我国公安部门信息安全保障技术体系建设探讨

Study on Technology System of China's Information Security

周国勇/ZHOU Guo-yong，欧阳满/OUYANG Man

公安部信息通信局，北京 100741

Bureau of Information Communication, Ministry of Public Security of P R China, Beijing 100741, China

[摘要] 信息、信息技术已经成为国家实力和国家安全的重要决定因素。结合我国信息安全发展的现状和存在的问题，提出了我国公安信息安全技术体系建设的目标、建设思路，以及信息安全技术体系的建设核心内容和关键技术，并对我国公安部门开展信息安全技术体系建设的保障措施提出了建议。

[关键词] 信息安全，技术体系 [中图分类号] TP393.08

[文献标识码] A [文章编号] 1000-7857(2005)09-0034-03

Abstract: Information and information technology have been the key factors for national strength security. Based on the present state and problems of China information security development, the object and methods of its technology system were proposed, and its main contents, key technology and assurance measures were also described.

Key Words: information security, technology system **CLC Number**: TP393.08

Document Code: A **Article ID**: 1000-7857(2005)09-0034-03

1 引言

当今社会，一个国家与民族的政治地位及其对国际事务的影响力，将越来越取决于：① 国家信息基础设施的发展水平，以及由此而形成的信息利用能力；② 国家的精神、思想价值观、文化和语言的传播及渗透能力；③ 对敌对精神文化、道德观点的阻止、改变和破坏能力。发达国家，特别是美国，把国家信息基础设施的建立当作是21世纪保持经济增长和确保世界领先地位的主要任务[1,2]。各国在经济、科技、社会文化(文明)，尤其是在军事各领域的政治争夺，越来越集中在信息优势的夺取上，而信息优势的夺取却直接地表现为网络信息保障与对抗[3]。

国家综合实力是由信息基础设施发展水平所决定的，信息已成为国家的一种重要战略资源和主要财富，对信息资源的争夺及信息流的控制是国家未来扩大与巩固政权的重要手段。因此，信息技术也是捍卫其国家利益和安全的有效手段，保障信息安全成为国家政治生活的重要任务之一[4,5]。

当前，我国信息化面临的问题是，大规模使用的硬件和软件几乎全部依靠进口，这使我国信息领域处于十分危险的状况。消除国家在信息领域的安全脆弱性，建立我国信息保障体系，是一项直接关系到国家生死存亡的重要任务，需要长期不懈的努力[6]。信息保障体系的建设是一项涉及网络的管理控制、运行控制和技术控制的系统工程。我国公安部门信息保障技术体系及其技术发展应该基于我国信息安全的现状，围绕网络信息空间"可知、可控、可管"体系的建立来开展。

2 我国信息安全存在的问题

2.1 我国信息安全技术的发展存在先天的不足

我国信息基础设施几乎全部是建立在国外的核心技术之上。计算机硬件、通信设备制造业的基础集成电路芯片主要依靠进口，甚至系统软件、支撑软件基本上也是国外产品。网络、硬件和软件方面自主技术的长期缺乏，导致了我国目前在互联网的核心控制水平上缺乏起码的自卫能力，形成了我国信息安全技术发展的先天不足局面。

2.2 我国信息安全体系建设尚处于不完善状态

我国网络信息安全技术研究起步相对较晚，但作为一门新兴学科和新兴技术研究领域，该研究近年来已引起了我国政府和学术界的极大关注。国内计算机网络信息安全技术的研究，现阶段多以网络防御技术为研究核心开展，与发达国家相比，在网络攻击技术、网络防御技术、网络攻防测试与评估技术上均有相当大的差距，在网络信息安全防御体系、大规模网络攻击、预警与防御、测试与评估、无线网络攻防等总体技术上差距则更大。

2.3 信息安全关键技术发展水平与国外存在明显的差距

根据网络信息安全概念的形成和发展，网络信息安全技术的发展可归纳为3个发展阶段：信息保密阶段、信息安全阶段和信息保障阶段。这3个发展阶段的技术特点如表1所示。

从网络信息安全技术发展阶段来看，目前我国网络信息安全的技术发展水平还基本上处于"信息安全阶段"，有关"信息保障阶段"的网络信息安全技术刚刚开始积累。我国的网络信息安全技术发展水平与美国尚存在着很大的差距[7]。

