

# 美国推动物联网发展的相关政策研究

乔 健

(中国科学技术部, 北京 100862)

**摘 要:** 本文总结了美国联邦政府为推动物联网发展所采取的一系列政策措施, 如构建技术标准体系、加强网络安全保障、制定“创新友好型”政策法规、保障频谱资源、支持研发与示范、促进行业协作等, 并分析了未来美国对物联网政策框架在基础设施、政策平衡、标准演进、市场发展等层面的考虑, 以期对我国物联网发展提出启示与建议。

**关键词:** 美国; 物联网; 信息技术

**中图分类号:** TP393 **文献标识码:** A **DOI:** 10.3772/j.issn.1009-8623.2017.06.004

物联网是新一代信息技术的高度集成和综合运用, 已成为全球科技与产业变革的核心驱动力, 以及经济社会绿色、智能、可持续发展的关键基础。目前在车联网、智能家居、医疗健康、智能可穿戴设备等重点消费领域, 物联网呈快速发展态势, 催生出一系列新产品、新服务和新业态; 而物联网与大数据、人工智能等技术结合, 在工业制造、城市管理、公共安全等领域有着更加重要的应用潜力。据预测, 到 2020 年全球联网设备将达到 260 亿件, 是 2015 年的 1.6 倍<sup>[1]</sup>, 而到 2025 年物联网对全球经济的贡献将达到 4 万亿~11 万亿美元<sup>[2]</sup>。

美国是物联网技术的主导者和先行者之一, 凭借雄厚的技术实力和市场积累, 物联网已在美国各领域得到了广泛应用。美国一直以来强调以企业为主体, 通过多方协商的方式引导产业发展, 政府针对各领域应用有针对性地出台政策, 促进技术创新并加强合理监管。由于物联网的复杂性、跨领域性和对经济社会的全方位的影响潜力, 美国近期强烈呼吁在国家层面制定物联网战略政策规划。

本文首先归纳美国联邦政府为推动物联网发展已采取的一系列政策措施, 其次介绍未来美国对物联网政策框架的一些考虑, 最后对我国物联网发

展提出几点启示与建议。

## 1 美国推动物联网发展的相关政策措施

### (1) 构建技术标准体系

物联网产业的迅速发展离不开新技术、新产品的统一标准, 以美国标准与技术研究院 (NIST) 为首的政府部门通过构建物联网技术标准体系, 提升不同技术协议和产品规范的互操作性, 促进产业发展。

2014 年, 美国标准与技术研究院成立了信息物理系统工作组 (CPS PWG), 广泛召集物联网与工业互联网领域的专家, 讨论形成对于信息物理系统基本概念的共同理解与方法论, 定义技术标准体系的基本原则, 从而促进其在制造、交通、能源、卫生等不同领域的开发与应用。2016 年 5 月, 该工作组发布了《信息物理系统框架》<sup>[3]</sup> 文件, 从参考架构、网络安全与隐私、时序与同步、数据互操作性、应用实例几个方面为物联网提供全面的定义和术语。该工作组还在智能制造、智能电网、灾害响应等一系列领域开展研究, 为物联网应用提供技术参考。

美国标准与技术研究院的工程实验室 (Engineering

作者简介: 乔健 (1984—), 男, 工学硕士, 主要研究方向为科技政策及国际科技合作。

收稿日期: 2017-06-03

Lab) 实施了多项计划, 开展促进物联网应用的计量研究。例如, 其传感与感知系统工作组进行与智能制造和建筑应用相关的计量研究, 其智能配电网高级计量项目旨在提高智能电表传感器技术的准确性。美国标准与技术研究院还在一系列物联网相关领域出台了技术标准框架文件, 如 2014 年 5 月发布了《智能电网互操作性标准框架与路线图》<sup>[4]</sup> 第三版, 2015 年 9 月发布了《大数据互操作性框架》<sup>[5]</sup>, 目前正在起草《基于物联网的智能城市框架》。

