doi:10.19735/j.issn.1006-0863.2018.10.22

智慧城市建设中“非传统安全危机”识别与应对*

余潇枫　潘临灵

[摘　要] 智慧城市建设在提高城市治理效率的过程中,也给非传统安全问题的衍生演化提供了复杂的环境,致使非传统安全风险难以识别,非传统安全危机难以掌控。智慧城市建设所要面对的主要风险与危机源是信息共享与使用中出现的安全威胁,其内容有决策的“非智慧”,参与的“非智慧”以及维护的“非智慧”。识别与应对智慧城市建设中的非传统安全风险与危机需要综合使用过程识别与类别识别方法,并在防范理念、治理架构、监管法制、使用工具、国际合作等方面着力优化以提升政府安全治理能力。

[关键字] 总体国家安全;非传统安全危机;智慧城市;网络空间命运共同体

[中图分类号] D035　[文献标识码] A　[文章编号] 1006-0863(2018)10-0127-07

在“全球风险社会”与国际社会加速转型的双重语境下,非传统安全威胁在世界范围内持续蔓延,并不断上升为足以危害人类生存与发展的非传统安全危机。如何识别与应对非传统安全的风险与危机是当前政府治理能力提升的题中之议。2006年国务院发布《国家中长期科学和技术发展规划纲要(2006-2020年)》以及实施该纲要的六十条配套政策,为智慧城市建设奠定了基础。随着大数据时代云计算、物联网、人工智能等技术的兴起,与国际“智慧星球”建设相应的智慧交通、智慧医疗、智慧电力、智慧海关等纷纷被提出和实践运用,我国智慧城市建设的蓝图日益清晰。2012年11月住建部《国家智慧城市试点暂行管理办法》,标志着我国在国家层面上开始智慧城市的试点建设。智慧城市建设中信息使用与共享,在提高城市治理效率的同时增大了非传统安全的风险,为非传统安全问题的衍生与演化提供了极为复杂的环境,致使某些非传统安全风险难以识别,非传统安全危机难以掌控,并可能在较大范围内对国家安全和发展造成损害,因而在智慧城市建设过程中如何识别和应对非传统安全危机成为对国家安全治理能力的重要考验。

一、智慧城市建设中的“非传统安全危机”

(一)信息安全的非传统特征

2014年国家安全委员会成立,在提出的总体国家安全观中强调既要重视传统安全,又要重视非传统安全,要构建集信息安全等十一类安全领域于一体的总体国家安全体系,将非传统安全的重要性提升到了国家战略的层面。在总体国家安全观中,信息安全不仅是基础性的安全领域,而且还关联甚至支配着所有的其它安全领域,信息安全呈现着传统安全与非传统安全相互交织的特征,可以说是信息时代最现实、最紧迫、最棘手的国家安全问题。

计算机网络技术的出现将人类带入一个数字化的信息社会,虚拟与现实交错、数字与事物融合、时间与空间压缩成为了人们新的生存方式。信息与人类对事物了解的确定性和不确定性相关,也与事物发展有多种结果的可能性相关。在信息化时代,信息是人生存与发展的“基质”,[1]具有普遍性、再生性和共享性等重要特征:“普遍性”是进入20世纪后科学家们对信息本质的一致认同,构成世界的“基质”除了物质和能量外还有信息,信息是标示自然界、人类社会以及人类思想领域的普遍性特征要素,离开信息,就没有世界存在

* 基金项目:国家自然科学基金重点项目“非传统安全问题风险识别与防范机制——以智慧城市治理中的信息共享与使用为例”(编号:71734002);国家社会科学基金项目“基于‘人的安全’的社会风险评估与安全治理模式研究”(编号:13XGL015);海关总署2018年署级课题“构建人类命运共同体视角下的国门安全治理体系研究”

作者:余潇枫,浙江大学非传统安全与和平发展研究中心主任,公共管理学院教授,博士,杭州 310058;潘临灵,浙江大学公共管理学院博士研究生,杭州 310058

的意义可言;“再生性”是信息与物质和能量的根本不同之处,信息具有再生和增值的过程,可以在原有的基础上产生、更新、再生出新的信息,进而生发出更高的效益与价值;“共享性”是信息的另一重要特征,它不仅可以快速传播,而且可以由无限的人使用,使用的人越多,其价值越高,共享性使得信息具有了更重要的社会意义。信息社会与大数据网络凸显出的“虚拟时空”使得社会交往方式从传统的平面形式转变成一种崭新的多元复合的立体形式,使得人的存在具有了从未有过的“信息人”特征,而电子信息网络一旦成为人们社会交往的主要工具与新的“物质手段”,社会将通过交往方式的改变以实现“信息人”的本质。[2]

