

中国西安新型智慧城市网络安全战略研究

Research on the New Smart City Network Security Strategy in Xi'an, China

石昊苏

Haosu Shi

西北政法大学管理学院 中国·陕西 西安 710122

School of Management, Northwestern University of Political Science and Law, Xi'an, Shaanxi, 710122, China

摘要: 论文从新型智慧城市网络空间安全概念出发,分析了智慧城市中国和其他国家发展现状,从四个方面指出智慧城市安全面临挑战,结合中国西安新型智慧城市网络空间安全战略愿景,重构西安新型智慧城市网络空间安全战略目标,提出西安新型智慧城市网络安全发展的三点建议。

Abstract: From the concept of new smart city cyberspace security, the paper analyzes the development situation of smart city at home and abroad, points out from the four aspects of smart city security challenges, combining with the cyberspace security strategic vision of Xi'an new smart city in China, reconstruct the cyberspace security strategic goals of Xi'an new smart city, and put forward three suggestions for the development of Xi'an new smart city cyberspace.

关键词: 智慧城市; 数字城市; 网络安全; 战略研究

Keywords: smart city; digital city; network security; strategic research

基金项目: 陕西省重点研发计划项目(项目编号: 2021NY-211); 西安市软科学研究项目——2021 西安新型智慧城市网络安全战略研究。

DOI: 10.12346/etr.v3i12.5025

1 引言

“新型智慧城市”概念在中国 2015 年底首次被提出,后上升为国家战略,是实现数据融合共享、体现新型政策机制、提升城市发展模式的系统创新工程。是综合运用 5G、物联网、人工智能、云计算、大数据、工业互联网等技术,促进城市规划、建设、管理和服务智能化的新理论和新模式,是将新型信息技术运用于城市各行各业的城市信息化的高级形态。2020 年两会之后,中国的北京、上海、深圳等多个城市掀起开展新基建的热潮,给新型智慧城市建设带来极大推动力。

2 智慧城市网络安全概念

2.1 新型智慧城市内涵

2008 年全球性金融危机爆发的背景下 IBM 提出了“智

慧地球”设想,在 2009 年又提出建设“智慧城市”的构想方案,该方案认为智慧城市可以实现政府部门相关领域的相互协作,为解决城市病提供新思路,促进各项社会事业的全面发展,成为城市管理的新形态。此后,越来越多的城市基于自身特色,制定战略规划,实施智慧城市建设。建设智慧城市,本质上是通过技术创新来引领城市生产生活方式的变革以及经济社会的发展。

2.2 新型智慧城市中的网络安全

新兴技术的迅速发展和智慧要求的不断提高,新型智慧城市的信息安全风险也日益突出。信息泄露、网络攻击等安全事件频发,国际上的“委内瑞拉大规模停电事件”“澳大利亚 3 万名政府雇员个人信息泄露”“驱动人生供应链入侵”等,中国近期较典型的滴滴出行 APP 收集个人信息问题都

【作者简介】石昊苏(1976-),男,中国陕西礼泉人,硕士,副教授,从事信息管理、决策支持系统研究。

给国家及城市信息安全稳定造成严重威胁，给智慧城市建设带来了新的安全风险和机遇挑战。

面对巨大的智慧城市网络安全风险，亟须建立健全智慧城市网络安全管理体系，从管理机制、制度规范、实施措施等方面加强体系建设，努力化解网络安全风险，促进智慧城市健康可持续发展。

3 智慧城市网络安全发展现状

随着维护国家网络空间安全已在全球形成普遍共识，作为国家网络空间安全的重要组成部分，城市网络空间安全，现已成为各国关注的焦点。

早在1998年，美国就已发布《关键基础设施保护政策》，并于5年后制定了全球第一份网络安全战略——《确保网络空间安全的国家战略》，其三大战略目标之一便是阻止针对关键基础设施的网络攻击。在此之后，美国又陆续出台了《网络空间可信身份国家战略》等一系列网络安全战略，并持续完善其网络安全战略框架。经过数年的评估，美国愈加重视对城市关键基础设施的保护，于2014年出台《提升关键基础设施网络安全框架》，拟通过深化政府与私营部门的合作，进一步提升城市关键基础设施的网络安全。英国于2009年正式公布了《网络安全战略》；俄、日两国于2013年分别发布了《俄罗斯联邦在国际信息安全领域国家政策基本原则》和《保护国民信息安全战略》，以强化城市网络空间安全等网络安全保障。与此同时，印度、澳大利亚、新西兰、加拿大、哥伦比亚等国也陆续颁布了网络空间安全战略。综上，其他国家大多采用制定法律、研制标准、实施计划等多种管理措施，保证智慧城市的网络空间安全^[1]。