此外, 美国交通部 (DOT) 的智能交通系统标准计划也在开展多个项目, 支持智能交通系统 (ITS) 标准和架构的互操作性, 包括进行标准测试、提供技术支持以及开发操作指南等。

### (2) 加强网络安全保障

物联网产品缺乏足够的计算和存储能力, 难以得到传统信息安全手段的保护, 因此病毒攻击防不胜防, 风险隐患日益突出。2016 年 10 月, 美国物联网设备遭到黑客攻击, 全美互联网服务出现大面积瘫痪。随着物联网应用向工业制造、能源电力和智慧城市等关键领域延伸, 一旦发生信息安全问题, 后果将十分严重。

美国政府采取了多项举措加强物联网信息安全。政府多部门发布白皮书或指南, 提升社会各界的物联网安全防范意识。2014 年美国标准与技术研究院发布《改善关键基础设施网络安全的框架》, 对包含物联网在内的多种连接技术给出了网络安全最佳实践和建议, 并于 2017 年 1 月根据反馈意见推出新版<sup>[6]</sup>; 2015 年, 美国联邦贸易委员会 (FTC) 发布物联网产品安全高级指南<sup>[7]</sup>, 指导企业在物联网产品设计之初即考虑安全原则; 2016 年 11 月美国国土安全部发布《确保物联网安全的战略原则》白皮书<sup>[8]</sup>, 向物联网设备和系统开发商、管理者及个人提出了一组网络安全实践准则建议。

针对物联网技术在能源、消费电子、医疗和智能驾驶等特定领域的应用, 美国出台了一系列技术指南或行动建议, 明确这些领域物联网产品的信息安全要求。2014 年, 美国标准与技术研究院发布了针对智能电网的安全指南<sup>[9]</sup>; 2015 年, 美国联邦通信委员会 (FCC) 发布了消费类物联网设备的网络安全要求<sup>[10]</sup>; 2016 年, 美国食品药品监督管理局发布指南<sup>[11]</sup>, 督促医疗设备厂商关注售出的

联网设备的安全问题; 此外, 美国交通部下属的国家高速公路交通安全管理局发布《智能车辆网络安全最佳实践》<sup>[12]</sup>, 明确具有联网功能车辆的安全保障要求。

针对物联网产品现存的安全漏洞, 美政府部门鼓励研发新技术以改善物联网设备的信息安全。美国国防部高级研究计划局 (DARPA) 于 2015 年 9 月发起“安全模拟”项目, 资助一系列前瞻性研究, 拟通过分析物联网设备的电磁、声光、温度等信号异常变化来检测病毒异常, 从而有效识别潜在的物联网攻击和入侵, 特别是那些可能绕过传统安全控制的攻击。

### (3) 制定“创新友好型”政策法规

针对自动驾驶、车联网等新兴技术, 美国相关政府部门积极推进政策法规制定, 引导技术应用, 扶植新兴产业发展, 同时注重规避新技术可能带来的负面影响。

2016 年 12 月, 美国交通部推出通知, 将考虑制定一项新法规, 要求所有汽车厂商为新出厂的消费车辆配备车对车 (V2V) 通信技术, 从而减少交通事故。目前, 该法规已正式进入立法阶段。如获通过, 汽车厂商将有四年时间去履行这一规定, 到 2023 年全美新上路的轻型车辆按计划都将安装车对车通信系统。与此同时, 美交通部正在考虑制定车对基础设施 (V2I) 通信技术的立法建议。

2016 年 9 月, 美国交通部发布了《美国自动驾驶汽车政策指南》<sup>[13]</sup>, 从自动驾驶汽车性能指南、州政府法规模型、美国国家公路交通安全管理局 (NHTSA) 现有的监管方式和新的监管方式四个方面, 为生产、设计、供应、测试、销售、运营或应用高度自动驾驶汽车的传统汽车厂商和其他机构提供了一个具备指导意义的前期规章制度框架。该指南采用美国汽车工程师学会 (SAE) 的定义作为评定汽车自动驾驶水平的标准, 从低到高分 L0 到 L5 五级, 并将 L3 及以上作为自动驾驶汽车的界线。该指南规定新的自动驾驶汽车或技术应满足 15 个要点的安全评估才能上路, 包括数据记录和共享、隐私、车辆网络安全、耐撞性能、消费者教育和培训、碰撞后表现、法规遵守特性、操作设计、物体和事件的探测及响应等。