信息安全是指信息风险防范与信息危害的消除,或者说是指特定信息系统的完好运行及其相应构件的良好保护。[3]信息安全对国家安全来说具有极其重要的意义,一方面,以电子信息网络作为载体构建新型关系的“虚拟共同体”,引起安全关系的变化并由此产生新型的人际与国际的安全关系;另一方面,网络行为体的社会互动极易滋生“隐形犯罪”与负面的“跨界联动”,将直接危害国家安全领域。从国家安全的角度分析,国家信息安全是技术层面的信息安全与政治安全、国际安全等领域交叉后的一种与更多政治社会内容相“复合”的安全形式。[4]无论是信息普遍性、再生性,还是信息的共享性,信息安全较之一般的安全关联性更广、复杂性更高,使得国家安全被置入了一个“全域性”的安全场景中,越来越显示出“总体国家安全”的重要性与迫切性。

在智慧城市建设过程中,信息安全总体上具有以下非传统性质的特征:

(1)易受攻击性。一方面网络信息技术普遍存在缺陷和漏洞,另一方面,国家的通讯、能源、航空等建设的诸多方面依赖网络传输数据,从而存在随时被攻击的危险;此外智慧城市建设中的网络储存有协同办公系统、交互查询系统、服务操作系统等大量重要信息,还建有无人超市、文化云平台、投资广场、公共安全数据库等以及储存有与此相关联的信息,如信用卡号码、交易记录、犯罪记录等保密数据,均存在被攻击和破坏的可能。

(2)同步跨国性。智慧城市建设中的网络具有“时空压缩化”的特点,在网络运行中,国界和其他地理距离往往“趋零”,这为犯罪分子及恐怖分子跨地域、跨国界作案提供了可能,也为“他者”甚至“他国”的信息监控与入侵提供了可能。目前全球网络治理体制尚未健全,一个国家的安全威胁极易波及其他国家,一个城市的安全威胁也极易与另一个城市的安全威胁相关联,从而“同步地”造成不同程度的伤害。

(3)人机复杂性。当人的复杂性与技术的复杂性以信息技术为载体缠绕在一起,就会使得传统的技术层面的问题成为非单纯技术层面的非传统安全问题。在智慧城市的信息网络平台上,网络的隐蔽性和虚拟性使得人类本性中的善恶充分展现,现实生活中的客观、公正和安全,在网络空间规制不完善的情况下无法得到明确体现和可靠保证。

(4)高度智能性。传统的信息运用基本依靠人工手段,其速度、精确性均有限。现代智慧城市建设中的信息运用,其高度智能化特性明显,工具对象和操作程序的选择针对性强,因而对应的攻击效率高,强度大,相应的防范难度增加。加上云端数据资源的高度共享性,不仅会存在信息泄露与滥用现象,而且在恶意软件的作用下还会导致智慧城市建设的脆弱性暴露。

(5)不可预测性。智慧城市建设中会面临各种不确定的风险与危机,不仅表现在移动终端系统存在不可预测的巨大信息安全隐患,而且其在被使用过程中也会存在不可预测的安全问题,“信息攻击”或“网络破坏”在何时、何地、何网络节点爆发是不可预测的,同时由于信息基础设施系统互相联通,一个系统受到攻击必然会波及其他系统。

(6)技术不对称性。当前世界各国信息技术发展水平极不平衡,操作系统、数据库等基础软件的所有权和使用权存在潜在的安全威胁。在智慧城市建设中不同程度的技术不对称性,自然会带来各类难以确定的威胁。加之信息安全保障技术还不成熟,各种隐患会普遍存在:较轻的表现为数据丢失,较重的将会导致IP和身份窃取,更严重的有金融欺诈和盗窃,甚至会引发“信息战”和“网络战”层面上的危害等。

(7)攻防不对称性。组织甚至个人可以与国家或者国际组织在网络攻击网络上进行对抗,由于其代价低,实现手段简单,不受国界限制,在智慧城市建设中如何抵御网络攻击是需要重点考虑的非传统安全问题。

(8)文化不相容性。智慧城市建设予以公民网络开放空间进行各类政府政策实施的评价以及各种政治活动的参与,但也为互联网上的无政府文化、异质性文化、非主流文化留下了表现的余地,有可能将现有“权力决定信息分配”模式转向“信息决定权力分配”模式。若个人和非国家行为体等“电子公民”跨越地理–政治边界以数码的形式发动大规模的网络运动,影响将会在短时间内快速波及各地,对国家文化安全乃至政治安全造成威胁。

