信息化进程的研究

吴志军[1] 杨义先[2]
(中国民航大学电子信息工程学院 天津 300300)[1]
(北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 100876)[2]

摘 要 针对信息化发展中各个阶段的显著特点,将其划分为信息化建设、信息安全保障和信息安全评价指标体系3个重要过程;并针对每个过程进行了研究,说明了3个阶段之间的关联关系;提出了适应于中国国情的信息安全保障IA(Information Assurance)的"运筹"(Operational)机制;研究了以"安全基线政策"(Security Baseline Policy)为核心的信息安全评价指标体系(Indicator)。最后,总结了每个信息化过程的发展特征,分析了今后的发展方向。

关键词 信息化,进程,信息安全保障,信息安全保障评价指标体系,安全基线政策
中图法分类号 TP310 **文献标识码** A

Research of Informationization Processing

WU Zhi-jun[1] YANG Yi-xian[2]
(School of Electronics & Information Engineering, Civil Aviation University of China, Tianjin 300300, China)[1]
(Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)[2]

Abstract This paper divided informationalization processing into three phases, informationalization construction, information assurance, and indicator. The relationships among the three phases were discussed. The characteristic in each phases was analyzed. The operational protect mechanism for China information assurance based on security baseline policy was presented. The indicator for information assurance was proposed.

Keywords Informationalization, Process, Information assurance, Indicator, Security baseline policy

1 前言

信息化的发展是人类社会文明进步的标志之一,信息化程度是衡量一个国家综合国力的重要指标之一。随着信息化的发展,各种信息技术蜂拥而至,大大加快了国际上信息化的进程。严格来说,信息化没有一个确切的定义,根据新公布的2006—2020国家信息化发展战略,对信息化的解释是充分利用信息技术,开发利用信息资源,促进信息交流和知识共享,提高经济增长质量,推动经济社会发展转型的历史进程[1]。

由信息化发展而形成的促进力是迄今为止人类社会最先进的生产力,它要求要有先进的生产关系和上层建筑与之相适应,一切不适应该生产力的生产关系和上层建筑将随之改变。它彻底改变了社会和人们的生产方式、工作方式、学习方式、交往方式、生活方式、思维方式等,并将使人类社会发生极其深刻的变化[2]。

信息化是一个内涵深刻外延广泛的概念。信息化的内涵主要体现在"信息通信",是指信息技术的自身发展,主要包括:(1)信息内容的极大丰富和信息形式的多样性;(2)信息科学技术的研究与开发,促进信息传输技术的飞速发展,即信息技术产业的高速发展及信息咨询服务业的高度发达和完善。信息化的外延主要体现在"信息价值",是指信息技术的广泛应用,主要包括:(1)信息化应用平台,包括信息资源、各种信息系统、公用通信网络平台等,例如金融、电信、证券、保险、民航、铁路、税收和海关8个国家重点信息系统,以及电信网络、广电网络和互联网络3个国家重要基础网络;(2)信息化运行环境,包括现代工农业、管理体制、政策法律、规章制度、文化教育、道德观念等生产关系与上层建筑;(3)信息化发展,包括劳动者素质、国家现代化水平、人民生活质量不断提高、精神文明和物质文明建设不断进步等[3]。

本文将信息化发展历程分为3个重要的历史阶段,并针对每个阶段的发展和特点进行了研究,明确了信息化发展中每个阶段的目标,以利于信息化的健康发展。

2 信息化进程

信息化发展是在一定的战略指导下,先建设信息基础,再搭建信息平台,然后通盘考虑信息安全的原则上进行的。它是一个4要素组成的多元实体,如图1所示。

到稿日期:2009-05-19 返修日期:2009-07-27 本文受国家973项目(No. 2007CB311203),国家863计划(No. 2009AA012439),国家自然科学基金委员会与中国民用航空总局联合资助项目(No. 60776808)和天津市应用基础及前沿技术研究计划项目(No. 09JCYBJC00400)资助。
吴志军(1965—),男,博士,教授,主要研究方向为通信网络和信息安全,E-mail:zhijun-wu@163.com;杨义先(1961—),男,博士,教授,主要研究方向为信息安全。

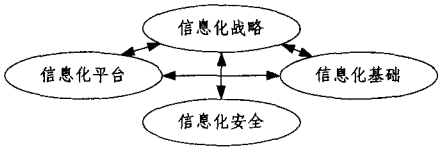

图 1　信息化发展的 4 个要素

信息化战略是指国家(宏观)、行业(中观)和企事业(微观)针对信息化进程制定的国家政策、发展规划和法律依据等;信息化基础是支撑信息化发展的基本理论、技术和设施;信息化平台是指信息化应用系统,例如国家 8 大行业(金融、电信、证券、保险、民航、铁路、税收和海关)信息系统和国家 3 大基础网络(电信网络、广电网络和互联网络);信息化安全则是在大力发展信息化的基础上,保证信息的保密性、完整性和可用性等。

