

网络空间安全学科简论

张焕国^{1,2}, 杜瑞颖^{1,2}

(1. 武汉大学国家网络安全学院, 湖北 武汉 430079;

2. 空天信息安全与可信计算教育部重点实验室, 湖北 武汉 430079)

摘要: 随着信息技术与产业的高速发展和广泛应用, 人类社会进入信息化时代。在信息化时代, 人类生活工作在网络空间中, 因此确保网络空间安全成为信息时代的基本需求。我国已经发展形成了完整的网络空间安全学科体系, 因此, 全面论述网络空间安全学科的体系结构与理论基础成为网络空间安全学科建设和人才培养的当务之急, 内容包括: 网络空间与网络空间安全的概念, 网络空间安全学科的内涵, 网络空间安全学科的主要研究方向及研究内容, 网络空间安全学科的理论基础和方法论基础。因此, 正确理解和掌握网络空间安全学科理论与体系结构, 不仅对我国网络空间安全学科建设和人才培养具有十分重要的指导意义, 而且对我国网络空间安全领域的科学研究和产业发展也具有十分重要的指导意义。

关键词: 网络空间; 网络空间安全; 网络空间安全学科; 学科建设; 人才培养

中图分类号: G642

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019021

Introduction to cyberspace security discipline

ZHANG Huanguo^{1,2}, DU Ruiying^{1,2}

1. School of Science and Technology of Cyberspace, Wuhan University, Wuhan 430079, China

2. State Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan 430079, China

Abstract: With rapidly development of electronic information technology and industry, human society comes into information age. In the information age human lives and works in cyberspace. There for, it is the base requirement for human to ensure cyberspace security in the information age. Now, our country has established whole one-level discipline of cyberspace security. So the top priority for us is that should discuss overall the architecture and base theory of cyberspace security discipline. It include the contents as follows: the concept of cyberspace and cyberspace security, the definition of cyberspace security discipline, main research area and contents of cyberspace security discipline, base theory and method theory of cyberspace security discipline. Consequently, we should correctly understand and know well

收稿日期: 2019-02-17; 修回日期: 2019-04-26

通信作者: 张焕国, liss@whu.edu.cn

基金项目: 国家重点基础研究发展计划(973 计划)基金资助项目(No.2014CB340601); 国家自然科学基金重点资助项目(No.61332019)

Foundation Items: The National Basic Research Program of China (973 Program) (No.2014CB340601), The National Natural Science Foundation of China (No.61332019)

论文引用格式: 张焕国, 杜瑞颖. 网络空间安全学科简论[J]. 网络与信息安全学报, 2019, 5(3): 4-18.

ZHANG H G, DU R Y. Introduction to cyberspace security discipline[J]. Chinese Journal of Network and Information Security, 2019, 5(3): 4-18.

the architecture and base theory of cyberspace security discipline. It is very important not only for discipline construction and personnel training but also for science research and industry development in our country.

Key words: cyberspace, cyberspace security, cyberspace security discipline, discipline construction, personnel training

1 网络空间与网络空间安全学科

当前,网络空间、网络空间安全和网络空间安全学科成为社会与信息科学技术领域关注的焦点之一。本节介绍它们的概念和内涵。

1.1 网络空间与网络空间安全的概念

人类社会在经历了机械化、电气化之后,进入了一个崭新的信息化时代。在信息时代,信息产业成为世界第一大产业。信息就像水、电、石油一样,与所有行业和所有人都相关,成为一种基础资源。信息和信息技术改变着人们的生活和工作方式。离开计算机、网络、电视和手机等电子信息设备,人们将无法正常工作。因此可以说,在信息时代,人们生存在由物理世界、人类社会和信息空间组成的三元世界中^[1-2]。

为了刻画人类生存的信息环境或信息空间,人们创造了 Cyberspace 一词。早在 1982 年,加拿大作家威廉·吉布森在其短篇科幻小说《燃烧的铬》^[3]中首次创造使用了 Cyberspace 一词,意指由计算机创建的虚拟信息空间。Cyberspace 在这里强调计算机爱好者在游戏机前体验到的交感幻觉,体现了 Cyberspace 不仅是信息的简单聚合体,也包含了信息对人类思想认知的影响。此后,随着信息技术的快速发展和互联网的广泛应用, Cyberspace 的概念不断丰富和演化。

2008 年,美国第 54 号总统令对 Cyberspace 进行了定义: Cyberspace 是信息环境中的一个整体域,它由独立且互相依存的信息基础设施和网络组成,包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统。

