, builds the security cornerstone of urban digital development, and ensures the rapid development of smart city.

Keywords:
Smart city; Network security situation awareness system; Cyber security information; Cyber security incident management

引用格式:闫琛,夏俊杰,高枫,等. 智慧城市安全态势感知体系的研究[J]. 邮电设计技术,2022(5):22-27.

1 智慧城市的安全背景

1.1 网络空间安全形势严峻

网络安全威胁国家安全,事关政治安全、社会民生安全。从近年国际、国内发生的网络攻击事件和案例中可以看出,网络空间安全形势越来越严峻,攻击者主要针对政府、工业、医疗、服务提供商、关键基础设施和消费者进行攻击。2010年,伊朗核设施遭遇"震网"病毒攻击,打开了网络空间摧毁或瘫痪物理世界的大门;2017年,不法分子通过改造"永恒之蓝"制作wannacry勒索病毒,英国、俄罗斯乃至整个欧洲以及中国国内多个高校校内网、大型企业内网和政府机构专网中招,被勒索支付高额赎金才能解密恢复文件。2021年12月,Log4j日志框架中一个严重的远程代码执行漏洞震惊了整个行业。越来越多的网络攻击、数据泄露、网络空间遭威胁等安全事件的发生,让人们认识到网络和信息设施安全的重要性。严峻的网络空间安全形势给城市管理者们带来不小的震撼,城市

收稿日期:2022-04-01

是网络和信息设施的综合体，对城市网络空间的攻击将对现实城市造成严重的影响。

1.2 我国智慧城市安全现状

我国《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》提出，加快数字化发展，建设数字中国，为我国数字城市建设指明了方向。《超级智慧城市报告》显示，目前我国在建的智慧城市达到500多个。智慧城市复杂、开放、互联的特点，以及城市的数字化区别于传统信息系统的服务方式、网络架构、数据资源等技术因素，加之受制于智慧城市物理主体建设的连带效应，导致了国内智慧城市在网络与信息安全上凸显如下几类问题。

a）智慧城市内的系统多、部门多，城市建设“繁荣且混乱”，网络与信息安全被“冷落”。

b）智慧城市全局性网络与信息安全顶层设计规划未得到足够重视。

c）面向智慧城市的新技术的防护能力有待突破。新型智慧城市是5G、云、大、物、智、链等新技术的集合体，新一代融合ICT技术与城市管理、公共服务、市民生活等诸多领域紧密结合，城市在“智慧”的同时如果不同步针对新技术提出新的信息安全解决方案，那么一旦出现安全问题，其结果很可能是毁灭性的。

d）区域发展的不平衡也是智慧城市信息安全的一大隐忧。未来智慧城市的部分应用面临全国互联互通的可能，我国西部、东北地区整体城市发展水平和网络与信息安全发展水平还比较弱，若这些城市的部分应用还与其他发达城市互联，则信息安全问题可能进一步发酵。

1.3 城市级安全管控复杂

智慧城市的规划建设引入云、大、物、智、链等新技术，新技术的引入伴生新的安全风险和问题，为城市安全提出更高的要求。

一是安全问题更加复杂。智慧城市涉及政府部门、基础设施、通信产业、IT产业等多个方面，同时融合公共服务、通信、金融、电力、能源、交通等多个行业，行业和领域的多样性和交错性使得安全与多个领域、行业相融合，安全问题更加复杂。

二是新技术引入对安全提出更高要求。智慧城市将云、大、物、智、链、5G等新技术融合应用于城市体系，赋能到城市级基础信息设施、关键系统与平台、信息技术应用创新产业等方面，不仅需应对新技术本身安全脆弱性及安全风险，更需应对多技术融合带来的潜在、未知安全风险，这些为智慧城市安全的规划建设提出了更高的要求。