(二)智慧城市中的“非传统安全危机”界定

德国著名社会学家贝克认为工业社会之后来临的是“风险社会”,[5]而英国著名社会学家吉登斯认为现代化使人类处在自身“制造的风险”[6]中,而制造风险的人为因素来自于技术、政治和道德。这种“制造的风险”有三个明显特征,一是超越了特定的时空界限,成为一种全球化风险,无人可以在风险中幸免;二是风险不断地在制造中“再制造”,由原生风险发展成为无法弥补的风险;三是风险超过思考的“本位”和范围,蔓延与扩散在世界之中,无人可以为其承担责任。[7]非

传统安全问题，尤其是信息安全问题的萌发与兴起，使得我们所处的生存环境比以往任何时候都更加充满复杂性、不可预见性和危险扩散性。各类非传统安全威胁成为一种当代社会的“蔓延性危机”，使得人类普遍身处不安全的现实中，这种现实会给社会带来巨大的危险与伤害。

智慧城市是将新一代信息技术充分运用于城市各行各业的基于信息和知识创新的城市信息高级化形态。有专家用“智慧城市 = 数字城市 + 物联网 + 云计算”的简单公式表达了智慧城市的核心要素。[8]智慧城市的概念源于“新城市主义”（New Urbanism）和“精明增长”（Smart Growth）运动，其目的是用于解决无计划、分散的城市扩展即“城市蔓延”（Urban Sprawl）带来的诸多问题。[9]在国家战略的推动下，我国智慧城市建设逐渐完善，但智慧城市建设中出现的敏感信息外泄和外部恶意获取等信息安全也逐渐暴露出来。[10]目前大多数智慧城市建设很大程度上是通过信息化建设提升自身行政效率和城市经济效益，与理想中打造成为民主的政府平台，关注百姓的安全感与幸福感仍有差距。[11]为了确保智慧城市建设的顺利进行，避免各种可能出现的潜在风险，当前对于智慧城市的研究也与非传统安全研究对接在一起。

由于信息与网络平台是智慧城市的基础，所以一旦信息出现安全问题，就很可能会对智慧城市造成毁灭性打击，从而影响国家安全与稳定。在智慧城市中的非传统安全危机主要是指直接由信息安全威胁引发的危机，尤其是信息共享与使用中出现的各类安全危机。智慧城市建设中的非传统安全威胁总体上可以分为两类：

（1）信息共享中安全性与保密性问题引发的威胁。信息共享可以在较大程度上解决“信息孤岛”的问题，是智慧城市建设中的重要组成部分，在城市建设中的安全意义极大。[12]智慧城市的各子系统通过互联网终端与外界进行互联与信息共享，原本存在于系统中的漏洞会被互联网放大，危害数据安全性和保密性的风险就会显现。[13]智慧城市建设中信息共享可能会带来的安全威胁主要有以下三方面：第一，虚假信息干扰。由于共享信息的安全性没有保障，会出现虚假信息和错误信息，影响用户体验和智慧城市中信息流通的质量，在一定程度上降低智慧城市的影响力和作用；[14]第二，信息泄密隐患。智慧城市建设中可能出现信息泄密；第三，共享不当造成的次生和衍生问题。由于信息共享不当会引发一系列非传统安全问题，甚至危及政治安全与国家安全。

（2）信息使用中安全性和合法性问题引发的威胁。大多数的组织或学者都认为智慧城市的构成是一个“复杂系统”，[15]如何在复杂系统中安全使用信息成为智慧城市建设的重要内容。在智慧城市建设中，个人与城市通过信息进行链接与捆绑，信息使用安全将会覆盖从个人到城市的多个层级：第一，信息泄露风险大。在物联网和云计算应用中，个人信息可能被随意感知并被转移到其他存储介质（如云存储）中，[16]高新技术装备和网络系统漏洞极易被黑客们攻击，个人身份数据、医疗记录、登录名和密码易被泄露；第二，非法使用概率高。据“棱镜门事件”披露，某些公司与外国情报部门合作，在软硬件系统中设置逻辑炸弹或电脑病毒，当处于战时或需要时，敌方可启动程序开启破坏，将导致城市系统失灵，城市功能的瘫痪，带来巨大损失。[17]