我们认为,美国的定义总体是合理的,但列出许多具体系统和网络,比较烦琐。而且,随着

信息技术的发展还会出现新的系统和新的网络,又需要对定义进行修改和调整。显然,这是不必要的。

除了美国之外,还有许多国家也对 Cyberspace 进行了定义和解释,但与美国的说法大同小异、各有侧重。

我们给出自己的定义:网络空间是信息时代人们赖以生存的信息环境,是所有信息系统的集合。

与美国的定义相比,我们的定义不仅抓住了信息环境和信息系统这两大核心内容,而且表述简洁。不会随着新系统和新网络的出现,重新修改和调整定义。

因此,把 Cyberspace 翻译成信息空间或网络空间比较好^[4-5]。其中信息空间突出了信息环境和信息系统这两大核心内容,网络空间突出了网络互联这一重要特征。本文主要采用网络空间这一名称。

众所周知,能源、材料、信息是支撑现代社会大厦的支柱。其中,能源和材料是物质的、具体的,信息是逻辑的、抽象的。信息论是信息科学的理论基础。信息论的基本观点告诉我们:系统是载体,信息是内涵。信息不能脱离系统而孤立存在。

人身安全是大家最关心的事情,也是大家最熟悉的安全问题。人身安全是人对其生存环境的基本要求,即要确保人身免受其生存环境的危害。因此,哪里有人,哪里就存在人身安全问题,人身安全是人的影子。同样,信息安全是信息对其生存环境的基本要求,即要确保信息免受其生存环境的危害。因此,哪里有信息,哪里就存在信息安全问题,信息安全是信息的影子。

因为网络空间既是人的生存环境,也是信息的生存环境,因此网络空间安全是人和信息对网络空间的基本要求。又因为网络空间是所有信息系统的集合,是复杂的巨系统,人在其中与信息相互作用、相互影响。因此,网络空间的信息安全问题更加突出。

根据信息论的基本观点,系统是载体,信息是内涵。因此,网络空间安全的核心内涵仍是信息安全,没有信息安全就没有网络空间安全。

1.2 网络空间安全形势严峻

当前,一方面是信息技术与产业的空前繁荣,另一方面是危害信息安全的事件不断发生。敌对势力的破坏、黑客攻击、利用计算机犯罪、网络上有害内容泛滥、隐私泄露等,对信息安全构成了极大威胁^[6-7]。

敌对势力对我国信息安全的破坏是经常不断的。据美国国家安全局(NSA, National Security Agency)前雇员爱德华·斯诺登爆料:美国针对中国进行了大规模的网络攻击,并把中国领导人、商务部、外交部、银行、电信公司、华为公司和清华大学等作为重点目标。美国国家安全局成功入侵了华为公司和清华大学,复制了大量的客户资料、产品源代码和科研文件。实际上,遭到美国入侵的单位远远不只华为公司和清华大学。2017年3月8日维基解密宣称,他们获得了几千份美国中央情报局(CIA, Central Intelligence Agency)在2013到2016年间的网络攻击活动秘密文件。这些文件不仅显示了CIA具有网络攻击的巨大能力和拥有庞大的黑客攻击武器库,而且还说明CIA能够攻击基于Windows、Android、iOS、OS X、Linux的各种信息系统,其中包括计算机、路由器、手机、车载系统和家用电器等。

黑客攻击已经成为经常性、多发性的事件。只要是全国性或国际性的大型活动,都可能遭到大量的黑客的攻击。计算机病毒等恶意代码是黑

客的主要攻击武器。目前,计算机病毒已有几千种,而且还在继续增加。追求经济和政治利益成为研制和使用计算机病毒的新特征。恶意软件的开发、生产、销售,形成了一条地下产业链。这是值得我们认真对付的。

利用计算机进行经济犯罪超过了传统经济犯罪。目前网上银行和电信诈骗成为恶性案件的高发区,钓鱼网站、伪造银行卡、网络诈骗、电信诈骗等给人民群众造成严重经济损失。

网络上有害内容泛滥。垃圾邮件满天飞、黄赌毒泛滥、伪科学的内容、政治上不健康的内容充斥网络,网络环境亟待规范和治理。创建网络精神文明成为我们的一项重要任务。

隐私保护问题严重。在国内外已经发生多起个人隐私数据被泄露的严重事件。例如,2018年3月爆出美国Facebook公司泄露了8000万用户个人数据的丑闻,给用户造成不可估量的损失。在我国也有不法分子在网上公开出售个人信息数据,严重侵犯了公民的隐私权。由此引发了大量恶性治安事件,严重扰乱了社会治安。