中国现阶段智慧城市网络安全工作主要集中在电子政务领域，缺乏在城市乃至国家层面对网络安全体系的顶层设计和总体把握。在智慧城市发展建设过程中，国家更为重视大安全观的建立并逐步形成国家战略指导思想。中国共产党第十八次全国代表大会报告中明确指出要“高度关注海洋、太空、网络空间安全”，2014年中央网络安全和信息化领导小组成立（习近平总书记亲自担任组长），进一步强化了网络安全工作的顶层设计和总体协调，为未来国家网络安全的保障与发展指明了方向。中央网络安全和信息化领导小组组长习近平在主持召开的第一次会议中强调“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题”。

4 智慧城市网络安全发展面临挑战

4.1 新技术应用的安全需求与滞后发展的相关安全解决方案之间的矛盾

随着云计算、大数据、物联网等大量新型信息技术在智

慧城市的深度应用、政府管理体制和业务模式不断创新，民众体验不断提升，技术引领城市发展的时代已经到来。但同时，传统的网络安全解决方案已无法有效解决新型信息技术带来的安全问题，这将给智慧城市的网络空间安全带来新的风险与挑战。

现阶段，如何加强对新型信息技术的安全性研究，发展行之有效的安全产品和安全解决方案，已成为智慧城市网络空间安全发展必须解决的首要问题。新型智慧城市的规划建设，必须在安全理念创新、新型安全技术研发和新型安全解决方案设计等方面入手采取有力措施，实现网络空间新技术运用与新风险防范的最佳平衡。

4.2 强调开放共享的本质特征与现行信息安全保密管理要求之间的矛盾

智慧城市是城市信息化发展的高级阶段，我们需要打破城市传统信息系统的壁垒，通过各类信息系统的互联互通、协同运作，实现城市数据的全面开放、按需共享，通过大数据应用提高信息增值利用的力度，促进智慧城市的可持续发展。智慧城市开放共享的本质，导致不同安全等级要求的数据共存于同一个网络空间，传统网络安全边界清晰、数据安全等级明确的数据环境将不复存在。能否确保数据在智慧城市网络空间的四类传统信息系统（即互联网应用系统、企业私有应用系统、工业控制类信息系统和国家保密类信息系统）之间安全交互共享，已成为城市数据开放共享能否可持续推进的重要依据。新型智慧城市的规划建设，必须从数据管理规章制度、分保/等保制度完善和数据监管机构建设等多方面入手采取有力措施，实现网络空间开放共享与保密管理的可靠平衡^[2]。

4.3 居民在网络空间工作、娱乐和生活的现实需要与个人隐私保护之间的矛盾

智慧城市是数据的总和，大数据的高度集中和广泛运用，是智慧城市的重要标签，也是智慧城市之所以智能的重要支撑。“人在网中、事在网中、物在网中”的客观存在，使得人的行为、人与人的交互、事物对人的响应都在网络空间留下完整的数据轨迹，这些在大数据中心存储的政府部门、社会组织 and 城市居民的海量数据，必然会涉及诸多国家机密、商业秘密和个人隐私。智慧城市在为我们提供优质、高效、精准服务的同时，无时不在、无处不在的数据收集也对确保公共数据安全和个人隐私保护提出严峻挑战。新型智慧城市的规划建设，必须从法规标准、技术保护和打击网络犯罪等多方面入手采取有力措施，实现网络空间行动自由与隐私保护的动态平衡。