三是智慧城市安全相关关键技术亟需被突破。需探索和突破城市建模安全、算法安全、仿真安全、信息交互安全、安全可视化等一系列关键技术。

四是城市级安全建设运营无例可循。智慧城市规划、建设和运行，包括各种智慧应用的迭代更新，安全贯穿始终，城市级安全建设运营无例可循。

根据对城市安全现状的分析不难看出，智慧城市的发展亟需要城市级的安全平台进行管控，统一协同和指挥，构筑起城市网络和信息设施的安全防线。

2 智慧城市的安全态势感知体系建设方案

2.1 总体思路

有别于传统基于单个系统或单个终端进行的防护、安全能力分散、安全防护很难穷举的情况，城市级安全是从城市全局、全域角度考虑，安全与城市的智能化建设同步生长，将安全能力部署到城市的每一个角落、每一个终端、每一张网，形成城市全域的安全防护体系，形成安全外循环和内循环，确保城市智慧、安全地运转。而智慧城市安全首要的而且比较重要的是需要搭建一个城市安全的基座——安全共生系统，将所有的安全能力都变成一个个最小的原子化能力，摆放在安全能力基座中，就像摆在货架上的商品一样。城市中任何系统、任何场景（如数字交通场景、医疗场景、生态环保场景等），只要涉及安全需求，都可以选购安全原子能力，通过智能化、自动化的安全编排系统进行编排和调度。

依托于安全共生系统的基座原子化能力，定制化的生成安全平台，并以安全服务的形式赋能智慧城市的建设，研究城市级“基座+平台+服务”的安全新范式。作为整个城市安全的大脑，安全态势感知平台应当首先搭建，并协同安全基座能力形成感知、分析、处置全程的城市安全态势感知体系。

2.2 设计原则

智慧城市的安全态势感知体系在设计之初应遵循以下几个原则，并基于此原则进行体系架构的搭建。

a）构建城市级安全基础设施。构建一套面向智慧城市建设的城市级安全基座，安全基座提供原子能力库、密码云等安全基础设施，提供城市级全时、全域、全程、全局、全要素的感知、分析、处置的安全能

力。依托于安全基座的原子能力，定制化地生成城市安全管控、感知、分析、指挥、处置系统，对城市安全进行整体性的防护。

b）创新服务运营模式，安全能力按需订购。创新城市安全“基座+平台+服务”新范式，依托城市级安全基座和安全态势感知等平台，提供定制化的感知、分析、处置指挥的安全服务，安全能力由安全编排系统进行智能编排和调度，按需订购。

c）统一接口，兼容演进。安全基座和感知平台等城市安全基础设施提供通用的接口与外部连接并向外输送能力。一方面，与现有单一行业/领域内的安全态势感知模块对接，形成整体性城市安全态势感知体系；另一方面，与现有业务系统对接，为其提供安全态势源数据及威胁情报等能力。

城市级安全态势感知作为智慧城市的安全大脑，在架构设计之初就要从城市的全局出发调取城市的基础设施、网络和数据，依托于安全基座能力生成全要素的安全数据，通过智能编排和调度应用到智慧城市的各类应用场景中，同时与原有行业内态势平台、安全系统、业务系统进行数据共享，形成城市级安全态势感知体系，赋能城市安全监测。

2.3 智慧城市安全态势感知平台的研究

城市级安全态势感知平台是整体城市安全态势感知体系下的核心平台，紧密结合智慧城市基础设施和信息设施的现状需求，构建态势感知核心能力，创新服务赋能。

智慧城市安全态势感知平台是要从城市各种业务和安全系统等城市基础设施、网络中获取业务和安全数据，汇集资产、运行、网络、告警、漏洞、事件、应急等数据，存储后生成安全态势评估、安全态势预测、攻防对抗分析、资产风险分析、威胁及异常行为分析、脆弱性分析等分析结果，然后以服务的形式进行整体和专题态势的展示，并生成安全结果的预警，以上是内循环的安全态势架构。通过城市级数据的采集、分析和处置，形成态势报告和协同分析、决策方案，提供给城市管理者进行统一调度指挥，各行业领域按照统一的城市安全态势感知平台指令进行对应的安全防护处置，构成外循环的城市安全态势架构。内循环态势+外循环态势构成城市级安全态势感知体系。城市安全态势感知平台架构如图1所示。