信息共享与使用中安全威胁的存在，会引发智慧城市发展中决策“非智慧”、参与“非智慧”、维护“非智慧”的三类危机。首先，城市决策是对城市管理的过程调整、政策制定和措施执行，种种虚假信息会导致决策“非智慧”危机。在信息时代，政府决策更多基于数据的分析，实际上城市管理中产生的数据并没有理想中的可靠，经济领域和政治领域的数据造假现象普遍存在，数据分析、解读和呈现并非与事实完全符合，大数据采集过程存在盲点与局限性，由此得出的决策是“非智慧”的。其次，城市参与是指城市多元主体关心、关联城市决策、建设与共享的过程，缺乏自下而上的治理会导致参与“非智慧”危机。智慧城市除了硬件配置，也需要一套相适应的城市治理模式，目前多数智慧城市建设仍采取以政府为主导“自上而下”的参与方式，缺乏粘性和活力，导致参与的“非智慧”。加之信息安全保障体系的结构脆弱性，缺乏对参与过程中信息共享与使用安全性的有效保护，使得参与“非智慧”风险加大。第三，城市维护是指对城市公用事业、公共设施的维护与建设，标准不规范与管理滞后会导致维护“非智慧”危机。一方面，目前关于大数据和物联网等核心技术标准不规范是我国智慧城市维护的一大阻碍，使用核心的超高频领域需支付高额专利费用，不利于企业的发展与智慧城市的维护；另一方面，在城市发展理念中，将城市维护错误理解为“电子化”，一味追求技术与设备的高、精、尖，从而忽视城市管理信息系统的“智能化”，直接影响信息化平台的运行效率与质量，导致维护的“非智慧”。由于决策“非智慧”、参与“非智慧”、维护“非智慧”危机的存在，目前智慧城市建设仍处于“智能城市”①阶段，离“智慧城市”目标较远。

二、智慧城市建设中的非传统安全危机识别

针对目前智慧城市建设的实践进程，有学者发现存在着“重项目，轻规划”“重建设，轻应用”“重模仿，轻研发”“信息孤岛整合难度大”“依赖技术手段”等问题。[18]在复杂的大数据网络环境中，首要解决的问题就是辨析出潜在的、可能诱发非传统安全危机的风

① 一般认为“智能城市”作为一种城市发展新阶段，以智慧的技术为核心，关键是实时反馈的数字神经网络和自主决策系统。而“智慧城市”中技术只是城市目标的一个组成部分而非全部，还包含了智慧的人本因素。

险源，并在此基础上根据其性质分类，匹配政府现有能力，提供不同模式的解决路径。

（一）非传统安全问题风险类别

目前非传统安全风险识别技术中比较得到认同的是时间识别、类别识别、过程识别、优先级识别四种：

（1）时间识别法。时间识别是以时间为维度来衡量非传统安全的风险，一般以标志性事件作为划分，在研究中有以冷战结束、金融危机、“9·11”事件等作为阶段性划分节点，来识别中国在各个阶段所面临的非传统安全问题。[19]其优势在于简单易行，能够快速识别出各阶段的各种风险，弊端是识别方式过于死板，操作上较难建立标准，识别范围过于宽泛，在识别结果上只能识别范围内风险，对于新问题、新趋势缺乏有效的识别力。

（2）类别识别法。类别识别法是目前较为普遍使用的识别方法，总体国家安全观中对于安全类型划分即使用类别划分法，研究中有按照风险发源地划分将非传统安全风险划分为内源性风险、外源性风险、双源性风险和多源性风险，[20]有按照指涉对象划分为国际安全、国家安全和人的安全。类别识别法可以有效区分不同种类的非传统安全风险并快速寻找到其风险特征，有利于根据风险特征而有针对性地采取预警、防控、应对等有效措施。其局限在于无法判断风险的危害性，尤其是对于衍生的、叠加的、复合的风险，无法准确识别风险等。

（3）阶段识别法。风险识别被普遍认为是一个动态过程，根据风险的演变阶段有学者提出将风险分为新生风险、交叉风险与复发风险，分别采取“识别－分析－定级”“确权－共担－追责”“消除－干预－规避”的防控机制。[21]其优点在于聚焦特定风险，根据风险的演变制定对应的解决机制，局限性在于无法同时处理大量案例。

（4）优先级识别法。由于一个国家和地区的不同历史时期和发展阶段面临的非传统安全的侧重点不同，有必要在类别清单基础之上设立优先级识别，[22]作为一种比较科学与规范的识别方法，该方法一方面保留了类别识别法的严谨与规范，另一方面能够较好把握危机程度，辅助科学决策。其局限在于无法识别类别中新出现风险。

综上所述，非传统安全的风险识别是当前非传统安全理论的前沿问题与重要趋势，对风险源的识别和分类是目前研究的主要内容。从研究对象来看，现有研究往往局限于某一类特定的风险，研究对象不够集中，并未回答在智慧城市的背景下，通过何种识别技术、路径和识别模型，可以防止潜在风险被泛化或忽视。