信息技术的发展推动了军事革命,出现了信息作战、网络作战等新型战法和网军等新型军兵种。早在1995年美国就提出了信息作战的概念,并成立了信息作战指导委员会。2009年10月美国正式成立网络司令部。2011年5月16日美国公布了“网络空间国际战略”,7月14日公布了“网络空间作战战略”,提出“陆、海、空、天、网”五维一体的美国国家安全概念。两次海湾战争和科索沃战争中,美国都成功实施了信息作战。2010年黑客利用震网病毒成功攻击了伊朗的核工厂,物理毁坏了大部分的铀离心机,重挫了伊朗的核计划。

除以上威胁之外,科学技术的进步也对信息安全提出新的挑战。由于量子计算和DNA计算具有并行性,从而使许多现有公钥密码(RSA、

EIGamal、ECC 等) 在量子和 DNA 计算机环境下不再安全^[8]。

综上所述, 网络空间安全的形势是严峻的。

对于我国来说, 网络空间安全形势的严峻性不仅在于上面这些威胁, 还在于我国在 CPU 芯片和操作系统等核心芯片和基础软件方面大量使用国外产品。这就使我国的网络空间安全形势更加严峻复杂。Windows 操作系统存在漏洞是大家熟知的。2017 年业界揭露出 Intel 公司的 CPU 芯片存在两个重大安全漏洞。2018 年, 美国挑起了与我国的贸易摩擦和制裁打压我国中兴、华为等公司。这些事件使我们更清楚地看到这一问题的严重性。

我国政府高度重视网络空间安全。2002 年, 党的十六大文件已经把信息安全作为我国国家安全的重要组成部分。2009 年, 胡锦涛总书记在第 64 届联合国大会一般性辩论会上强调了信息安全等非传统安全的重要性。2012 年, 党的十八大文件进一步明确指出, 要“高度关注海洋、太空、网络空间安全”。2013 年年底, 中央网络安全与信息化领导小组成立, 负责统一领导我国网络安全与信息化工作。2014 年, 习近平总书记在中央网络安全与信息化领导小组第一次会议上指出: “没有网络安全, 就没有国家安全。没有信息化, 就没有现代化”。2016 年 11 月 7 日, 我国颁布了《中华人民共和国网络安全法》, 这是确保我国网络安全的基本法律。2016 年 12 月 27 日, 国家互联网信息办公室和中央网络安全与信息化领导小组办公室联合发布了我国《国家网络空间安全战略》, 文件明确了确保我国网络空间安全和建设网络强国的战略目标。2017 年 3 月 1 日, 外交部和国家互联网信息办公室共同发布了《国家网络空间国际合作战略》, 文件明确规定了我国在网络空间领域开展国际交流合作的战略目标和中国主张。2017 年 10 月 18 日, 习近平总书记在十九大报告中再次强调, 加快建设创新型国家和网络强

国, 确保我国的网络空间安全。2018 年 3 月 21 日, 中央决定: 中央网络安全与信息化领导小组改组为中央网络安全与信息化委员会, 负责相关领域重大工作的顶层设计、总体布局、统筹协调、整体推进、监督落实。这一变动意味着, 其指导网络安全和信息化工作的职能将进一步加强。2018 年 4 月 20 日, 习近平总书记在网络安全与信息化委员会工作会议上指出: 要主动适应信息化要求, 强化互联网思维, 不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力。核心技术是国之重器。没有核心技术, 就只能受制于人。要下决心、保持恒心、找准重心, 加速推动信息领域核心技术突破。

网络空间安全事关国家安全、社会稳定、经济发展和公众利益。我们必须加快国家网络空间安全保障体系建设, 确保我国的网络空间安全。

人才资源是第一位的资源。因此, 网络空间安全人才培养是我国国家网络空间安全保障体系建设的必备基础和先决条件。网络空间安全学科与专业则是网络空间安全人才培养的基础平台。