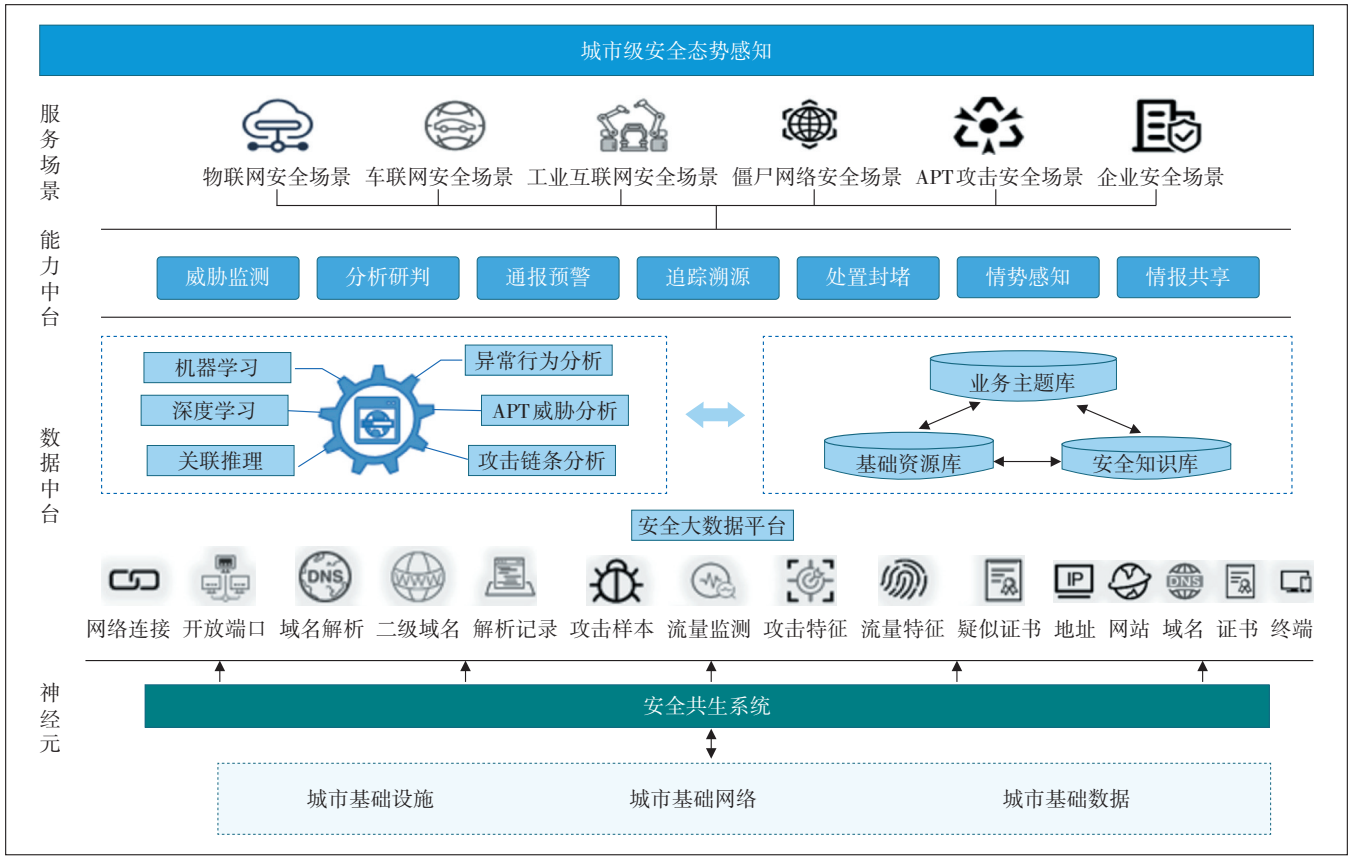


图1　城市安全态势感知平台架构

城市安全态势感知平台全方位感知城市网络空间安全态势，实现持续监测、威胁分析、情报共享、溯源定位、协同处置、攻防一体的功能，融合全网安全数据、威胁情报、基础资源库等核心资源，基于运营商在网络通道侧的全网布防，从被动的防御转变为主动的攻防，从点状防护拓展为立体防护，协助行业开展新基建和新技术安全监管、网络空间威胁监测与治理、智慧城市安全综合治理，持续为城市网络安全赋能，提高网络安全防御能力，守卫城市安全。主要体现在以下几个主要的方面。

a）城市级全域安全实时动态感知（一网监测）。实时分析和处理城市运行的各类信息，展现城市运行状态。

b）城市级安全智能辅助决策（智能分析）。通过智能分析和仿真预测，为城市管理者提供决策支持，使城市管理者能够提前预见问题，应对危机和管理资源。

c）城市级多领域协同共治（快速处置）。推动城市级安全管理向跨部门、多层级和多地域协同模式转变，逐步建立起以安全信息为核心、以安全事件为驱动的新一代城市级安全能力。