智慧城市区别于“智能城市”“数字城市”“信息城市”等相关概念的核心在于强调以“人”为核心价值，聚焦人的需求、价值及实现，围绕人的生存与发展展开信息技术的可持续创造与应用，而非在纯技术上（如互联网、云计算）的突破与运用。智能技术、数字鸿沟、智能互通等引发的威胁造成了智慧城市的“结构性脆弱”，是智慧城市与生俱来的特征，是智慧城市安全的属性。[23]由此可见，智慧城市建设中的主要风险不仅来自外部与他者，而且更多的是来自于城市内部与自身。本文在以上各种风险识别思路的基础上，针对智慧城市的特点，提出一种综合了过程识别与类别识别的“综合性识别”方法。根据非传统安全问题发展和演变过程，按照其内在规律性，“综合性识别”主要可以分为风险来源、发展形式、传递路径、演化结果四个关键环节：

（1）风险来源。风险来源分为突发来源和渐发来源，该区分与发生时间和处置者对于事件的把握均有关系，其中突发来源的前期并未有任何影响与表现，而渐发来源一般都留有一定的反应和准备时间。智慧城市建设中的风险来源多为突发来源。智慧城市的运营和建设得到了各种智能技术的支持，信息技术作为一把“双刃剑”，在创造便捷的同时也隐藏着各种难以预测和管理的风险与难题，问题的超前性、威胁的自发性、风险的难控性，对识别和判断风险造成极大困难。

（2）发展形式。发展形式分为空间扩展与程度扩展，空间扩展指在空间蔓延，程度扩展指在烈度上增强。智慧城市中的危机发展形式多为空间扩展与程度扩展结合。智慧城市局部的风险能够突破时间和空间的界限，迅速造成城市整体的不安全，增加城市的“脆弱性”。如地震后局部地区的城市功能受损，将跨过地理空间限制，直接连带影响如通信、交通、能源、卫生等其他城市功能系统，在危害程度上造成指数增长，成为城市运行的整体性威胁。

（3）传递路径。传递路径分为自发路径与触发路径，自发路径指风险并未引起其他相关的变化和不良后果，只是自身的演变，如一次性爆炸后引发火灾，触发路径是指风险触发其他变化，从而引起不良后果，如火灾后的“火借风势、风助火威”。智慧城市中的危机传递路径多为自发与触发结合。智慧城市内部与城市之间的互联互通，危机以“跨界”存在，跨越城市、跨越国家、跨越区域的威胁导致风险或危机传播更具有破坏性。

（4）演化结果。演化结果分为优化结果和劣化结果两种，演化结果在于对“转折点”的把握，优化是指通过应对使得风险消除、危机转化为转机，劣化是指应对处置不当，产生“失稳效应”，[24]从而影响整个系统的正常运行与安全。智慧城市建设核心的“制网权”已与“制陆权”“制海权”“制空权”并列成为安全争夺的制高点，智慧城市中危机的演化结果已不仅是防范能力的体现，而且将会关系到城市的生存或毁灭。

（二）非传统安全问题风险识别能力要求

非传统安全作为一种“广义安全”，[25]其主要理论

分析来自把人的生存状态分为四个层级：优化状态、弱化状态、劣化状态和危险状态，并将这四种状态与人的生存需求的安全状态相联系，可以得到四种安全状态：生存优态、生存弱态，生存劣态，生存危态。[26]根据管理科学中的“情境－应对”决策范式，风险可以从发生频率和可控性两个角度区分（表1），当风险符合发生频率低及可控性高，可以将该风险称为“常态风险”，爆发的危机称为“常态危机”；因常态危机应对失当而引发的复合性、系统性和异质性冲突的危机，即可控性低与发生频率高的危机，称为“非常态危机”，如因网络隐私泄露引发的社会安全危机等，直接对社会结构和政权稳定造成整体性和持续性危害等；至于发生频率低可控性低或频率高与可控性高的风险存在有常态危机与非常态危机两种可能，前者脆弱性在可控性低上，后者的脆弱性在发生频率高上。