2.4 信息安全产业体系尚未完整建立，产业对技术发展的推动力尚未形成

产业是推动技术发展的动力，但我国信息安全产业刚刚起步，产业规模及产品的技术水平尚处于初级阶段，促进产业发展的良性循环体系尚没有建立起来，更谈不上形成对技术发展的推动。

收稿日期：2005-06-07

作者简介：周国勇，男，北京市东长安街14号公安部信息通信局，博士，主要从事信息网络安全研究；E-mail: zhgy889@sohu.com

表 1　网络信息安全技术各发展阶段的技术特点

发展阶段	信息保密阶段	信息安全阶段	信息保障阶段
技术特点	加密	完整性 保密性 可用性	防护 检测 响应与恢复

2.5 国际安全形势对我国信息安全提出了新的严峻挑战

进入 21 世纪,尤其"9.11"事件以后,国际政治非线性相互作用越来越复杂,世界多处局部动荡与紧张局势明显加剧,恐怖主义成为当前国际安全形势的主要挑战。信息恐怖直接威胁个人心理以及社会(或团队)意识,是当前恐怖威胁的主要表现形式。在我国,信息恐怖主义的主要表现形式为:① 网上危害国家安全的案件十分突出,敌对势力、民族分裂主义势力、法轮功邪教组织等利用互联网进行宣传煽动、组织串联、策划暴力和恐怖活动,对我国国家安全构成了严重威胁; ② 危害计算机信息网络安全的案件呈现连续上升趋势;③ 利用互联网进行经济和金融犯罪、诈骗、盗窃、敲诈勒索犯罪的情况明显增多,危害严重;④ 在互联网上妨碍社会公共管理秩序的案件大量发生。

当前,信息恐怖的种类多样化、手段高科技化的趋势明显,跨地区犯罪以及利用网络进行宣传煽动的违法犯罪情况十分突出。信息恐怖主义对我国信息安全提出了严峻的挑战。

3 我国公安部门信息安全技术体系建设的目标与思路

3.1 建设目标

坚持积极防御、综合防范的方针,以保障公安网络信息基础设施和重要应用系统安全,创建安全健康的网络环境,保障和促进公安信息化发展,维护国家安全、社会稳定和公众合法权益为目标,全面提高公安部门信息安全防范、控制、保护、应急处置和侦察打击水平。

3.2 建设思路

3.2.1 基于信息保障的观点,构筑公安信息安全体系

信息保障就是基于纵深防御的思想构筑信息安全体系,纵深防御就是采用一个层次化的、多样性的安全措施来保障用户信息及信息系统的安全。信息保障的概念已经不局限于信息的保护,而是着眼于对整个信息和信息系统的保护与防御,以确保其安全性(包括对信息的保护、检测、反应和恢复能力)。

3.2.2 围绕信息风险管理,开展公安信息安全技术研究

风险管理是自然循环的,包括理解任务目标、理解信息保护需求、描述风险特征、描述可以做什么、决定将做什么和执行决策等过程,包含风险信息获取、风险识别与评估、风险控制的关键技术。安全的目标就是要降低风险,因此,风险的评估、管理与控制是公安信息安全研究的关键。

3.2.3 以安全监控为核心,建立公安信息安全动态保护系统

信息安全技术体系的功能要求是:制止消极信息作用;防止信息资源被中断、入侵和攻击;向主体提供有关战略性威胁的"指示与报警","检测"信息资源被破坏、入侵和攻击的程度;建立恢复信息资源安全的服务;对消极信息作用的信息防御反应。信息安全监控是能及时获取计算机网络和信息系统的运行状况、潜在的安全漏洞,实时发现风险与攻击状态并予以告警的重要手段。因此,安全监控是信息安全技术体系的重要组成部分,是信息网络系统安全的基础,是突出重点、制定合理安全防护策略的前提。

3.2.4 建立安全信息共享中心,提供信息安全积极防御能力

建立互联网安全信息共享中心,实现对网络安全信息(即网络安全漏洞、网络攻击信息、网络传播的有害信息、有害网站及网上违法犯罪活动等信息)的共享,进而实现对监控信息的搜索、分类、挖掘等技术的研究,建立适合我国国情、与国际接轨的安全信息共享技术体系和标准体系,从而提高对网络信息系统安全信息的综合分析与应用能力。

