信息安全的概念及方法论探讨

胡昌振
(北京理工大学网络安全技术实验室,教授　北京 100081)

〔摘要〕 本文探讨了信息安全的基本概念,描述了信息安全、信息保障与信息对抗的关系,阐述了信息安全研究方法论,并讨论了信息安全技术系统的设计原则。
〔关键词〕 信息安全　概念　方法论　设计准则　　〔中图分类号〕 TN97　TP393　N3

信息的实质是通过信号实现对物质与能量的调节和控制,而信息所调控的物质和能量一般远大于信息所包含的物质和能量。因此,由信息安全导致的损失,不仅是指信息自身价值所遭受的损失,而且还包括其可能造成的其它方面的更大损失。

在当今社会,信息已成为国家的主要财富和一种重要战略资源,国家综合实力的竞争越来越集中在信息优势的争夺上,而信息优势的夺取,直接地表现为信息安全与对抗。信息安全已逐步成为国家政治、经济、科技、文化,特别是军事等安全领域的一个重要方面。

概念体系是任何技术领域的初始理论和方法论基础,对信息安全概念的完整认识,无疑是信息安全技术研究的基础。

一、信息安全概念体系

1. 信息安全的基本范畴

发展能力数据　国家经济地图集和人口生活质量与可持续发展能力数据库主页均提供了动态制图和空间数据查询路径,通过交互式界面,用户可任意选取派生的结构化地图数据库、单项或多项制图指标、地图表达方式、自定义数据分级和确定色彩色级方案,按省级或县级空间单元可视化;也可以分指标进行查询、检索。

5. **模型分析**　为 Web 用户提供各种数据挖掘与共享的策略和方法、有效的空间数据浏览和查询工具。这并非仅为终端用户获取数据带来便利,更重要的是通过数据的获取、结构化处理、分析、提炼,为进一步实现由数据的获取、共享到知识规律的形成和发现提供参考方案。

(1) **人口预测**　人口数据经时空、属性结构化处理,可根据一个时期的人口出生、死亡、生育水平、人口迁移等单项专题指标、相互关系及其时空规律,以及未来人口政策和经济发展水平的分析,建立人口预测模型,对人口及其性别进行初步分析预测,包括 2005 年和 2010 年全国分区人口规模、变化趋势及其性别差异[9],为用户提供数据挖掘与共享方案。

(2) **宏观区域经济分析、评价**　以 GDP 增长持续性分析为例。选取各省 1990、1992、1995 和 1997 年人均 GDP 指标,并计算其占全国比重的排名及变化趋势。为有助于深入了解各省国民经济变化、发展的差异性和空间格局,将 GDP 增长的持续性分成了 6 种类型:稳定增长,包括河北、黑龙江、福建、江西、山东、河南、广东;振荡增长,包括北京、上海、江苏、浙江、广西;持续平稳,包括天津、安徽、湖北、湖南、西藏;持续振荡,包括海南;振荡减少,包括四川、云南;逐步减少,包括山西、内蒙、辽宁、吉林、贵州、陕西、甘肃、青海、宁夏、新疆。

最后要指出:从我们的工作实践中发现,为了充分、有效地实现空间数据信息共享,除了进行深入细致的调查、根据用户需求对空间数据进行分类分级管理与共享外,需要加强对空间数据的可视化动态交互、分析模型的透明性和在线服务功能等的研究,以提高空间数据信息共享的水平与层次。

参 考 文 献

[1] Letourneau, F. A fully integrated geo - spatial data warehouse, Proceedings of 19th International Cartographic Conference, Ottawa, ICA, 1999, 1301 - 1310
[2]中华人民共和国行政区划单元分类与代码标准(GB/T 2260 - 1995),中华人民共和国国家标准. 国家技术监督局. 北京:中国标准出版社,1996
[3]中华人民共和国国民经济行业分类与代码标准(GB/T 4754 - 94),中华人民共和国国家标准. 国家技术监督局. 北京:中国标准出版社,1995
[4]刘若梅,蒋景瞳,贾云鹏. 中国可持续发展信息共享元数据标准实施. 见:中国地理信息元数据标准研究. 中国 21 世纪议程管理中心,北京:科学出版社,1999, 36 - 46
[5]Ahl V, Allen T F H. Hierarchy theory: A vision, vocabulary and epistemology, Columbia University Press, New York, 1996
[6] 郭腾云. Web GIS 系统的实现技术及其开发研究. 地理研究,1999,18(S):119 - 127

