浅析如何深化公安改革促进网络安全等级保护工作

蒙晓颖

（广西省桂林市龙胜各族自治县公安局　广西　桂林　541700）

[摘　要]互联网在给我们带来便利的同时，也带来了一些挑战。近年来，在世界范围内先后发生了多起针对工业、能源等关键信息基础设施行业的攻击，引发了多起危害国家安全的重大安全事故，严重损害国家安全。

[关键词]网络安全；等级保护；公安改革

【DOI】10.12252/j.issn.2096-6261.2021.03.101

网络安全等级保护制度是《中华人民共和国网络安全法》规定的基本制度，在维护我国网络空间安全方面发挥了关键作用。本文研究了当前国内外的网络安全形势和我国的网络安全等级保护工作，分析了网络安全等级保护工作中存在的问题，并通过深化公安改革结合公安工作实际，从管理安全、技术安全、法律困境、人才培养等方面为我国网络安全等级保护工作提几点建议。

一、等保2.0安全标准下网络安全等级保护工作中存在的问题

（一）安全管理滞后，管理规范化、服务化程度不高

目前的网络安全等级保护定级备案工作还处于人工提交、审核纸质材料的阶段，相对滞后于“互联网+政务服务”的发展。与此同时，在网络安全等级保护2.0安全标准的要求下，现有的管理制度和管理方法相对滞后。所谓的网络信息安全，不是一个口号，更不是某一项具体措施，而是要充分结合信息网络安全的需求，应用相应的管理办法，实现对网络信息安全的实时掌控。

（二）技术水平落后，基础信息化程度有限

我国网络安全等级保护工作自2006年才以制度的形式在全国范围内实施，由于发展较晚，我国的网络安全等级保护技术还尚不成熟，在物理环境、安全保障、定级测评机制、信息系统安全建设等方面与西方发达国家仍有差距，尚不能做到对网络中的各类风险实时监测，对各类网络信息系统进行动态保护。

（三）执法依据模糊，执法规范化能力不强

目前，各部门在实际的行政执法工作中还在一定程度上存在执法主体不明确、执法权限不明确、执法边界不清楚的问题，可能会导致各监管部门推诿扯皮或一个单位重复受到各监管部门处罚的现象，形成了相对较重的被监管压力，不利于互联网行业的发展。

二、通过深化公安改革促进网络安全等级保护工作几点思考

（一）加强网络安全等级保护工作的服务化和制度化建设

（1）简化定级流程，完善服务方式

改革服务方式，依托国务院《“互联网+政务服务”技术体系建设指南》和“放管服”工作，结合深化公安改革的创新网络社会治安治理机制和深化公安行政管理改革任务，建立完善全国统一的网络安全等级保护服务管理平台，优化网络安全等级保护备案流程，让备案单位少跑腿，甚至不跑腿，提高备案效率。

（2）缩小地区差异，完善管理制度

国家加大对网络安全信息技术欠发达地区的资金支持和设备投入，积极通过政策向这些地区引入专门的技术型人才，并通过各个省份间的一对一帮扶缩小地区间技术差异，统筹网络安全信息保护资源，改善网络安全技术落后地区或部门的工作窘境，切实做到网络安全等级保护工作在全国范围内统筹进行，全面铺开。

（3）强化人员管理，落实安全要求

重视人员录用工作，筛选具有一定工作能力，政治素养，实战水平的工作人员，在人员配置上保证网络等级保护工作的有效开展。与此同时建立健全工作人员脱岗保密教育制度，强化工作人员日常的安全意识教育和培训，完善外部人员访问管理制度。优化人员管理模式，强化网络安全等级保护2.0安全标准的要求下的人员管理。

（二）加强网络安全监督管理领域的环境规范化和技术信息化建设

（1）重视物理环境，强化监督管理

公安机关和其他网络监管部门和各评测机构依据服务器机房物理环境的安全的实际要求，并结合我国现行的法规政策明确物理环境的安全标准，包括机房场地位置的要求；物理访问控制的要求；防盗窃防破坏的要求；防火、防水、防静电、防电磁干扰的要求以及电力供应的要求等。与此同时，公安机关可以将网络安全等级保护工作中的服务器机房物理环境的安全检查纳为日常警务工作的一部分，同日常的消防检查一样，制定完善的检查方法、检查周期、检查标准，采用抽查、定期检查等方式对各服务器机房的物理环境进行监管，找出存在的问题，并可以通过下发类似整改通知单的方式指出服务器机房的问题所在，降低网络安全等级保护工作中物理环境安全风险。

（2）通过技术革新，完善安全保障体系

公安机关和工信部等网络管理部门要根据现有的网络安全应对举措和潜在的网络安全运行风险认真分析研判，真抓实干做好创新工作。一是防护技术、防护手段的创新，相关部门加大对信息技术，信息人员的资金投入，通过自主研发、资金引进的方式革新现有的网络安全防护技术，同时与科研院校、技术企业开展深入的合作，不断学习新的网络信息技术，引进新的网络信息防护资源。二是工作方式方法的创新，工作方式要从传统的安全检查逐渐转变为实网攻击演习，锻炼公安机关等网络监管部门的应急处突能力，同时能够提前发现问题，提出解决方案。三是安全防御体系的创新，首先是让网络信息安全系统具备“免疫能力”，即网络系统在被攻破以后，也能正常的执行工作。其次，让网络安全防御工作具备“适用能力”，即网络安全系统匹配其安全等级的需要及业务的应用。再次，让网络安全防御体系具备“成长能力”，即要从各种网络攻击和网络安全事故中吸取教训、总结经验，各地方、各网络安全机构、部门也要交流合作，互通互联，不断提高应对风险的能力。

三、结语

网络安全等级保护制度是我国关于网络安全的基本政策，也是网络时代医疗、教育、金融、电子政务等领域能安全发展的重要保障。通过网络安全等级保护工作，能有效发现各个行业信息系统与国家安全标准之间存在的差距，找出当前系统存在的安全隐患和系统漏洞，通过比对具体要求，完成各行业系统的安全整改，提高信息系统的安全等级和抗风险能力，合理的规避和降低网络运行风险

参考文献

[1]沈昌祥.创新和发展我国信息安全等级保护制度[J].网络安全技术与应用，2020（4）：2-4.