4 我国公安部门信息保障技术体系的建设内容和关键技术

4.1 建设内容

完善的技术体系是我国公安部门信息保障体系建设的基础。我国公安部门信息保障技术体系应该建立 6 种安全机制, 即阻止、防护、报警、监测、恢复和响应,并实现如下功能:① 阻止消极信息作用;② 防止信息资源被中断、入侵和攻击;③ 向主体提供有关战略性威胁的报警;④ 检测信息资源被破坏、入侵和攻击的程度;⑤ 建立恢复信息资源安全的服务;⑥ 对消极信息作出信息防御反应。

信息保障所面对的是一复杂系统环境,我国公安部门信息保障技术体系应该基于如图 1 所示的建设内容,建设成为包括信息安全防护体系、信息安全监控体系、信息安全管理体系和安全事件应急响应体系等 4 大信息安全体系的积木体系,并建立 4 大技术体系之间的信息反馈。

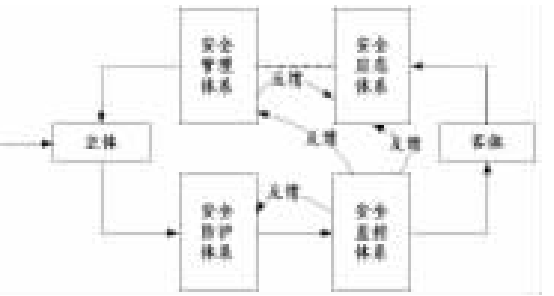

图 1　信息安全技术体系的逻辑关系

4.2 关键技术

公安信息保障技术应该围绕如图 2 所示技术能力的形成发展,并主要解决如下两方面的问题:① 国内自主成熟网络信息安全技术应用;② 公安特色网络信息安全核心技术研究。

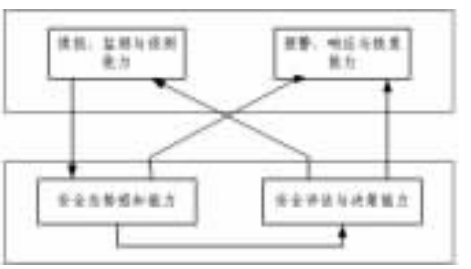

图 2　信息安全技术能力的逻辑关系

因此,我国公安信息保障技术发展,应该围绕网络信息空间"可知、可控、可管"能力的建立,开展如下关键技术研究。① 信息网络安全信息共享技术:重点解决信息网络安全信息共享体系的建立,信息网络安全信息共享规范与技术标准的制定,信息网络安全共享信息的综合分析与数据挖掘,信息网络安全的风险评估与风险管理等技术问题;② 信息网络安全监测与侦察技术研究;③ 信息网络安全检测与识别技术研究: 重点解决网络环境下违法犯罪行为的数据截取、发现和定位,互联网信息监控,网络安全信息的数据关联与融合等技术问题; ④ 信息网络安全态势评估技术研究:重点解决网络安全状态的检测与评估,网络攻击的态势评估与毁损评估,网络攻击的毁损设备定位与识别,网络攻击者的识别、定位与跟踪等技术问题;⑤ 信息网络安全应急响应与恢复技术研究:重点解决网络安全报警处置,网络欺骗与取证,网络的攻击反制等技术问题; ⑥ 信息网络安全信息综合管理与控制技术研究:重点解决网络安全设备的综合管理与监控,网络安全监控系统的自身防护,网络安全状态的可视化等技术问题。

集团企业 ERP 系统维护模式研究

Research on Maintenance Modes of Group Organizations' ERP System

高玉飞/GAO Yu-fei,王有为/WNAG You-wei, 刘 杰/LIU Jie

复旦大学管理学院, 上海 200433

School of Management, Fudan University, Shanghai 200433, China

[摘要] 系统开发和实施技术不断地发展成熟, 与此相比, 系统维护问题显得突出。特别是集团企业的 "企业资源规划"(Enterprise Resource Planning, ERP)系统复杂,维护问题就更加突出。至今,人们对一般企业信息系统维护的研究还只局限于相关模型、具有某种特性的信息系统(实时系统、网络系统等)的维护问题,以及与维护效率相关因素(维护人员的经验,系统的复杂性等)的研究,较少有人对 ERP 系统维护问题进行专门研究,更少对集团企业的 ERP 系统维护模式给予足够重视。对此,在对两个大型集团企业调研的基础上,总结集团企业的特点,分析与其 ERP 维护相关的因素,进而得出比较适合集团企业 ERP 的维护模式:自己维护为主、多种维护模式相结合的集中式维护。