随着信息化建设的发展,信息系统的组成和功能越来越复杂,系统也越来越庞大。从 20 世纪 90 年代末起,随着计算机病毒和攻击的出现,信息化面临巨大的挑战。因此,信息安全保障应运而生。21 世纪初,随着信息安全保障的大力发展,以及信息化进程的顺利进行,世界各国对重要信息系统的信息安全越来越重视。为了保障信息化系统的长效和安全,开始了信息安全保障评价指标的研究。

由于物质基础和社会环境不同,信息化起点不同,世界各国的信息化内容也不尽相同,因而它们各自的信息化过程必然要表现出一定的特殊性。每个过程又经历几个明显的阶段,具有鲜明的特点。通观信息化发展的进程,它具有 3 个明显的阶段:信息系统建设、信息安全保障 IA(Information Assurance)系统和评价指标体系(Indicator)。本文就信息化的这 3 个发展进程进行研究,总结了每个过程的发展特征,并给出了今后的发展思路。

2.1　信息化建设

与国际上信息化发达的国家相比,中国的信息化建设起点较低,表现在以单位、企业和个人购买计算机方面。而国际上,以美国和日本为首的发达国家,其信息化建设是以通信和网络为基础的。中国信息化进程大约在 20 世纪 80 年代起步,90 年代开始进入快速发展阶段,90 年代下半期进入高速发展时期[7],其整体特点是快速发展。

经历了近 30 年的信息化发展过程,中国信息化建设的发展历程可以划分为 3 个明显的阶段。

(1)信息化的定义阶段

在中国信息化建设的早期,由于对信息化这个新鲜事物没有实际的接触,中国学者在表述信息化概念时,比较普遍地将侧重点放在信息技术和经济活动方面,很少有人对它进行完整的描述[4]。

虽然对信息化的定义及其内涵和外延的内容不能确切和统一,但该定义阶段中的探讨和争论已经为信息化在中国的发展画出了一个比较清晰的轮廓。中国的信息化发展也正是在这种概念模糊、物质缺乏的窘境中开始摸索前进的。

(2)以计算机为代表的信息化建设

"信息浪潮"在中国开始掀起的时候,计算机作为人们可以直接接触到的信息化产品,成为人们追崇的对象。可以说在一定时间内,计算机成为信息化的标志。

由于网络和通信技术的落后,该阶段的计算机没有与其他计算机进行联网和通信,不能达到信息和资源共享的功能,基本上属于"单兵"作战。因此,该阶段信息化的主要特点是计算机的使用率不高,没有做到物尽其用。大多数计算机只是用于简单的文字处理、财务统计或者游戏等较低层次的信息处理工作。即使在信息化程度较高的一些信息服务部门,长期以来,除少数机构外,其信息系统、数据库等也处在技术水平低、规模小、资源少的状况下,而且大多是自成体系、以内部服务为主的封闭系统,没有向社会开放[3]。

(3)以网络为代表的信息化建设

以网络为代表的信息化建设阶段分为早期和现在两个时期。

1)早期

互联网刚在中国发展的前期,由于绝大多数政府部门和企事业单位对这种新鲜事物抱着观望的谨慎态度,没有马上投入人力和物力去开展这项信息化建设工作,因此在中国普通大众接触互联网是从调制解调器通过电话线开始的。随着互联网热潮的兴起,政府和企业纷纷上马"上网工程"[3]。由于没有明确的目标以及对信息的观念及其应用认识不足,因此投入了大量资金和人力之后,发觉除了建起内容长期没有更新的网站之外,几乎没有其它什么实质的应用。因此,这个时期,中国信息化的工作是很肤浅的。

2)现在

当今网络技术和通信技术的高速发展,极大地推动了信息化的进程。信息化成果的应用相当广泛,已经渗透到社会的各个层面。电子政务和电子商务以及 3G 和 4G 技术的发展和应用日趋成熟。国民经济和社会信息化事业发展迅速,信息化建设整体态势日益呈现出更加注重应用、实效以及与经济和社会协调发展的突出特征。具体表现在以下几个方面[5]:

① 我国信息产业国际竞争力不断提升。具有世界影响力的企业,例如联想和华为等在世界信息产业占有一席之地。我国有自主知识产权的信息技术,例如 TDS-CDMA 和 WAPI 等正在努力成为国际标准;