#### （4）保障频谱资源

频谱是包括物联网在内的信息技术应用所必需的稀缺资源，美国联邦通信委员会等政府部门采取一系列措施，释放更多的频谱资源，平衡许可频段与免许可频段的供给，促进物联网商业应用快速发展。

2016年8月，美国联邦通信委员会全票通过了“频谱新领域”提案，旨在向广泛应用于医疗保健、教育、车联网、智能能源的第五代移动通信（5G）开放24GHz以上高频频谱共计10.85GHz。美国也成为世界上第一个为5G通信技术规划频谱的国家。其中，许可频段数量是目前美国联邦通信委员会已授权许可频段的4倍，免许可频段资源数量是Wi-Fi所使用的频率资源的15倍。

美国联邦通信委员会表示，美国的5G频谱策略的最终目标是在低频段、中频段、高频段分别开放频谱资源，为下一代无线网络部署提供保障。因为5G技术涉及智能天线系统、新的传输模式、低能耗系统、网络虚拟化等多种技术的组合，因此需要在多个频段采取新的不同接入方式。在适用于广域覆盖的低频段，美国正在通过“激励拍卖”促使广播公司将他们的600MHz低频频谱释放出来，未来移动运营商将有机会在激励拍卖中获得这些低频频谱；在频谱应用效率最高的中频段，美国联邦通信委员会制定了3.5GHz频段频谱共享机制，并将在未来释放更多中频频谱。

#### （5）支持物联网相关技术的研发与示范

美国联邦政府及其各部门重视通过支持物联网相关技术的研发与示范应用，加快技术进展。2015年9月，美国启动跨部门的“智能城市计划”，希望通过物联网技术解决市政挑战并改善政府服务，并投入超过1.6亿美元开展从联网车辆试点到先进应急响应技术的研究。2016年9月，白宫再次为该计划追加预算8000万美元，集中于气候变化、交通、公共安全、城市服务等领域的物联网技术应用。

美国交通部是推进智能交通物联网应用的主管部门。2015年2月，交通部的智能交通系统计划发布了2015—2019战略计划，详细介绍了车对车通信等研究项目。2015年9月，交通部为纽约市、怀俄明州和坦帕市提供共计4200万美元的资金，

用于车车互联技术测试，包括车对车和车对基础设施通信技术，以期提高公共安全并减少拥堵。2015年12月，美国交通部启动了智能城市挑战赛，从联邦智能城市计划中拨款4000万美元，并与私营公司合作，为获奖城市提供额外的2000万美元资金和各种物联网管理工具。2016年10月，交通部宣布提供5660万美元的额外拨款，资助8个城市的高级交通技术项目。

美国其他政府部门也发起多个研发示范项目，促进物联网应用推广。美国环保局（EPA）于2016年8月发起了智能城市空气挑战赛，向两个获奖社区授予最高5万美元的奖励，参赛社区需要部署数百个网络空气质量传感器，并制定收集、管理和共享空气质量数据的计划。美国国土安全部（DHS）2015年1月发起的“下一代第一响应者”计划，致力于开发保护应急响应者、减少响应时间和改进决策的互联技术。美国疾病控制和预防中心（CDC）于2015年10月启动了一个试点研究项目，利用包括物联网在内的新兴技术监测地下采矿环境以保护矿工健康。美国农业部国家食品和农业研究所（NIFA）开展教育和应用资助项目，推动农业部门与大学和研究机构合作，采用物联网和精准农业数据创新技术，以更好地收集和分析动物生产、森林生产和作物生产的数据。

此外，美国也十分重视物联网技术的基础研究工作。美国国家科学基金会（NSF）通过信息和智能系统计划、计算和通信基础计划等为与物联网相关的各种研究项目提供资金；还通过小企业创新研究/小企业技术转移计划（SBIR/STTR）为智能健康和生物医学、电子硬件、机器人和无线技术等物联网领域的技术开发项目提供种子基金。