(责任编辑　王宏章)

信息价值是研究信息资源改变的基础。信息安全的概念建立在信息价值和信息损失的基础上，其范畴可通过信息损失来确定。

信息资源是主体可以获取并用于其活动的信息总和。根据对主体的影响，信息资源可分为有价值信息和中性信息，而信息的价值又可分为积极价值和消极价值。

信息作用指主体的信息资源或其实现信息的过程（包括获取、传递、存储、处理、分发和管理等）中所发生的偶然或有目的的改变。这种改变具有不以主体意愿为转移的性质。信息作用可以不直接通过信息而是通过对其所支持主体（包括个人、组织、社会、国家等）施加“物理”影响，或者对信息主体本身（如人的感觉器官、团体的管理机构等）施加影响来实现。

信息损失是主体所不希望的、具有否定价值的、客观上改变其信息资源的一种信息作用。这种消极价值具有损害主体利益，影响需求满足、方案制定和实施，降低活动效果，增大活动消耗，妨碍组织活动及管理等作用。

信息损失可以从其受到损失的数量和概率两方面进行定量评估。信息损失的数量和概率主要取决于主体、客体、风险源和信息作用等特点；社会和法律基础、技术发展水平以及信息对抗手段的数量和能力等因素。

2. 信息安全、信息保障与信息对抗的关系

信息对抗是感知对方的信息资源，使对方遭受信息损失，同时保障己方免遭类似影响的信息作用过程。

信息安全保障是信息对抗的组成部分。信息对抗中，对立主体双方都不仅企图通过信息作用给对方造成信息损失或其它损失，而且还需防止类似作用给己方造成损失，即保障己方的信息安全。

信息安全指的是一种防止与避免信息损失的受保护状态。只有当可能的信息损失在可接受的限度内，信息才是安全的。

从概念上讲，信息对抗与信息安全保障是一个过程，而信息安全则是一种状态。

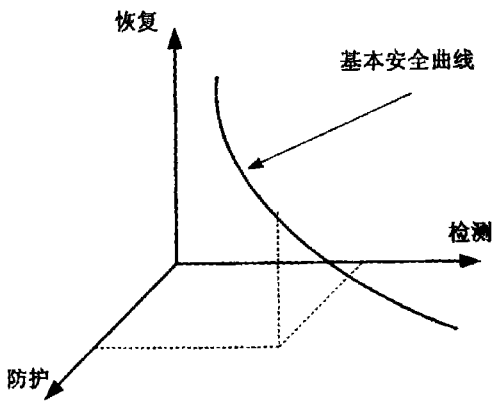

图 1 信息安全与信息安全保障的关系

信息安全保障包括防护、检测和恢复 3 类机制。对所有信息系统，为提供信息安全保障，存在大量的防护、检测和恢复组合，如图 1 所示。

图 1 中，曲线代表满足给定安全需求的信息安全状态集合，即信息安全可以通过不同的防护、检测和恢复机制的组合而获得。

3. 信息安全的基本类型

信息安全包括信息心理安全和信息技术安全两种基本类型。

信息心理安全所保护的客体是个人心理以及社会（或团队）意识。个人心理包括意识、神经系统等内容，社会（或团队）意识包括宗教、意识形态、精神文化、道德、社会心理、科学等内容。信息心理安全的任务是保障宗教、政治观点、道德、艺术等不受侵害。在社会（或团队）意识方面，信息心理安全是同错误的世界观（如占星术、邪教等）及伪科学作斗争；在个人心理方面，信息心理安全则是同散布和宣传神秘主义、反理性主义等作斗争。

