doi:10.3969/j.issn.1000-1247.2016.09.015

信息安全技术管理体系建设探讨

钱　康
中国信息通信研究院安全研究所

面对新时期互联网管理面临的新挑战，应加强信息安全技术管理体系建设，充分发挥技术手段在互联网信息安全综合管理中的作用。

1 高度重视技术能力在信息安全管理中的重要作用

当前，互联网发展迅猛，新技术新业务层出不穷，“互联网+”不断推进，以云计算、大数据为代表的新一代信息通信技术不断向经济社会各领域渗透融合。同时，信息技术的广泛应用，加速了网络安全事件的跨界蔓延，导致安全事件数量大幅增加，网络与信息安全威胁持续升级扩散，微博、微信等社交媒体快速普及使得信息监测与处置难度增大，云计算、大数据、CDN等技术的广泛应用使得信息定位与追踪溯源艰难，暴露出传统属地化监管的局限性，信息安全监管形势异常严峻。

网络安全威胁和网络结构发展变化，对网络安全防护思路和技术手段提出了新的挑战，促使安全防御技术向智能化演进，云与大数据技术成为关键。依托云平台，可实现恶意样本的广泛采集、高速分析和实时全网部署，以提升未知威胁的防御能力，增强防御效率；借助大数据分析能力，可实现自动化威胁识别、阻断和追溯，降低传统防御工具的误报率，提升网络防御性能。因此，必须切实加强信息安全技术能力建设，按照以技促管、技管结合的原则，建立与信息安全管理相适应的信息安全技术管理体系，这是维护国家网络与信息安全的根本之策和重要基础。

2 应建立“部-省-企业”三级技术管理架构

目前，我国信息安全管理包括部、省、企业三个层次，工业和信息化部、省通信管理局和企业是信息安全管理的主体，多年来形成了比较完整的管理体系，发挥了重要的作用。但是这个体系还不完善，一个重要方面就是缺乏与之相适应的高效技术管理架构，导致信息安全基础管理薄弱、境内违法信息监测与处置难、跨省联动协办效率低、态势信息滞后等问题的出现。因此，应着力建立起部、省、企业三级技术管理架构。在这一架构中，应以企业侧系统为基础，由各个互联网接入服务企业（含基础、增值）按照行业标准建设，主要负责基础数据采集与上报、信息安全监测与处置任务的执行；以省通信管理局侧系统为中枢，由各省通信管理局建设，主要负责全国数据归集校验、本地信息安全任务管理与部级指令中转；以部级系统为首脑，主要实现全国信息安全任务指令调度与分发、国内互联网业务及资源安全监管。

通过三级架构，可以有效形成覆盖全国的信息安全技术监管能力，从而覆盖31省通信管理局、三大基础电信企业及增值企业，能够实现全国互联网违法信息实时监测、智能预警、准确定位、联动管理，进而全面提升全国互联网行业管理能力、互联网信息安全保障能力。

3 形成信息安全大数据挖掘分析能力

当前，大数据资源价值凸显，数据安全威胁升级蔓延，以数据资源为目标的安全威胁行为不断增多，网络数据已成为信息安全管理着力保护的重要资产。然而，数据保护与之不相适应，还面临着数据跨境流动、开放共享等焦点问题规则不明确，数据安全事件的防范、取证、溯源、追责困难等问题。同时，管理部门也缺乏对全国互联网基础资源、违法信息、违法违规网站、信息安全检测处置等各方面的全国信息安全基础数据，从而无法全面、准确掌握我国信息安全现状，也无法及时预警我国信息安全态势，更缺乏对全国信息安全数据的公开发布。

为此，应针对监管空白和缺失，在加快数据安全保护立法、加强数据安全监管的同时，构建全面的数据安全保护体系，包括健全和完善相关的安全技术体系、安全标准和评估体系等，形成信息安全大数据管理能力。应通过加强信息安全综合管理技术手段，接收企业上报数据、其他行业管理系

（下转66页）