#### （6）促进行业协作

美国政府各部门发起多项计划，推动政产学研用各机构形成产业联盟，开展公私合作，共同突破物联网应用领域的关键技术瓶颈，并形成集群效应。例如2015年11月，美国国家科学基金会推出了大数据区域创新中心计划，召集学术、产业、政府和民间利益相关者群体形成四家创新中心，致力于推进物联网与数据驱动的创新，包括精准农业、智能社区和自然灾害管理等，协调来自50个州的250个组织开展创新活动，以促进伙伴关系，合作应对

区域挑战。

美国于 2012 年发起的“国家制造业创新网络计划”（后更名为“制造业美国”），也是近年来公私合作推动产业联盟创新的典型案例。其中若干研究所重点关注物联网技术，如能源部牵头的智能制造创新研究所（Smart Manufacturing）和国防部牵头的高级功能性织物研究所（AFFOA）等。

## 2 美国发展物联网的未来政策框架

美国联邦政府采取了上述一系列政策措施，支持物联网发展。但这些举措基本都局限于个别政府部门，或基于单一应用领域，缺乏国家层面的整体战略性规划。2016 年初，美国国会提出了《发展物联网创新与增长》（DIGIT）法案，要求商务部成立一个工作组，召集政府、行业、消费者和民间利益团体，系统审查目前妨碍物联网发展的政策和做法，并改善联邦机构之间在物联网问题上的协调，使整个美国联邦政府更好地把握物联网所带来的机遇。目前，这一法案仍在国会讨论过程中，能否最终通过有待观察。

美国商务部下属的美国国家电信和信息管理局（NTIA）于 2017 年 1 月发布了一份题为《促进物联网发展》<sup>[4]</sup> 的绿皮书，全面介绍了物联网发展现状及其对于美国社会的重要意义，并提出了未来美国物联网政策的四点框架建议，供全社会讨论。

### （1）保障基础设施与公共资源

随着物联网应用的快速拓展，通信基础设施、频谱、互联网地址等资源将成为显著的制约因素，需要相应政策加以保障。思科公司预测，到 2018 年全球网络数据量将比 2013 年增长 22 倍，对光纤等网络基础设施提出巨大挑战，政府应与私营部门合作加快基础设施更新步伐。物联网应用将与 5G 技术协同发展。不同应用场景对于数据传输速度、数据延时及网络稳定性有不同的要求，需要的频谱资源也各有不同，政府应及早做好频谱分配规划，平衡许可频段与免许可频段的利用，并大力开发频谱共享技术以提高频谱利用效率。第 4 版互联网协议（IPv4）仅能实现 43 亿个互联网地址，远不能满足未来物联网的应用需求，需要向第 6 版互联网协议（IPv6）平滑过渡，但过渡过程中的软硬件兼容性、网络安全隐患等问题需要政府的顶层协调。

### （2）制定平衡性政策

物联网的发展将为社会带来深刻的变化，也会带来网络安全、隐私保护、知识产权等方面的一系列挑战，政府需要制定平衡性政策：一方面要防范新技术可能带来的风险，另一方面要鼓励创新，避免过度监管阻碍技术进步。

在网络安全领域，风险不断变化，管理措施应具有灵活性。美国标准与技术研究院的《改善关键基础设施网络安全的框架》文件提供了总体架构原则，又可适应每个部门的具体需求，受到各界好评。物联网产品应将安全因素纳入全生命周期管理，在设计初期即充分考虑安全因素，并采取措施在使用过程中不断进行安全更新。

在隐私领域，工业物联网与消费物联网应用对于隐私与数据收集的要求显然不同，应针对具体领域制定政策，避免一刀切，防止过于苛刻的隐私要求阻碍创新。美国联邦贸易委员会作为美国隐私监管的主要部门，应继续将目前的监管原则应用于物联网与大数据领域，打击隐性歧视，保护数据安全，促进透明的决策过程。