信息技术安全所保护的客体是各种信息技术系统。比如在军事方面，被保护客体是指通信系统、军队指挥自动化系统、武器控制系统、侦察技术系统、无线电电子对抗系统，以及为相应人员提供信息保障服务的技术系统（如计算机网络）等。

4. 信息安全的工程概念

工程上，信息安全是与风险相联系的概念，通过信息安全风险管理与控制实现。信息安全风险是信息价值、脆弱性和威胁等 3 个变量的函数，如图 2 所示。

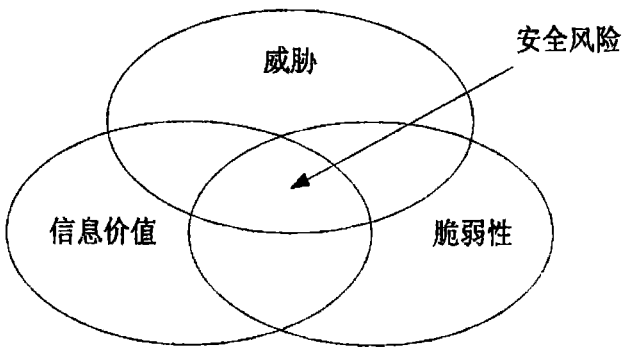

图 2 信息安全风险组成

所谓脆弱性，就是可以被用来颠覆、利用、损坏和破坏信息资源的方式；所谓威胁，就是具备利用脆弱性能力的主体。

信息安全风险管理与控制是一个信息风险的测量、识别、控制及其最小化的过程，即在给定的信息损失约束下，协调信息资源的价值、脆弱性和威胁的过程。

二、信息安全研究方法论

1. **复杂系统观点**

作为一个人工系统，信息安全系统是简单系统，但其工作环境却是复杂的。信息主体和客体相结合所构成的信息安全系统是一个复杂系统，其复杂性体现在：(1) 系统各组成之间的联系广泛而紧密，每一组成的变化都会受到其它组成变化的影响，并会引起其他组成的变化；(2) 系统具有多层次、多功能的结构，每一层次均成为构筑其上一层次的单元，同时也有助于系统某一功能的实现；(3) 系统在发展过程中能够不断地学习并对其层次结构与功能结构进行重组及完善；(4) 系统是开放的，与环境有密切的联系，能与环境相互作用，并能不断向更好地适应环境的方向发展变化；(5) 系统是动态的，处于不断发展变化之中，其本身对未来的发展变化有一定的预测能力。信息安全系统所处理的是复杂环境中的主体行为问题，因此，信息安全的研究必须基于复杂系统的观点。

2. **从定性到定量的综合集成方法论**

信息安全是通过主体对客体的信息作用体现的，在信息安全所面对的开放的复杂巨系统环境中，信息作用具有时空复杂性。信息作用的复杂性决定了信息安全问题不能简单地采用还原论的观点处理，必须注重整体论与还原论的辩证统一，即采用从定性到定量的综合集成的思想方法，追求整体效能。

基于整体论和还原论相结合的思想，信息安全技术应以“人”为核心，运用定性分析与定量分析相结合；分析与综合相结合；专家知识的集成、专家经验判断与计算机运算相结合的方法，综合处理信息安全中的科学理论、经验知识和专家判断等问题。

三、信息安全技术系统设计原则

1. **信息安全技术系统的特点**

从系统工程角度，信息安全技术系统具有如下特点。

(1) **规模性** 信息安全技术系统由多种不同类型的信息安全技术联合组成。根据安全目标的不同，这些信息安全技术可能密集设置在某台主机上，也可能分散部署在同一内部网或广域网上。尽管整个信息安全技术系统由多种不同类型的信息安全技术联合组成，但这些信息安全技术彼此并不孤立，而是密切配合、有机协调成为一个整体，共同完成一个统一的安全目标。