表1　常态风险与非常态风险识别表

频率 / 可控性	低	高
低	常态 / 非常态	非常态
高	常态	常态 / 非常态

区分“常态危机”与“非常态危机”的意义在于，在数据时代云计算、物联网、人工智能等技术的广泛应用下，风险发生频率显著增加，风险形态超前，传统的危机应对方式并未能有效解决对应管理部门缺乏、专业救援队伍缺乏、相应法律保障缺乏，现实条件应对缺乏的“非常态危机”。例如互联网传播具有信息丰富、表达快捷、渠道多元、传播急速等特点被广泛使用在政府信息公开中，但网络舆情涉足多个领域，突发性明显，易被发酵，热点、焦点、沸点异常复杂多变。同时，由于网络传播渠道的多样性、信息内容的差异性、信息传播的叠加性，网络信息传播极易出现升级、拐弯、变质，政府与公民在现实中的实体关系与在网络上的虚拟关系的冲突，现实价值观与网络价值观的冲突、社会利益与网民利益的冲突，对政府执政能力和社会公信力造成了极大的考验。之所以强调非常态危机，是强调常态危机的不当应对会引发更为严重的跨职能部门权限的整体性政治危机或社会危机。

不同的危机类别和不同的安全状态下对政府风险识别能力要求不同。安全风险类别从常态到非常态，风险来源、发展形式、传递路径、演化结果愈加复杂，识别程度愈加困难。安全状态从生存危态到生存优态，对社会承受能力、风险应对能力要求逐渐增加。从危机类别、安全状态与应对能力三个维度创建分析矩阵（图1），可见当社会面对非常态危机时，而对于安全状态的需求是安全优态时，需要的风险识别能力最强，对风险和危机的掌控能力最强，对“临界点”“关键点”“转折点”的把控最恰当，对应的政府能力要求最大，如在智慧城市建设中应对突发的、破坏性的网络舆情危机对政府的能力要求。

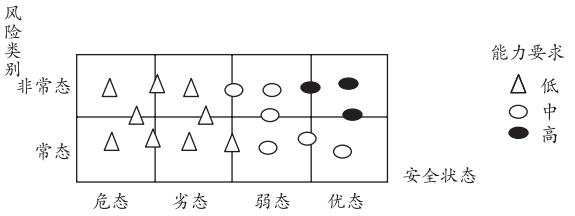

图1　危机类别、安全状态与应对能力矩阵图

三、智慧城市的非传统安全危机应对

智慧城市中的非传统安全危机应对形势较传统城市更为严峻，信息共享与信息使用中的非传统安全危机防控主要路径有三：即智慧城市的决策、参与、维护如何“更智慧”。首先是决策需要更智慧：城市决策的参考要素增多，决策时间区间大幅缩短，决策将更侧重整体性与前瞻性，并且更多地从静态决策转向动态、实时、联动式决策。其次是参与需要更智慧：大数据平台的开放以及以此为基础的各类网络应用的开发，将使更多利益主体和公民个人更加方便掌握城市中的各类信息并参与其中，智慧城市建设的参与更侧重于普遍性与互动性的实现。第三是维护需要更智慧：在数字化不断充分实现的条件下，城市治理的透明度和公开度的需求大大增加，智慧城市建设更加依赖于高精度空间数据的大量采集，其维护更应侧重精密性与时效性，危机的预案与防范措施更侧重可仿真性与可控性。为了实现决策、参与、维护的“更智慧”，智慧城市建设与危机防控需要在防范理念、治理架构、监管法制、使用工具、国际合作上加以优化，以适应挑战。

（一）防范理念优化

智慧城市治理中，信息通信技术的融合和发展，推动了信息共享与知识扩散，依托物联网可实现城市功能中的智能化呈现；云计算和智能分析技术可以支持城市治理中大量信息的处理和决策；信息技术发展与全球化、城市化的互动重塑了城市空间。然而，在实践中不乏一些城市将“智慧城市”作为一种城市推广的营销手段，在实质性投入和建设方面甚少，亦或是用智慧城市概念作为包装，有学者针对智慧城市发展的矛盾提出智慧城市标签化（Urban Labelling）现象，质疑智慧城市的理念、背后逻辑和可持续发展问题。[27]识别与应对非传统安全危机的首要任务是防范理念的优化，厘清智慧城市建设背后的隐藏逻辑，厘清智慧城市建设中技术决定论倾向与对资本依赖的局限，辨析智慧城市治理中决策、参与和维护环节中的主要任务，从单一防范拓展到全面防范，从部门防范扩展到大众防范，从强制防范延伸到自主防范，从战术防范提升为战略防范，同时考虑到常态危机与非常态危机的两种可能，推动城市健康可持续的发展。