4.4 全面开放互联环境下的社交网络发展与维护安全有序和谐的网络空间之间的矛盾

自由已成为互联网络空间的基本属性，智慧城市开放互

联环境下的社交网络发展,更是为信息自由和言论自由提供了前所未有的便利。凭借新媒体/自媒体的匿名性、虚拟性、交互性强、传递速度快等特点,用户能够无所顾忌地讨论公共事务和批评政府及官员,舆论监督更加直接、深入和有效。但同时,由于网络空间具有虚拟性、易操控性、非理性、匿名性和无责任性等特点,反动危害思潮的宣扬以及虚假信息、谣言的传播也变得愈发难以控制。新形势下网络空间的综合治理将面临全新的挑战。新型智慧城市的规划建设,必须从深化新形势下政治制度宣传研究和强化网络舆情监测引导能力两方面入手采取有力措施,实现网络空间言论自由与和谐安全的理性平衡。

5 中国西安智慧城市网络安全发展建议

西安市“十四五”期间担负着国家中心城市建设重要任务,肩负一带一路改革开放排头兵和创新发展先行者的重要使命。2021年3月《西安市国民经济和社会发展第十四个五年规划和二〇三五年远景目标纲要》《西安市“十四五”智慧城市建设和数字经济发展规划》,对建设西安新型智慧城市提出新要求。推进“实景三维西安”,打造数字城市底座,深化城市运行管理“一网统管”,完善应急指挥平台,建设智慧城市运行管理中心,推动智慧社区、智慧校园、智慧医院、智慧商圈等,建成全民共享的智慧民生服务体系。构建“545”新型智慧城市体系(即构建资源、技术、应用、服务和管理等五个体系;打造城市综合运营、智慧城市支撑、公众生活服务和产业创新发展等四大能力;实现信息全面透彻感知、数据开放共融共享、城市治理精准精细、为民服务便捷高效、产业经济快速发展等五项目标)。

所以,从技术体系、组织、制度、管理等多方面综合考虑,通过顶层设计与统筹协调,探索西安新型智慧城市网络安全空间安全发展战略意义重大^[3]。

5.1 西安新型智慧城市网络安全战略愿景

实现智慧城市网络空间的体系安全集约安全、开放安全、和谐安全。即以城市大安全观为指导,统筹所有政府部门、社会组织和城市居民的网络安全利益,实现体系化安全;以合理的人力、物力、财力投入和能源消耗,打造绿色低碳的智

慧城市网络空间公共安全基础设施和公共安全服务,实现集约式安全;为城市公共数据的创新开和共享利用,提供可靠的数据安全保障和隐私安全保护,实现开放式安全;创建城市政府部门、社会组织和居民个人三方共建、共治、共享的安全有序和谐网络空间。

5.2 西安新型智慧城市网络安全战略目标

以打造安全的智慧城市为总目标,遵循“分网系、分领域实施,全过程、全要素保障,民主化、法治治理”的指导思想,建立集“安全基础设施体系、安全防护治理体系、安运营体系与安全管理体系”为一体的智慧城市网络安全体系,针对“城市行安全、统一安全监管、打击网络犯罪、公共数据安全和隐私保护、应急应”五个重点关注问题,健全具备“监测、防御、打击、治理、评估”功能、全面覆盖智慧城市网络安全的安全保障与综合治理方案。

5.3 中国西安新型智慧城市网络安全发展建议

统筹网络安全顶层安全设计。在西安新型智慧城市设计之初,统筹考虑城市的网络安全安全问题,从技术、管理等综合各方面保障新型智慧城市网络安全建设顺利进行。

建设基于大数据的城市网络空间态势感知系统。充分利用大数据技术,对海量系统日志、网络日志、安全日志及其他相关数据进行汇总、分析和挖掘,在掌握网络安全态势的基础上,采取事前预警、主动防御等手段及时掌握网络舆情态势、妥善处理突发网络舆情事件、防止各类安全事件的发生。

建立健全智能城市网络安全组织机构。建立健全由决策机构、协调机构、管理机构、执行机构、监管机构和技术顾问团队组成的新型智慧城市网络安全组织机构。

参考文献

- [1] 武岳山.“智慧地球”概念的内涵浅析——IBM的“智慧地球”概念说了些什么? [J].物联网技术,2011(4):1-2.
- [2] 辛本健.美国《确保网络空间安全的国家战略》评述[J].外国军事学术,2003(4):41-42.
- [3] 金鹏,刘鑫蕊,郭昆亚,等.用于支撑智慧城市运行管理的智能电网大数据挖掘系统及方法:201510243729[P].2015.