(2) **环境关联性** 整个信息安全技术系统的技术功能与性能的实现，在很大程度上会受到实际环境因素的影响与制约。

(3) **层次性** 信息安全技术系统具有多层次体系结构的性质，一般的构成为：基本层由多种信息安全技术与可独立发挥作用的设备组成；第二层在平台或站点一级，由多种不同的信息安全技术与设备组成，具有小规模的控制中心、信息处理设备，形成一个中规模的信息安全技术系统；最高层信息安全指挥控制中心是整个信息安全技术系统的核心部分，直接由信息安全管理员管理。即使如此，依据安全级别不同，这种信息安全技术系统还可能是更高级别信息安全技术系统的分系统。

(4) **可控制性** 信息安全技术系统不是那种人类尚无法驾驭的自然系统，而是人为设计的，因此应该是可控制的。作为操作者，“人”是信息安全技术系统的核心，设计时应该被当作信息安全技术系统的主要功能元件。为使信息安全管理员在系统功能中发挥重要作用，信息安全技术系统的主要分系统的控制台上都应设置人/ 机交互接口。信息安全技术系统是一种对抗系统，比一般工程系统更复杂，必须充分考虑对抗因素的影响，实施冗余储备、保密设计，确保系统的可靠性和生存力。

(5) **不确定性** 在复杂的信息安全威胁环境中，信息安全技术系统的输入是随机性的，系统可能获取的威胁数据一般是重叠混杂、残缺不全的，具有很大的不确定性。

2. **信息安全技术系统设计的功能考虑**

信息安全技术系统设计应考虑法律、政策、制度、情报、技术和信息资源等环境因素（见图 3 所示）。

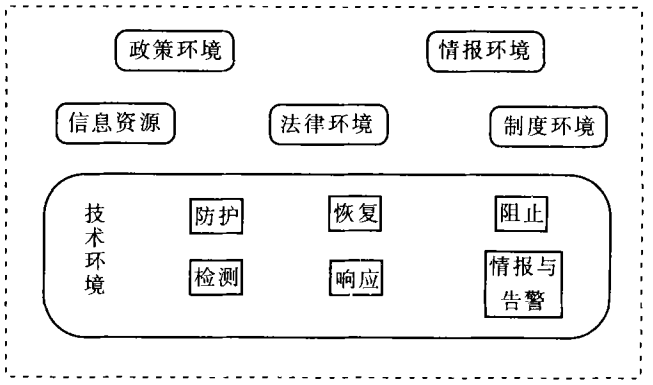

图 3 信息安全技术系统设计的考虑因素

信息安全技术系统的功能要求是：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；对消极信息作用作出信息防御反应。一般来说，制止与防止消极信息作用是预防性的信息安全保障要求，检测、恢复和反应则是操作性的要求。为满足上述需求，在所建立的信息安全

保障投入基础上，应该确保信息资源运行的灵敏性、可靠性和持续性。

信息安全技术系统功能可描述如下。

(1) **阻止** 明确信息资源安全焦点;采取必要的信息资源安全立法行动,强化法律;执行必要的信息资源安全条例;公布明确的信息资源安全政策;制订信息资源安全启蒙、培训和教育计划;制订信息资源安全管理与控制措施;协调各种信息安全努力;发展有效的信息资源保护、检测、恢复和反应能力。

(2) **保护** 实施风险分析与风险管理;开发减少风险的技术措施;作出管理决策;制订减少风险的计划;试验、审查安全保护手段;积极采用先进的保护技术。

(3) **情报与报警** 提供所需的情报支持;为播发战争警报提供所需的指挥、控制、通信与计算机系统。

(4) **检测** 提供有关破坏、入侵和攻击的实时检测;共享敏感的情报(如威胁、脆弱性、入侵和攻击)及与之相关的方面(如情报、执法、市场和隐私)。

(5) **恢复** 评估威胁的性质和程度,以提供规范的攻击报告,并制订重新分配和恢复相关信息资源的优先等级;向信息资源主体发出警报;隔离和控制"损失";重新部署关键信息资源的机能,以及关键信息资源的职能和活动;恢复信息资源的全部运行能力。

(6) **响应** 核查攻击的性质、程度、发起者等,以便作出相应的反应;研究可反应选择的范围,如民事诉讼、刑事诉讼、军事力量、情报诱导、外交行动、经济赔偿;采取直接反击行动;恢复以可靠、灵活和机敏为信息防御基础的威慑作用。