（二）治理架构优化

智慧城市治理中，信息的共享与使用涉及庞杂的主体，存在复杂的信任问题和授权问题，对应的非传统安全保障体系非常脆弱。发达国家在非传统安全风险

和危机治理体系上已经形成一套较为完善的架构，如英国“渐进整体型”架构，在风险治理管理环节充分包纳风险意涵，实现风险治理职能的全覆盖；美国“国土安全型”架构，从国家战略高度将保护意识和降险理念集成于国家风险治理系统，建立全社会集成、共同参与的动员运行机制；加拿大“综合平衡型”架构，将风险识别、评估与应对从政府治理实践扩展到组织结构、功能、过程与文化之中，各个层面将风险评价结果集成到部门决策中。智慧城市中云计算、物联网、人工智能等技术的运用，将极大地整合资源，改变城市教育、交通、医疗信息独立、割裂的状态。然而“信息孤岛”仍是当前智慧城市建设中资源整合的最大障碍。在技术层面，缺乏统一的行业标准、建设标准和评估标准来约束和指导，不同系统之间对接复杂无形增加“智能孤岛”的可能；[28]在管理层面，由于部门横向协同困难和行政分割现象的存在，在技术上容易解决的问题，但是在现有管理体制中难以实现。有学者提出面对智慧城市建设中因智能技术、数字鸿沟、智能互通等特性引发的威胁，为突破内外分离、敌我差异、进攻与防御的二元划分，应构建具有“总体安全”或“场域安全”特征的“无边界安全共同体”作为应对智慧城市安全结构脆弱性的一种架构优化，[29]同时也为防止常态危机转化为非常态危机以及有效应对非常态危机提供整体性的制度保障。

（三）监管法制优化

我国作为智慧城市建设的后起之国，在信息安全、隐私保护、人工智能等方面的法律法规都尚未成熟，尤其是对大数据的隐私保护的重视程度不够，对问题爆发的反应灵敏度不够。2012年以来，我国对大数据环境下的信息共享、信息安全和隐私保护重视程度逐渐升高，2014年成立中央网络安全和信息化领导小组，负责国家网络安全和信息化发展重大问题，2016年出台《国家安全法》，对个人信息的使用和保护做了规定，在《国家信息化发展战略纲》中提出将研究制定《个人信息保护法》、《未成年人网络保护条例》促进信息化发展。智慧城市和大数据的发展，一方面赋予了信息安全与隐私保护新的内涵和意义，另一方面也对此提出了更高的要求和挑战，个人隐私权已经从传统的“生活安宁不受干扰”的消极权利演变为具有积极意义的“信息隐私权”。在此背景下，应尽快解决目前信息安全和隐私保护法律规定零散而不完整的现状，加快制定和颁布《个人信息保护法》，构建完善的个人信息保护法律体系，完善应急管理“一案三制”中关于网络信息安全应对的相关说明。

（四）使用工具优化

智慧城市治理中，治理工具与应用系统建设自身的不完善，也是诱发非传统安全问题的重要风险源。伴随科学技术发展的不断进步，量性工具方法已较为普遍地在非传统安全危机识别中得到了利用，现代高科技手段在国家风险检测、评估、信息传播中发挥出工具保障性的作用。在智慧城市建设中，大量的时事数据为城市中的突发事件和危机事件的预测与应对提供了更好的工具，很大程度上增加了风险识别预判的准确性。但在实际操作中，一方面，智慧城市评价指标中普遍以技术和硬件为导向，忽视工具对危机识别与应用的辅助与促进，以在实践中具有代表性的IBM智慧城市评估标准、欧盟中等规模城市智慧排名评价指标和浦东新区智慧城市指标体系1.0三者为例，评价指标中涉及智慧经济、智慧公民、智慧治理、智慧技术、智慧环境、智慧生活六个大类，[30]缺少风险识别、应急管理、危机应对的对应指标；另一方面，技术层面大量工具目前仍受制于他人，存在极大的安全威胁，当前最重要的是掌握拥有自主知识产权的核心技术和关键技术，包括传感器、芯片尤其是高频RFID等物联网核心技术层面的突破，网络数据平台的建设，大数据收集、存储、集成和处理系统建设。

（五）国际合作优化

从国际上智慧城市的开发运作模式看，具有公私合作、政企联盟等多种思路，如公私合资建设管理，典型代表是赫尔辛基Arabianranta项目；如政府带头私人企业参与，典型代表是新加坡One North项目；如政府投资管理，研究机构和非盈利组织参与，如阿联酋Masdar项目。从国际经验和实际国情来看，我国发展智慧城市比较适合采取政府主导投资，国内外多家城市开发公司合作规划开发的模式，以促进城市运行的可视化、可控化、智能化、可预测及可量化评估与持续优化。在全球化、信息化时代，城市建设中的信息共享、信息安全与隐私保护已经是各个国家共同面临的问题。第三届世界互联网大会指出信息安全的发展特点是“无国界、无边界的”，提出“深化网络空间国际合作”构建“网络空间命运共同体”，为智慧城市建设中应对信息共享、信息安全与隐私保护提供了路径。

[参考文献]

[1][2]余潇枫，张彦．“信息人假说”的当代建构[J]．学术月刊，2007（2）．

[3][4]余潇枫．非传统安全概论[M]．杭州：浙江人民出版社，2006.228，234-236.