②信息技术在金融、电信、广电、海关、交通(民航、铁路和公路)等国家重点行业的管理中日益发挥重要作用。信息化成果在社会服务领域的应用日益广泛。国有大型企业信息化步伐不断加快,中小企业信息化建设热情日益高涨;

③ 电子政务在国家机关和政府部门已经普遍使用。电子商务在各行业的生产经营、供应采购、产品销售和对外贸易等环节发挥着愈来愈重要的作用;

④ 信息技术在农业领域的应用得到了进一步重视,各级政府和企业整合多种信息资源,积极开展面向"三农"的市场和科技信息服务[5]。

2.2　信息安全保障

信息化作为生产力,极大地推动了世界的发展,同时也带来了许多问题。其中,最为突出的就是信息安全问题。因此,《2006—2020 国家信息化发展战略》中将"信息安全"纳入其中,使其在 1997 年国家信息化发展战略的 6 要素基础上成为第 7 个要素。随着信息化的发展,信息化系统面临各种攻击者的综合威胁程度越来越高,而对攻击者的技术知识和技巧的要求越来越低。信息安全问题成为严重威胁信息化进程发展的障碍。

为了很好地保障信息化进程的顺利发展，针对信息安全问题，信息安全保障应运而生。伴随着信息化的发展历程，信息化和信息安全保障像一对孪生兄弟一样，一起在风雨中成长。信息安全保障的发展经历了以下3个过程[6-8]：

(1)单一防病毒系统

由于早期计算机基本为单机运行，没有通过网络连接，因此信息安全问题主要表现在计算机病毒方面，例如当时的大麻病毒和word宏病毒等。所以，早期的信息安全保障措施是采用单机版病毒防护软件(或者称为杀毒软件)。但是，当时由于经费和开放等方面的限制，病毒防护程序基本为国产。虽然在使用中存在不少问题(例如在杀word宏病毒的时候容易破坏word文档本身等)，但逐渐被广大民众所接受。

(2)简单的信息安全产品堆砌

随着互联网的普及，越来越多的计算机通过网络互连，带来了网络安全问题。此时，信息安全保障的任务主要是防范病毒、阻止入侵和抵御攻击等。相应的网络安全产品越来越多，例如防火墙和入侵检测等。网络供应商ISP(Internet Service Provider)和企事业单位为了保障网络的安全，购买和安装了防火墙和入侵检测等安全产品设备。由于没有系统化保护的思想，以及缺乏相关网络安全的规范和指南，因此形成了信息安全产品简单的堆砌局面。这种做法被称为“老三样”[6-8]：砌高墙、堵漏洞和装警报，属于典型的“头疼医头，脚疼医脚”。其结果是导致防火墙越砌越高、漏洞越堵越多、入侵检测系统越做越复杂、恶意代码库越增越大和安全事件越来越多，从而使得误报率持续增多、安全投入不断增加、维护与管理更加复杂和难以实施以及信息系统的使用效率大大降低。

产生这种局面的主要原因是当前信息安全产品的主流是防火墙、入侵监测和防病毒软件。这些安全产品是从互联网中共享信息服务和电子商务的平等交易等的安全需求中假定而来的。它的前提是用户不确定，没有一个明确的边界。常规的信息安全保障手段只能是以共享信息资源为中心，在外围对非法用户和越权访问进行封堵，以达到防止外部攻击的目的。而对共享源的访问源端不加控制，不能查找和控制信息安全隐患和系统漏洞的根源，而在安全事件的外部寻找解决途径[6-8]。

(3)系统化的、积极的信息安全保障体系

随着信息安全事件日趋严重，造成的经济损失与日俱增，中国政府和企事业单位开始高度重视信息安全保障工作。国家和有关部门从1993年起就已经开始制定相关法律、行政法规、部门规章等法律文件，规范信息化发展。这些法律文件包括全国人民代表大会2004年8月28日发布的《中华人民共和国电子签名法》[9]和2002年12月28日通过的《全国人民代表大会常务委员会关于维护互联网安全的决定》[10]。

国家信息化领导小组于2003年8月26日发布了《加强信息安全保障工作的意见》(中办[27]号文)[11]，第一次提出建设全面的、系统化的信息安全保障系统。27号文件中指出：“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。其核心是重点保障基础信息网络和重要信息系统安全，全面提高信息安全防护能力。