3. **信息安全技术系统的设计准则**

信息安全技术系统设计是系统科学和系统工程思想、原理和方法的具体实践和运用。在研究、处理信息安全技术系统设计问题时,应该以系统涌现性原理和复杂适应系统原理为理论基础,并遵循如下基本原则。

(1) **整体性原则** 考虑系统整体要求,把信息安全技术系统局部部件和局部要素置于所在的系统之中,进行全局考虑、综合处理。树立目的性、实用性观点,系统设计以追求实用效果为出发点。

(2) **协同性原则** 分析和描述信息安全技术系统组成间的因果关系、配合关系,并以此为条件,通过组合优化与控制,使系统整体功能达到最佳。把环境依存关系作为重要约束条件之一,确保系统能在恶劣信息环境中完成信息安全防护任务,实现特定的安全功能。同时,设计者应该即时掌握信息安全技术发展状况和趋势,预测未来的系统需要,应用其它技术领域的最新成果。

(3) **结构性原则** 设计系统时,要综合考虑系统结构关系。基于外部行为选择合理的系统结构方案,通过简洁的内部结构,确保理想的外部行为,这是结构性原则的具体体现。借助现代数学方法,按内在联系、结构、功能关系,将系统各要素形式化、定量化,通过系统模型,科学、严密地评价系统,为设计信息安全技术系统提供定量依据。

(4) **满意准则** 对复杂系统,最优设计是很难实现的,次优设计则要付出很大代价。应该在给定满意程度下,实施满意设计,即设计结果足以完成预定使命,同时也基本合理。

参 考 文 献

[1] A. X. 沙瓦耶夫著. 国家安全新论[M]. 北京:军事友谊出版社,2002
[2] 王越. 以科学的态度正确对待信息安全问题. 网络安全技术及应用[J],2003,36(12)
[3] 胡昌振. 在合作与竞争中寻求发展. 计算机安全[J],2003,24(2)
[4] 胡昌振. 把握我国信息安全技术跨越式发展机遇. 计算机安全[J],2003,31(9)
[5] 胡昌振. 网络入侵检测的误警问题探讨. 信息安全与通信保密[J],2003,32(8)
[6] 王智远等主编. 联合信息作战[M]. 北京:军事友谊出版社,1999
[7] 胡昌振. 基于指挥控制的网络安全防御体系. 信息安全与通信保密[J],2002,20(8)
[8] 王寿云等. 开放复杂巨系统[M]. 杭州:浙江科技出版社,1996
[9] 石纯一. 定性推理方法[M]. 北京:清华大学出版社,2002
[10] 钱学森. 创建系统学[M]. 太原:山西科技出版社,2001
[11] 成思危主编. 复杂性科学探索[M]. 北京:民主与法制建设出版社,1999

(责任编辑 苏 青)

(上接第 41 页)

他发现:等离子球可以通过分裂成两个球进行复制,在适当条件下也能变得更大,即吸收中性氩原子后撕开它们,成为离子和电子,并扩大等离子球的边界层;它们可以通过放射电磁能交流信息,使其它等离子球内部的原子以特定的频率振动。这种等离子球不仅可以完全满足自组织系统的要求,而且是最早的气体细胞。

Sanduoviciu 甚至认为:这种气体细胞可能是在电暴中产生的地球上的第一批细胞。他说,等离子球的出现看来很可能是生物进化的先决条件。布鲁塞尔大学的物理化学家 Gregoire Nicolis 说:这种可能性很大,像 DNA 这种生物分子也可能在等离子球存在的温度下产生。

但 Sanduoviciu 强调,虽然等离子球的形成需要高温,但却可以在较低的温度下继续存在。这可能是发生正常的生物化学作用的一种环境。他的工作最令人感兴趣的意义是,这些等离子球可能是其它行星上的生命形式的起源。这意味着我们对地外生命的研究方案可能需要重新考虑。

(刘先曙)