[5][德]乌尔里希·贝克．风险社会[M]．上海：译林出版社，2004.

[6]Anthony Giddens. *Runaway World: How Globalization is Reshaping Our Lives*. London: Routledge, 2002.

[7]余潇枫．“平安中国”：价值转换与体系建构——基于非传统安全视角的分析[J]．中共浙江省委党校学报，2012（4）．

[8]李德仁，姚远，邵振峰．智慧城市中的大数据[J]．武汉大学学报(信息科学版)，2014（6）．

[9]Burchell R W, Downs A, Galley C C, et al. The Activities and Benefits of Smart Growth. *Population*, 2003, 49.
[10]娄欢,黄志华,徐啸峰等:三大信息安全策略为智慧城市保驾护航[N].人民邮电报,2016-03-24.
[11]许庆瑞,吴志岩,陈力田.智慧城市的愿景与架构[J].管理工程学报,2012,26(4).
[12]Washburn D, Sindhu U. Helping CIOs Understand "Smart City" Initiatives. *Growth*, 2009(2).
[13]Catteddu D. *Cloud Computing: Benefits, Risks and Recommendations for Information Security*. Heidelberg: Springer Berlin Heidelberg,2010.17.
[14]Jin J, Gubbi J, Marusic S, et al. An Information Framework for Creating a Smart City Through Internet of Things. *IEEE Internet of Things Journal*,2014(2).
[15]IBM 商业价值研究院.智慧地球[M].东方出版社,2009;Caragliu A, Bo C D, Nijkamp A P. Smart Cities in Europe. *Urban Insight*, 2011(2).
[16]张毅,陈友福,徐晓林.我国智慧城市建设的社会风险因素分析[J].行政论坛,2015(4).
[17]袁艺.智慧城市的网络安全隐患及对策[J].中国信息安全,2016(7).
[18]辜胜阻,杨建武,刘江日.当前我国智慧城市建设中的问题与对策[J].中国软科学,2013(1).
[19]余潇枫,李佳.非传统安全:中国的认知与应对(1978~2008年)[J].世界经济与政治,2008(11).
[20]余潇枫.非传统安全概论[M].北京:北京大学出版社,2015.73-74.
[21]唐钧.社会公共安全风险防控机制:困境剖析和集成建议[J].中国行政管理,2018(1).
[22]Emmers R, Caballero-Anthony M, Acharya A. *Studying non-traditional security in Asia: trends and issues*. Marshall Cavendish Academic,2006. pp7-10.
[23][29]廖丹子.无边界安全共同体——探智慧城市公共安全维护新路向[J].城市规划,2014,38(11).
[24]张沱生,史文.中美安全危机管理案例分析[M].北京:世界知识出版社,2007.83.
[25]余潇枫.从危态对抗到优态共存——广义安全观与非传统安全战略的价值定位[J].世界经济与政治,2004(2).
[26]余潇枫.非传统安全与公共危机治理[M].杭州:浙江大学出版社,2007.44,101,34.
[27]Hollands R G. Will the Real Smart City Please Stand Up? *City*, 2008(3).
[28]蒋建科.智慧城市建设别陷入更大信息孤岛[N].人民日报,2012-05-21.
[30]王思雪,郑磊.国内外智慧城市评价指标体系比较[J].电子政务,2013(1).

(责任编辑 葛 东)

Identifying and Coping with Non-traditional Security Crises——A Study Based on the Construction of Smart City

Yu Xiaofeng Pan Linling

[**Abstract**]While constructing a smart city, the efficiency of urban governance is raising, which provides a complex environment for non-traditional security issues and makes the risk hard to identify and the crisis hard to handle. The main risks and crises of a smart city are caused by network information security on network platform, especially by sharing and using information. The risks and crises include unsmart decision, unsmart participation and unsmart safeguard. Identifying and coping with "Non-traditional Security Crises" need to use process identification and category identification comprehensively. The enhancement of security governance ability is necessary in prevention ideas, supervision institutions, regulatory tools and international cooperation.

[**Keywords**]outlook on overall national security, non-traditional security crises, smart city, a community of shared future in cyberspace

[**Authors**]Yu Xiaofeng is Director at the Center for Non-traditional Security and Peaceful Development Studies and Professor at School of Public Affairs, Zhejiang University;Pan Linling is Postgraduate at School of Public Affairs, Zhejiang University. Hangzhou 310058