2.4 城市安全态势感知平台功能

城市级安全态势感知系统实现对城市端、网、云、系统的全面威胁持续监测、威胁分析、威胁溯源、威胁预警、安全支撑、应急响应、数据共享和态势可视等8项主要的功能。城市安全态势感知平台主要功能架构如图2所示。

a）威胁监测。具备网络行为监测和检测、攻击行为识别、僵木蠕病毒识别、未知特征攻击识别、加密流量异常监测、邮件安全监测、隐蔽信道识别、黑客工具及行为监测、样本的提取与分析等威胁情报监测功能。

b）威胁分析。实现城市资产风险分析、威胁异常分析、全时数据分析等分析能力。

c）威胁溯源。实现城市信息设施中的数据留存、数据解析、数据溯源取证等能力。

d）威胁预警。基于关联漏洞、异常行为日志、关联威胁情报以及历史攻击趋势，形成城市全局性的威胁预警能力。

e）安全支撑。实现漏洞数据支撑、安全事件数据支撑、网络攻击威胁数据支撑等能力。

f）应急响应。实现应急组织、应急场景、应急预案、应急资源、应急响应流程等管理功能。

g）数据共享。实现横纵向数据共享、威胁情报共

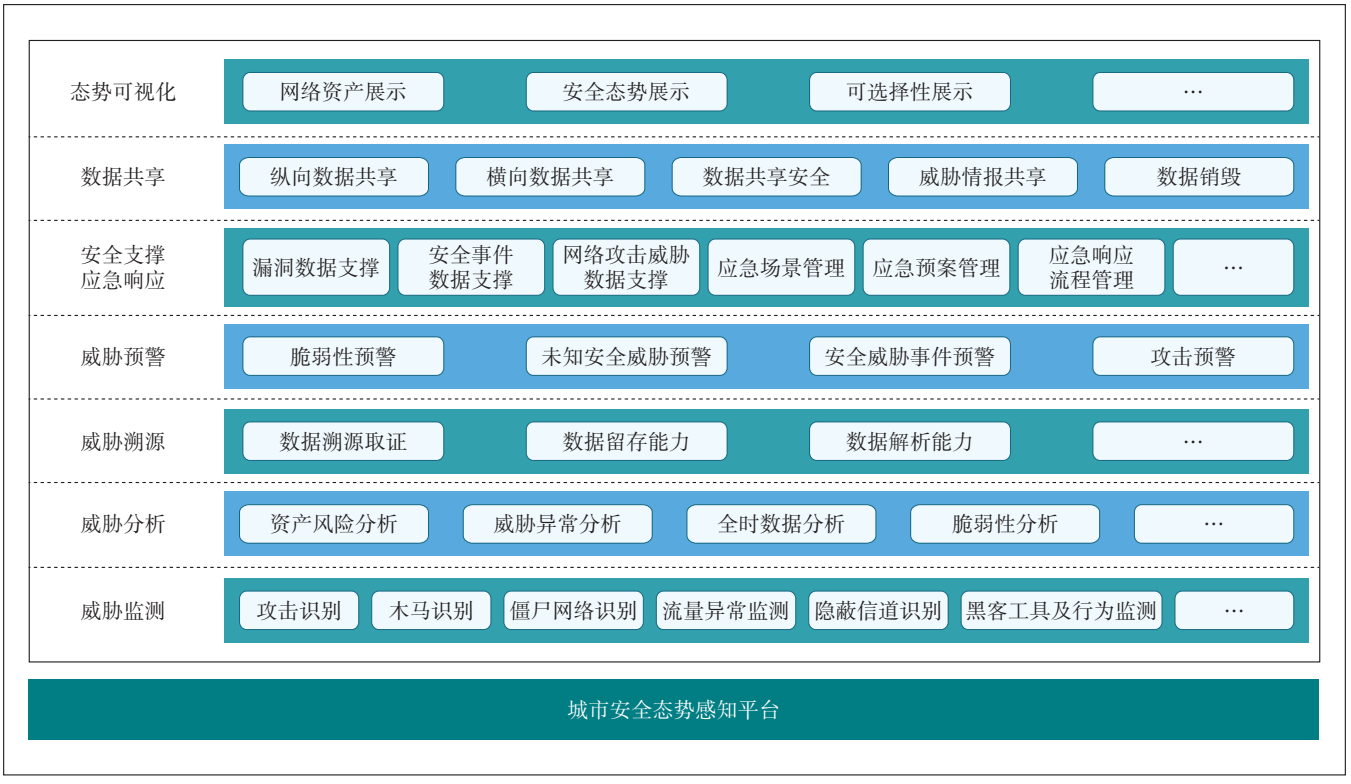


图2　城市安全态势感知平台功能

享、共享数据安全、数据销毁等功能。

h）态势可视化。动态呈现城市全域、全局、全时、全程、全要素的资产和安全态势的展示和分析支撑能力。

2.5 城市安全态势感知平台的运营