国际上信息化先进的国家已经制定了详尽的信息安全保障计划。其中，美国采用主动防御的信息安全保障机制；俄罗斯采用的是时序机制。我国信息安全保障则为基于安全基线政策(Security Baseline Policy)的运筹(Operational)保障机制。安全基线政策是从宏观、中观和微观3个角度，在国家、企事业和用户3个层次上，根据战略、管理和技术3个方面的法律依据、管理基础、实施手段和技术方法的具体内容制定的基本信息安全保障策略及其基本要求。

基于安全基线政策的运筹保障机制，其含义不言而喻就是运筹帷幄。安全基线政策的主要内容表现在：

(1)战略保障

战略保障实际是为信息化的发展提供法律依据。根据中国信息化的发展界定法律边界，规划发展蓝图和指明策略方向。

(2)管理保障

管理保障是为信息化发展制定协调制度。根据中国国情制定实施办法，颁布具体条例和说明执行程序。

(3)技术保障

技术保障就是具体的实施方法。根据美国安全工程能力成熟度模型SSE-CMM分析系统的功能需求，设计系统的整体方案，建立系统的协同机制，进行系统的安全运行管理，完成系统的安全时间审计和实施系统的安全态势监视。

因此，基于安全基线政策的运筹保障机制从等级保护的角度出发，利用安全系统工程(Security System Engineering)设计的理念，从应急响应、灾难备份、安全监测、入侵检测和病毒防护等方面系统地对信息系统提供全面的信息安全保障。

2.3 信息安全保障评价指标体系

信息安全保障系统的建设状况以及保障效果需要有一个科学的评价体系来衡量。这个评价体系就是信息安全保障评价指标体系，它是在安全基线政策基础上对信息安全保障系统进行检验。建立信息安全保障评价指标体系的目的如下：

(1)检验信息安全保障系统是否达到系统信息安全的要求；

(2)信息安全保障系统的保障效果，包括保障周期(保障的时间)，即在什么时间需要增加什么样的保护措施；

(3)系统信息安全状态的监控和信息安全态势分析。

完整的信息安全保障评价流程包括3个过程：静态评估、动态评估、状态评估。

(1)静态评估：评价纸面上的东西，即评价信息安全保障设计的方案文档、制定的安全措施档案和安全管理的标准规范等。主要的评价内容为：安全方案的合理性、安全措施的正确性和标准规范的科学性。静态评估的主要手段是专家打分和问卷调查。

(2)动态评估

动态评估是对信息系统和信息安全保障系统的运行情况做出判断。该过程需要统计信息系统和安全保障系统日常运行的记录数据，包括信息安全值班的所有记录和安全审计的日志等，例如网络流量、网络带宽、协议，以及入侵检测、防病毒、防火墙和安全审计等原始记录数据和统计显示数据。对记录数据进行统计和处理，得到信息安全的评价结论。

(3)状态评估

状态评估过程是检验信息安全保障的效果，主要表现在对信息和信息系统的安全属性(保密性、完整性、真实性、可用

性、不可抵赖性、抗毁性、生存型和有效性)进行测试和检验。主要手段包括两种:第一种为渗透测试,模拟黑客攻击的渗透测试技术,有助于查找信息系统的脆弱点和检验信息安全保障系统的效果;第二种为专项测试,针对信息和信息系统的某个安全属性,采用专业技术进行单项测试,检验信息安全保障在某个功能上的保障效果。

针对上述3个评估过程可以得到3种信息安全评价指标:静态(功能)指标、动态(运行)指标和状态(属性)指标。它们构成了信息安全保障评价指标的核心。

3 分析总结

信息化发展历程中的3个进程之间的关系是互为基础、相互制约。它们都是建立在一定的基础之上,由核心技术作支撑搭建起来的应用平台。其内涵如图2所示。

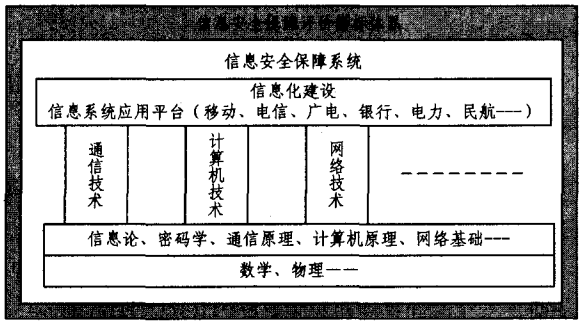

图2 信息化内涵

其中,信息化的基础和支撑的含义如下:

(1)基础

从技术角度分析,信息化的基础包含两个层次的内容:

① 通用基础层

通用基础层包括数学和物理等基础性的知识和方法,属于信息化最底层的铺垫。

② 信息基础层

信息基础层包括信息论、密码学、通信原理、计算机原理和网络基础理论等专业基础知识。信息基础层是在通用基础层之上的。

(2)支撑

在信息化基础之上,就是支撑整个信息化系统的支柱——关键技术。信息系统的支撑关键技术包括通信技术、计算机技术和网络技术等。

在基础之上,利用关键技术支撑起来的就是信息化最核心的部分——信息系统(信息应用平台)。在信息化发展中,由于信息通信的需要,按照某种业务需求,各行各业都建立起不同功能和业务类型的信息系统,即能够提供某种业务能力的信息应用平台。

信息系统应用平台面临很多的安全威胁。如果一个信息平台能够提供业务服务功能,却不能保障用户的信息安全,让用户的合法信息外泄,或者用户账号等被盗,则该信息平台根本不具有完整的服务功能,而且很快就会失去其应用价值。因此,必须具有相应的信息安全保障系统。所以应在信息系统之外建立一道屏障,保护信息系统免遭外来的攻击和入侵,该屏障就是信息安全保障系统。由于信息安全问题不仅仅存在于信息系统(应用平台)上,而且存在于支撑技术和基础中,因此,信息安全保障系统不仅要在应用层面,而且要在关键技术和基础设施层面实施全面的保护。

为了更好地检验和促进信息安全保障系统的功效,对信息安全和信息安全保障进行全面的、科学的评估,必须建立信息安全保障评价指标体系,即从战略、管理、工程和技术4个方面,在宏观、中观和微观3个层面,根据安全基线政策的要求,利用一组可量化的指标建立信息安全保障系统的评估体系。

实质上信息化的3个进程是循序渐进和循环周期发展的,如图3所示。3个过程首尾相接,承前启后,并互相促进。

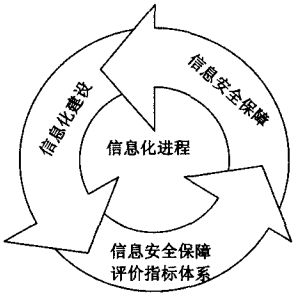

图3 信息化3个进程之间的关系

结束语 中国信息化进程经历了3个具有明显特征的阶段。可以看出与国际上信息化发展历程相比我国信息化发展的每个阶段的开始时间相对滞后,起始水平相对较低。虽然,中国在社会信息化方面取得了巨大成就,但是我们不能因此而盲目乐观。信息化是一个复杂的巨工程,必须综合考虑信息化进程中3个阶段存在的各种问题,及时调整发展的方向和节奏。

目前,中国信息化水平与国际先进水平还有较大差距。尤其是信息化重点单位的网络和信息安全形势不容乐观,全行业的网络和信息安全意识还比较淡薄,重要网络和信息系统还存在安全隐患,影响较大的网络与信息安全事故时有发生。因此,应该明确制定信息化发展各个阶段的目标和任务,研究和开发具有自主知识产权的信息化技术,努力实现我国信息化的高速发展和全面应用。

参 考 文 献

[1] 中共中央办公厅,国务院办公厅. 2006-2020年国家信息化发展战略[D]. 2006(06):1-28

[2] 信息化[EB/OL]. http://baike.baidu.com/view/27.htm#3

[3] 崔建国. 关于加快中国信息化进程的思考与对策[J]. 上海社会科学院信息研究所,上海社会科学院学术季刊,2001(4):117-126

[4] 陈曦. 对于中国信息化概念及进程的思考[EB/OL]. 赛迪网,2007-05-28

[5] 赵树峰. 中国信息化建设现状与发展趋势[EB/OL]. 中国吉林网,2006-01-19

[6] 杨晨. 六大要素支撑我国信息安全保障体系——访信息安全专家曲成义[J]. 信息网络安全,2005(3):11-12

[7] 信息科学与工程学院. 曲成义研究员来信息学院谈国家信息安全保障体系[EB/OL]. 中国科学院研究生院新闻网,2006-03-20

[8] 曲成义. 构建国家信息安全保障体系的思考[J]. 信息安全与通信保密,2004(5):20-21

[9] 全国人大委员会. 中华人民共和国电子签名法[C]//第十届全国人民代表大会常务委员会第十一次会议. 北京,2004

[10] 全国人大常委会. 全国人民代表大会常务委员会关于维护互联网安全的决定[C]//第九届全国人民代表大会常务委员会第十九次会议. 北京,2002

[11] 国家信息化领导小组. 中办[27]号文:加强信息安全保障工作的意见[R]. 2003:1-17