[关键词] 系统维护, ERP, 集团企业, 集中式维护 [中图分类号] C931.6, F270.7
[文献标识码] A [文章编号] 1000-7857(2005)09-0036-04

Abstract: The system maintenance becomes more and more notable with the development of system developing and implementing technologies. Particularly, the maintenance problems of the group organization's ERP (Enterprise Resource Planning) system are more distinctive because of its complexity. Up to now, researches have been limited to relational models, maintenance problems of specific systems such as real-time systems or web-based systems, and factors related to the efficiency of maintenance activities such as maintenance men's experiences or the systems' complexity. While few concentrate on ERP systems and even few take care of the maintenance problems of group organizations' ERP system. Through investigating two large group organizations, this paper concludes the characteristics of group organizations and analyzes its factors related to maintenance efficiencies. Further more, it summarizes a relatively suitable maintenance mode for group organizations' ERP systems: the centralized maintenance with self-maintenance and multi-maintenance.

收稿日期: 2005-03-14
基金项目: 国家自然科学基金(70401010)资助
作者简介: 高玉飞,男,上海邯郸路 220 号复旦大学管理学院,博士生,研究方向为信息系统维护;E-mail: mygyf@yahoo.com.cn

5 我国公安信息安全技术体系建设的重要保障措施

5.1 加强信息安全理论的基础研究

必须加强信息安全理论的基础研究,建立以信息安全防护为目的,以信息安全学为核心,以信息技术学、信息工程学、信息管理学、信息社会学、信息经济学为支持,与国家和社会各领域的学科群相融合的信息安全理论体系。加强信息安全关键技术和相关核心技术以及信息技术产品的安全可控技术和信息化新技术的相关安全性的研究。

5.2 加快信息安全法制建设

加快信息安全法制建设,首先要加快制定和修订与信息安全相关的法律法规工作,其次要加快信息安全执法队伍的建设,做到有法可依, 严厉打击危害公众利益和国家安全的网络违法犯罪活动。

5.3 推进公安信息安全标准体系的建设

结合我国信息安全发展现状和国际发展趋势,在抓紧制定我国信息安全技术与管理标准的同时, 还应注重信息安全标准的推广应用工作, 充分发挥标准在信息安全保障体系建设中的基础性和规范性作用。

5.4 促进信息安全产业的快速发展壮大

要加快提高我国信息安全产业关键技术的研发能力和自主创新能力,迅速掌握信息和信息安全关键领域的核心技术;加快培养具有高度国家责任感和历史使命感的信息安全产业高素质技术人才,加快提高信息安全产业服务的水平和质量。

6 结论

构建行业信息安全保障体系是最近几年信息安全领域研究的热点问题之一。本文从国家安全角度出发,分析了我国信息安全发展的现状和存在的问题,具体探讨了我国公安部门信息安全保障技术体系建设的相关问题。"可知、可控、可管",是我国公安部门信息安全保障体系建设应有的目标,也对其它行业部门信息安全保障体系建设具有参考意义。

参考文献(References)

[1] 黄鹏, 等. 美国网络空间安全国家战略[R] .信息产业部电子科技情报所,2003
[2] 维恩·斯瓦图. 信息战争[M]. 北京:国际文化出版公司,2001
[3] David S Alberts,John J Garstka,Frederick P Stein. Network centric warfare: developing and leveraging information superiority [M]. CCPP Publication,1999
[4] 王智远等主编. 联合信息作战[M]. 北京:军事友谊出版社,1999
[5] A·X·沙瓦耶夫著. 国家安全新论[M]. 北京:军事友谊出版社,2002
[6] 王越. 以科学的态度正确认识信息安全问题 [J]. 网络安全技术及应用,2003,36(12)
[7] 胡昌振. 把握我国信息安全技术跨越式发展机遇 [J]. 计算机安全,2003,31(9)

(责任编辑 苏 青)