城市安全态势感知平台以城市作为单元体，运营模式必须考虑城市的统一管理和全局性。创新运营模式，将态势感知安全能力按需订购，为城市各类应用场景和需求提供定制化态势感知服务。明确城市安全态势感知平台的管理方、使用方和建设运维方，制定清晰的职责和组织机构，管理方负责城市安全态势的统一建设、管理、指挥和调度，提供方结合使用方需求提供安全能力输出，提供定制化安全态势感知分析、监测、研判及定期的城市级安全态势报告，支撑政府、委办局、企事业单位和行业用户对网络攻击、舆情、病毒、漏洞、威胁、恶意程序等网络安全事件决策和应对处置，形成端到端的安全态势感知全生态链条的全局性、闭环管理。城市安全态势感知平台的运营如图3所示。

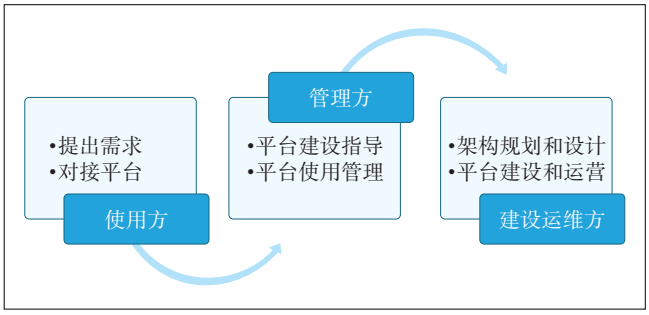


图3　城市安全态势感知平台的运营

3 城市级安全态势感知的应用场景和效果

城市级安全态势感知体系是为公共安全、数据安全、网络安全的网络空间提供态势感知、安全管理的服务，为城市级指挥调度、城市管理等公共服务提供数据协同、报告协同、通报协同、能力协同的支撑，为城市车联网、物联网、工业互联网等城市基础设施及应用提供监测预警、安全防控、协同处置的能力。对于城市级安全态势感知主要应用场景可以按需定制，推荐场景有：城市态势感知大屏、网络安全应急指挥、城市关键信息基础设施安全态势感知、城市政务网络攻击监测、重保活动大屏等等。

依托系统对某智慧城市的网络安全态势进行资产画像、威胁趋势呈现、威胁分析、攻击溯源、研判分析、问题跟踪，实现对智慧城市全域的安全事件的协同应急、联动处置。城市安全态势感知平台主要应用结果和数据分析展示如图4所示。