在知识产权领域，物联网的应用可能带来关于软件与数据的所有权、访问权与使用权的新问题。例如传感器网络采集的数据究竟属于谁，各方对于数据处理有何权利等。一般来说，事实性物理量（如温度）不享受版权保护，但声音、图像等数据很有可能涉及版权问题，需要知识产权局进一步厘清其中的法律问题。

### （3）推动技术标准进步

美国强调私营部门主导的标准制定方法。政府作为标准化过程的召集者和促进者，应确定技术标准的需求与基本原则，如美国标准与技术研究院在信息物理系统、智慧城市、网络安全等领域出台的一系列框架文件。物联网应用不同层面的普遍问题，如技术、连接性、互操作性、功能、安全性、可用性等，都应通过行业标准加以解决，促进技术推广。

由于物联网技术和应用的广泛性，由单一的标准开发组织来开发所有所需的标准是不现实的。美国国家标准协会认为，物联网的标准化应遵循多路径方法，即允许满足给定要求的多重解决方案在公平的市场环境中相互竞争，最终的标准在开放的过程中由市场决定。

美国政府表示将在联合国相关部门,如国际电信联盟标准化部门(ITU-T)和世界知识产权组织正在进行的物联网标准化活动中继续发挥作用,敦促标准化过程向所有利益攸关方开放,并鼓励国际伙伴在可行的范围内采用国际标准。

#### (4) 鼓励物联网市场发展

美国政府可以采取一系列措施,鼓励物联网市场的发展和增长,如通过政府采购等手段成为物联网设备的优先使用者,帮助解决物联网发展中产生的劳动力问题,通过指标测量更好地对物联网的发展进行规划等。作为新兴技术的优先使用者,政府部门可以降低企业投资新技术所面临的风险,同时通过积极部署物联网技术并挖掘数据的潜力,改善政府自身的运作模式与治理水平。预计到2025年,美国80%的制造企业将普及物联网技术,政府一方面需要大学和企业合作,加强物联网相关技术的教育体系建设,满足迅速增长的人才需求,另一方面要采取措施保障受到物联网影响的工人的权益,如避免数据滥用对工人的隐性歧视等。政府应建立指标体系,评估物联网在成本节约、生产率提高等方面的贡献,从而深入理解物联网在工业价值链中的作用,通过观察哪些部门正在迅速采用物联网,更好地制定物联网的发展规划。

### 3 启示与建议

随着物联网从碎片化、孤立化应用为主的起步阶段迈入跨界融合、集成创新的新阶段,物联网大规模爆发式增长的序幕已经开启。我国在物联网发展政策环境、技术研发、标准研制、产业培育和行业应用方面取得了显著成绩,物联网已成为推动经济社会智能化和可持续发展的重要力量。但从发展阶段来看,我国物联网仍处于应用层次偏低和向规模化探索的初期,技术成熟度不高,行业壁垒和信息孤岛依然存在,跨领域跨行业的互通共享与应用协同明显不足,阻碍了大规模应用。我国与美国的发展阶段不同,产业结构与政策框架区别很大,但美国各界针对物联网发展的思考对我国仍有一定的借鉴价值。

#### (1) 统筹制定跨领域的物联网国家战略

物联网涉及领域广,环节多,影响面超出任何单一行业或部门,需要政府加强统筹规划与顶层设

计,制定协调有序的物联网发展战略,并与国家发展的整体规划相融合。政府各部门在技术研发、标准制定、数据共享、基础设施建设、信息安全保障、频谱资源分配等环节要加强协同配合,发挥战略统筹优势。我国应在2013年发布的《物联网发展专项行动计划》基础上,继续加强顶层协调机制,跟踪世界物联网发展的最新态势,借鉴其他国家的有效经验,不断破除影响物联网发展的体制机制障碍,推动物联网产业快速发展。