1.3 网络空间安全学科的学科内涵

早期传统的信息安全强调信息(数据)本身的安全属性, 认为信息安全主要研究确保信息的以下属性。

秘密性: 信息不被未授权者知晓的属性。

完整性: 信息是正确的、真实的、未被篡改的、完整无缺的属性。

可用性: 信息可以随时正常使用的属性。

信息论的基本观点告诉我们, 信息不能脱离它的载体而孤立存在。因此, 我们不能脱离信息系统而孤立地谈论信息安全。也就是说, 每当我们谈论信息安全时, 一定不能回避信息系统的安全问题。这是因为, 如果信息系统的安全受到危害, 则必然会危害到存在于信息系统之中的信息

的安全。据此, 我们应当从信息系统角度来全面考虑信息安全的内涵。

注意: 这里的信息系统是一般的抽象概念, 它包括所有的具体信息系统。

从纵向来看, 信息系统安全主要包括以下 4 个层面: 设备安全、数据安全、行为安全、内容安全^[4,9-11]。其中, 数据安全即早期的信息安全。信息系统安全的层次结构如图 1 所示。

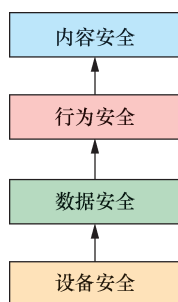


图 1 信息系统安全的层次结构

1) 设备安全: 信息系统设备(硬设备和软设备)的安全是信息系统安全的首要问题。这里包括 3 个侧面。

① 设备的稳定性: 设备在一定时间内不出故障的概率。

② 设备的可靠性: 设备能在一定时间内正确执行任务的概率。

③ 设备的可用性: 设备随时可以正确使用的概率。

2) 数据安全: 采取措施确保数据免受未授权的泄露、篡改和毁坏。

① 数据的秘密性: 数据不被未授权者知晓的属性。

② 数据的完整性: 数据是正确的、真实的、未被篡改的、完整无缺的属性。

③ 数据的可用性: 数据可以随时正常使用的属性。

3) 行为安全: 行为安全从主体行为的过程和结果考察是否会危害信息安全, 或者是否能够确

保信息安全。从行为安全的角度分析和确保信息安全, 符合哲学上实践是检验真理的唯一标准的基本原理。

①行为的秘密性: 行为的过程和结果不能危害数据的秘密性, 必要时行为的过程和结果也应是保密的。

②行为的完整性: 行为的过程和结果不能危害数据的完整性, 行为的过程和结果是预期的。

③行为的可控性: 当行为的过程出现偏离预期时, 能够发现、控制或纠正。

4) 内容安全: 内容安全是信息安全在政治、法律、道德层次上的要求, 是语义层次的安全。

①信息内容在政治上是健康的。

②信息内容符合国家法律法规。

③信息内容符合中华民族优良的道德规范。

根据上面的分析, 要确保信息安全, 就必须确保信息系统的安全, 也就是必须确保信息系统的设备安全、数据安全、行为安全和内容安全。因此, 信息安全包含设备安全、数据安全、行为安全和内容安全 4 个方面的内容。

要确保信息系统安全, 必须综合采取法律、管理、教育、技术多方面的措施, 综合治理。千万不能忽视法律、管理、教育的作用, 许多时候它们的作用大于技术。“七分管理, 三分技术”是信息安全领域的一句行话, 是人们在长期信息安全工作中总结出来的经验。

就确保信息系统安全的技术措施而言, 信息系统的硬件系统安全和操作系统安全是信息系统安全的基础, 密码和网络安全等技术是信息系统安全的关键技术。任何一种信息安全技术, 可能在解决某些信息安全问题方面具有优势, 但是都不可能解决所有信息安全问题。确保信息系统安全是一个系统工程, 只有从信息系统的硬件和软件的底层做起, 从整体上综合采取措施, 才能比较有效地确保信息系统的安全。而且, 任何一种

信息安全技术，只有融入信息系统中，才能发挥实际作用，否则是不能发挥实际作用的。

为了表述简单，在不产生歧义时可以直接将信息系统安全简称为信息安全。实际上，在多数情况下是不会产生歧义的，而且大家已经这样称呼了。

信息论的基本观点告诉我们，信息只有存储、传输和处理 3 种状态。据此，要确保信息安全，就必须确保信息在存储、传输和处理 3 种状态下的安全。

据此，我们给出网络空间安全学科的定义：网络空间安全学科是研究信息存储、信息传输和信息处理中的信息安全保障问题的一门新兴学科。

信息论的基本观点又告诉我们，系统是载体，信息是内涵。据此，网络空间安全的核心内涵仍是信息安全，没有信息安全就没有网络空间安全。

网络空间安全学科是综合计算机、通信、电子、数学、物理、生物、管理、法律和教育等学科，并发展演绎而形成的交叉学科。网络空间安全学科与这些学科既有紧密的联系和渊源，又具有本质的不同，从而构成了一个独立的学科。网络空间安全学科具有自己特有的理论、技术和应用，并服务于信息社会。