4 城市级安全态势感知体系发展预测

随着网络空间安全态势的日益严峻，城市级网络安全能力、平台、产品、服务体系化产业发展前景广阔。

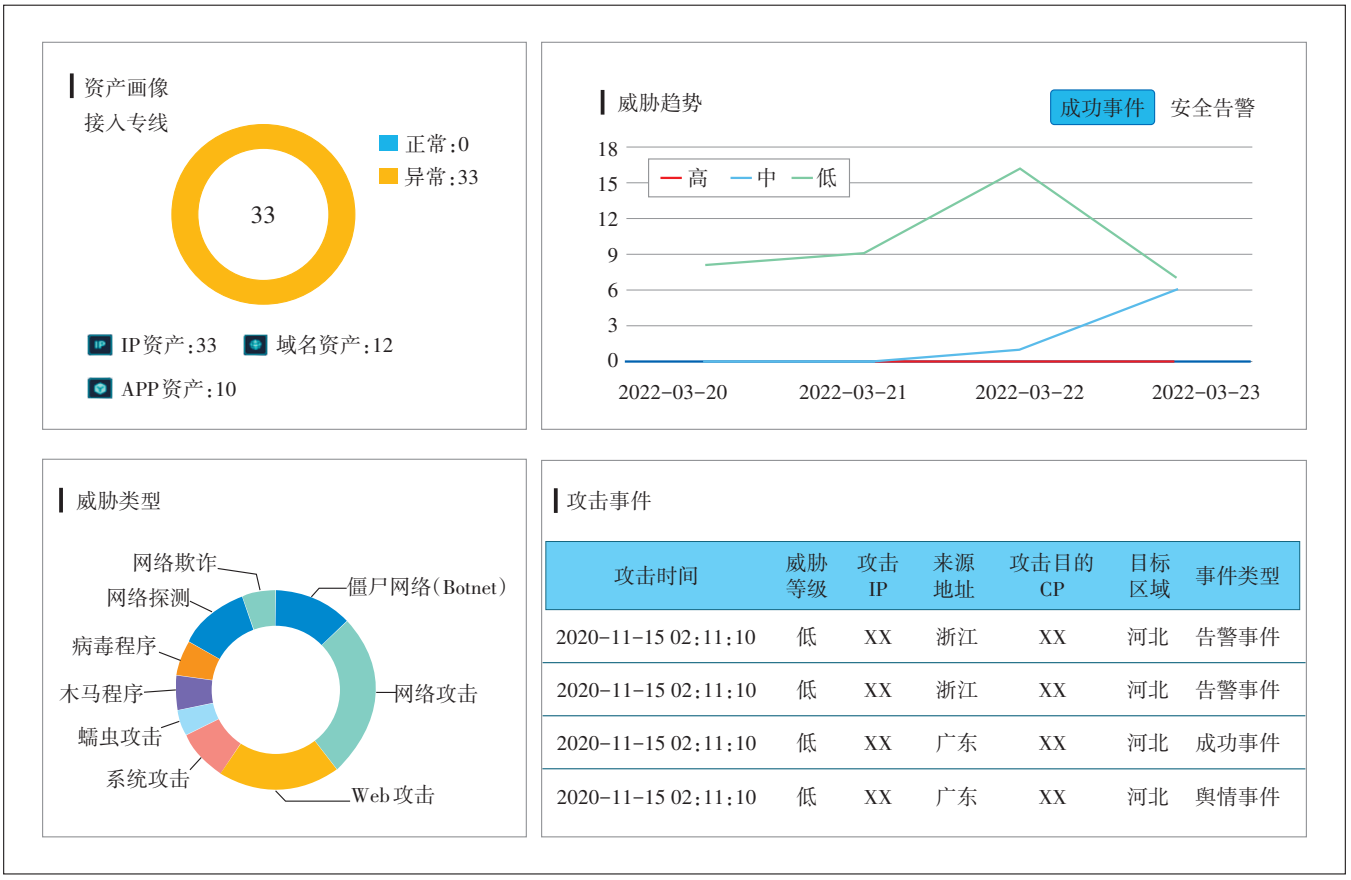
目前，国内外网络安全态势产品研发可归纳为2类，一是基于网络安全威胁识别的网络安全态势感知产品，二是基于物理行为监控的视频类安防态势感知。从应用场景维度，面向单一场景（移动通信网、物联网、工业互联网、办公内网等）的态势感知产品和感知能力较为成熟。当前，亟待从城市级全局出发，建设贯通跨网、跨域的威胁监测能力，形成跨行业、跨领域、跨生态、多维物理和数字城市场景下的全时、全域安全威胁分析和态势感知能力，打造城市级安全标杆，引领城市级安全态势感知产业发展。

