

对二十一世纪我国信息安全领域发展的几点看法

卿斯汉^{*}

(中国科学院信息安全技术工程研究中心 北京 100080)

关键词 信息安全, 建议

在计算机和网络深入千家万户的信息时代, 信息安全已经成为全球性问题。没有信息安全, 就没有真正的政治、军事和经济安全。西方发达国家十分重视信息安全, 美国多年来一直将信息安全技术列为国防重点项目, 并已形成庞大的信息安全产业, 作为其实现信息霸权的有效手段。欧洲、日本、加拿大、澳大利亚和以色列等国也在信息安全领域投入巨资, 拥有相当规模的信息安全产业。

目前, 我国对信息安全领域日益重视, 并已初步形成一支信息安全方面的技术队伍。但是, 我国在该领域的总体水平与国外相比还有较大差距。其主要原因是:

起步晚, 基础薄弱, 目前尚无广泛应用的自主版权安全技术平台, 一些重要的安全基础设施也有较大差距。

④投入不足。美国的网络安全投资一般约占网络总投资的 10%—20%, 而我国还不足 5%。

④技术成果转化缓慢, 信息安全产业尚处于起步阶段。

现就如何加快我国信息安全领域的发展谈几点看法。

(1) 发展我国自主的关键技术。信息安全领域的基础技术, 如操作系统、应用软件、芯片等大部分依赖进口。在这种状况下, 引进国外先进技术仍然是十分必要的。但在信息安全领域, 必须要追赶 21 世纪世界先进水平, 必须发展我国自主的关键技术, 将关键性的安全技术掌握在自己手中。另一方面, 信息安全是一项系统工程, 既包括攻、防两方面的含义, 又包含防护、检测、反应和恢复等信息安全保障内容。我们需要有效地防范可能发生的信息攻击, 同时, 也要为可能出现的信息冲突准备反击手段, 在信息战的环境下具有“生存能力”。“十五”期间, 我国信息安全领域的投资会有大幅度提高, 但我们仍必须有重点地发展。首先应着眼于创新性强、具有重大杠杆作用的突破性技术, 并将这种技术有效地应用到我国的信息安全基础设施之中。其次要大力开发具有共性和普遍性的关键技术, 逐步改进我国信息基础设施的安全保障能力和生存能力。

^{*} 中国科学院信息安全技术工程中心主任, 研究员
收稿日期: 2000 年 12 月 14 日

(2) 制订目标和计划。“十五”期间,发展信息安全核心技术和产品,使我国信息安全产业初步形成规模。实现国家标准《GB17859-1999—计算机信息系统安全保护等级划分准则》规定的第三级(安全标记级)技术要求,形成系列信息安全产品。同时进行第四级(结构化保护级)和第五级(访问验证保护级)产品的前期研究,尽快研发出相关技术和产品。

优先发展的关键技术和产品有以下三类:

基础类,包括密码、关键元器件、安全处理器、安全操作系统、安全数据库、网络安全平台等。

④核心类,包括认证与抗抵赖、防火墙技术、安全 Web 服务器、网络安全检测与评估、网络攻防、电磁辐射和干扰检测与防护等。

④应用类,包括涉密网络基础安全平台、安全电子商务及互联网基础平台、病毒防治、备份与灾难恢复、安全管理等。

(3) 要加强支持信息安全领域发展的宏观决策。

要统一指挥,步调一致。面对 21 世纪信息安全发展的机遇和挑战,当务之急是加强我国对信息安全领域的宏观管理。对国家信息安全重大基础设施进行宏观决策,发布国家信息安全政策,批准国家信息安全规划,对国家面临的重大信息安全紧急事件做出决断等。进一步协调各主管部门的工作,统一步调、统筹规划,加快我国信息安全领域发展的步伐。

④要大幅度增加信息安全领域的人、财、物力的投入。应在“十五”期间大幅度增加投入,应将宝贵的有限经费用于支持在信息安全领域已有基础、并已做出显著成绩的单位,避免重复建设和低水平的重复开发。

④要积极支持技术创新。技术创新是信息安全产业发展的灵魂。国家的任何宏观决策都必须有利于信息安全技术的进步。信息安全管理的主管部门应研究信息安全关键技术的发展趋势,制订国家信息安全规划,制订国家信息安全基础设施规划,审批重大信息化工程的信息安全技术路线和措施,组织制订信息安全的标准和规范,组织制订信息安全产品的评测标准和规范,制订鼓励信息安全产业发展的政策,制订处理信息安全突发事件的应急对策等。

要加强信息安全在立法、标准和教育等方面的工作。我国要在 21 世纪成为信息安全的强国,就必须加强信息安全的立法、标准和管理等方面的建设,增强全民族的信息安全意识。

除信息安全产业的正规军,即研究信息安全的传统队伍和新兴力量之外,应当主动引导和积极组织社会的研究力量。目前,“信息安全学”已成为一门新兴学科,许多大学和科研院所都开设了本科、硕士和博士课程。今后应进一步加强信息安全的培训工作,对领导干部、系统管理人员、企业主管和部门经理等,分别进行针对性的培训。只有全民信息安全素质提高了,我国在信息安全领域才会真正立足于世界先进之林。