#### (2) 推动物联网跨领域应用示范项目

政府在推广新技术应用的过程中,可有效补偿企业风险,加强资源统筹,发挥不可或缺的作用。目前的物联网应用多是在特定领域的闭环应用,层次低,成本高,规模化不足,为此,政府应致力于加强通用协议和标准的研究,组织产业联盟着力解决关键共性问题,推动物联网面向不同行业不同领域应用的互联互通、资源共享和应用协同,通过开环应用示范工程推动集成创新,总结形成一批综合集成应用解决方案。

#### (3) 加强面向物联网应用的前瞻性研究

目前,无人驾驶、车车互联等物联网智能应用正呈现加速发展态势,预计很快将投入市场应用。物联网在重塑生产生活方式、变革产业形态的同时,也为社会带来如安全、伦理、隐私等一系列深层次的挑战。我国应借鉴发达国家经验,及早对技术的社会影响进行前瞻性研究,通过广泛的咨询对话机制形成社会共识,及时调整政策框架,使政府治理模式跟上技术进步的速度。■

#### 参考文献:

- [1] Cisco. VNI forecast highlights tool[EB/OL]. [2017-05-31]. [http://www.cisco.com/c/m/en\\_us/solutions/service-provider/vni-forecast-highlights.html](http://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html).
- [2] McKinsey Global Institute. Unlocking the potential of the Internet of Things[EB/OL]. [2017-05-31]. <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>.
- [3] Cyber Physical Systems Public Working Group. Framework for cyber-physical systems[EB/OL]. [2017-05-31]. <https://s3.amazonaws.com/nist-sgcps/cpspwg/files/>

- pwgglobal/CPS\_PWG\_Framework\_for\_Cyber\_Physical\_Systems\_Release\_1\_0Final.pdf.
- [4] NIST. Framework and roadmap for smart grid interoperability standards, release 3.0[EB/OL]. [2017-05-31]. <https://www.nist.gov/sites/default/files/documents/smartgrid/Draft-NIST-SG-Framework-3.pdf>.
- [5] NIST. Big data interoperability framework: volume 4, security and privacy[EB/OL]. [2017-05-31]. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-4.pdf>.
- [6] NIST. NIST releases update to cybersecurity framework[EB/OL]. [2017-05-31]. <https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework>.
- [7] FTC. Building security in the Internet of Things[EB/OL]. [2017-05-31]. <https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf>.
- [8] Department of Homeland Security. Strategic principles for securing the Internet of Things[EB/OL]. [2017-05-31]. [https://www.dhs.gov/sites/default/files/publications/Strategic\\_Principles\\_for\\_Securing\\_the\\_Internet\\_of\\_Things-2016-1115-FINAL\\_v2-dg11.pdf](https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf).
- [9] NIST. Guidelines for smart grid cybersecurity[EB/OL]. [2017-05-31]. <http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>.
- [10] FCC. Applying Security to Consumer IoT Devices Subcommittee Technical Considerations White Paper[R/OL]. [2017-05-31]. <https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf>.
- [11] FDA. Postmarket management of cybersecurity in medical devices[EB/OL]. [2017-05-31]. <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>.
- [12] NHTSA. Cybersecurity best practices for modern vehicles [EB/OL]. [2017-05-31]. [http://www.nhtsa.gov/staticfiles/nvs/pdf/812333\\_CybersecurityForModernVehicles.pdf](http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf).
- [13] DOT. Federal automated vehicles policy[EB/OL]. [2017-05-31]. <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016>.
- [14] NTIA. Green Paper: Fostering the Advancement of the Internet of Things[R/OL]. [2017-05-31]. <https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things>.

## Policies Research for Promoting the Internet of Things in the U.S.

QIAO Jian

(Ministry of Science and Technology of China, Beijing 100862)

**Abstract:** This paper summarizes a series of policy measures adopted by the US federal government to promote the development of the Internet of Things (IoT), such as building a system of technical standards, strengthening cybersecurity, formulating innovation-friendly policies and regulations, protecting spectrum resources, supporting R&D and demonstration, and promoting industry collaboration. It also analyzes some US considerations of the future policy framework of the IoT, including aspects of infrastructure, policy balance, standards evolution and market development, in order to shed lights on the development of the IoT in China.

**Key words:** US; Internet of Things; information technology