5 结束语

城市级安全态势感知体系是理论创新和实践创新相结合的产物。本研究创新性地提出“基座+平台+服务”的城市安全新范式，以城市为视角突破安全理论，创新安全模式，提高安全等级，从智慧城市的全局、全域、全时、全程、全要素出发，将安全能力覆盖到数字世界和物理世界，这是全新的城市级安全范式。安全基座将安全能力按需调度和输出，生成定制化的城市安全态势感知平台，以服务的形式赋能到城市建设和管理中，为城市发展提供全面的感知、分析和处置的端到端的安全能力，为智慧城市的运营保驾护航。

参考文献：

[1] 沈昌祥，张焕国，冯登国，等. 信息安全综述[J]. 中国科学(E辑：信息科学)，2007，37(2)：129-150.
[2] 罗军舟，杨明，凌振，等. 网络空间安全体系与关键技术[J]. 中国科学(信息科学)，2016，46(8)：939-968.
[3] 张应辉，郑东，马春光. 网络空间安全体系及关键技术[J]. 中兴通讯技术，2016，22(1)：10-13，18.
[4] 沈昌祥. 建好网络空间一级学科 加快安全可信体系建设[J]. 中国信息安全，2016(12)：50-51.
[5] 张旭. 基于共生理论的城市可持续发展研究[D]. 哈尔滨：东北农



攻击时间	威胁等级	攻击IP	来源地址	攻击目的CP	目标区域	事件类型
2020-11-15 02:11:10	低	XX	浙江	XX	河北	告警事件
2020-11-15 02:11:10	低	XX	浙江	XX	河北	告警事件
2020-11-15 02:11:10	低	XX	广东	XX	河北	成功事件
2020-11-15 02:11:10	低	XX	广东	XX	河北	舆情事件

图4　城市安全态势感知平台应用效果

业大学，2004.
[6] 王慧强，赖积保，朱亮，等. 网络态势感知系统研究综述[J]. 计算机科学，2006，33(10)：5-10.
[7] 龚正虎，卓莹. 网络态势感知研究[J]. 软件学报，2010，21(7)：1605-1619.
[8] 王娟，张凤荔，傅翀，等. 网络态势感知中的指标体系研究[J]. 计算机应用，2007，27(8)：1907-1909，1912.
[9] 叶云，徐锡山，齐治昌，等. 大规模网络中攻击图自动构建算法研究[J]. 计算机研究与发展，2013，50(10)：2133-2139.
[10] 席荣荣，云晓春，张永铮，等. 一种改进的网络安全态势量化评估方法[J]. 计算机学报，2015，38(4)：749-758.
[11] 陈秀真，郑庆华，管晓宏，等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报，2006，17(4)：885-897.
[12] 赵文涛，殷建平，龙军. 安全态势感知系统中攻击预测的认知模型[J]. 计算机工程与科学，2007，29(11)：17-19.
[13] 潘垚辰. 基于共生理论的城市更新研究[J]. 智能建筑与智慧城市，2021(9)：38-39.
[14] 张勇. 网络安全态势感知模型研究与系统实现[D]. 合肥：中国科学技术大学，2010.
[15] 许建华. 基于机器学习的网络安全态势预测方法的研究与实现[D]. 北京：北京邮电大学，2016.
[16] 贾焰. 网络安全态势感知[M]. 北京：电子工业出版社，2020：11-37.
[17] 何军. 智慧城市顶层设计与推进举措研究——以智慧南京顶层设计主要思路及发展策略为例[J]. 城市发展研究，2013，20(7)：72-76.
[18] 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求：GB/T 22239-2019[S]. 北京：中国标准出版社，2019.
[19] 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术 网络安全等级保护测评要求：GB/T 28448-2019[S]. 北京：中国标准出版社，2019.
[20] 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术 网络安全威胁信息格式规范：GB/T 36643-2018[S]. 北京：中国标准出版社，2018.
[21] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会. 信息技术 安全技术 信息安全管理体系 概述和词汇：GB/T 29246-2017[S]. 北京：中国标准出版社，2017.

作者简介：
闫琛，工程师，主要研究方向为智慧城市安全、信息系统安全、网络安全等；夏俊杰，中国联通智能城市研究院副院长，教授级高级工程师，主要研究方向为移动通信网安全、信息安全、应用安全等；高枫，教授级高级工程师，主要研究方向为移动通信网安全、信息安全、应用安全等；陈奇柏，工程师，主要研究方向为网络安全、数据安全、生态应用等。