网络空间安全学科属于工学。但考虑到网络空间安全学科的多学科交叉性和现阶段我国信息安全专业的实际情况，允许学校给信息安全专业的毕业生授予工学或理学或管理学学士学位^[9]。

目前，我国网络空间安全学科领域的本科专业有信息对抗技术专业、信息安全专业、保密管理专业、网络安全与执法专业、网络空间安全专业。

专业与学科有着密切的关系，但两者又是不同的事物。学科是科学层面的概念，它有明确独立的内涵、研究方向与内容、理论基础和方法论基础。专业是培养本学科领域专业人才的教育组

织实施形式。专业的设置必须遵循以下两点：一是专业的方向与内容要符合本学科的方向与内容；二是专业的设置必须适应社会对人才的需求。因此，一个学科下面允许设置一个或多个专业，专业的名称可以与学科名称相同，也可以与学科名称不同。

下面从信息论角度简单分析信息在存储、传输和处理 3 种状态下的特点，以及它们与信息安全的关系^[12]。

信息在正确的传输状态下，信息形态不发生变化。例如，通信设备发送一个“0”，如果通信是正确的，则接收设备收到的也是一个“0”。信息的形态没有发生变化。如果通信设备发生故障或信道有干扰、遭受到攻击，信息发生错误，则接收设备收到的将是一个错误的“1”。反过来看，如果接收设备接收到的是“0”，它可能是在通信正确的情况下，发送设备发送“0”的正确结果；也可能是在发送设备有故障或信道有干扰、有攻击的情况下，发送设备发送“1”的错误结果。二者必居其一，情况比较简单，这就是著名的二元对称信道模型（BSC）。如图 2 所示，其中 P_c 为正确传输的概率， P_e 为错误传输的概率，且 $P_c + P_e = 1$ 。信息存储的情况与信息传输相同。因此，信息在正确的传输和存储状态下，信息形态不发生变化，情况相对简单。这对我们确保信息安全是有利的。

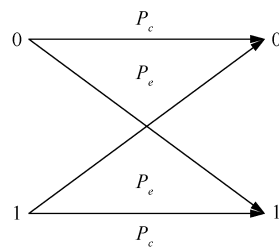


图2 二元对称信道模型

香农（Shannon）提出了利用纠错码和密码确保通信中的数据完整性和保密性的理论和技术。

实践证明, 香农的这一理论和技术是十分成功、有效的。纠错码和密码具有坚实的数学理论基础, 从而成为一门科学。由于信息存储与信息传输的数学模型一致, 即存储本质上也是一种传输。因此, 香农的这一理论和技术用于存储系统也是十分成功、有效的。由此可见, 单纯的信息传输和信息存储的信息安全问题解决得比较好。

与信息在正确的传输和存储状态下信息形态不发生变化不同, 信息在正确的处理状态下信息形态要发生变化。例如, 往运算器 θ 中输入一个“ x ”和一个“ y ”, 如果运算是正确的, 则从运算器输出的是一个“ $x\theta y$ ”。信息的形态发生了变化。反过来看, 情况就复杂了。如果运算器输出的是“ $x\theta y$ ”, 它可能是在运算器无故障和无攻击的条件下, 往运算器 θ 中输入一个“ x ”和一个“ y ”的正确运算结果; 也可能是两个输入中任何一个或运算器发生错误的结果。产生错误的原因可能是故障, 也可能是遭受到攻击。与信息传输相比, 情况复杂得多。因此, 解决信息处理的安全问题比解决信息传输和存储的安全问题更困难。二输入计算模型如图 3 所示。

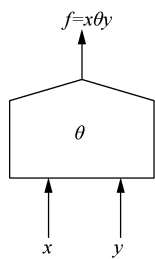


图 3 二输入计算模型

信息处理中信息形态变化, 使其安全问题比传输和存储更复杂。目前许多信息处理安全措施尚处于技术层次, 还没有上升到科学层次, 需要进一步研究和提高。受纠错编码用于数据传输和数据存储十分成功的启发, 许多学者曾研究用于运算器的纠错码, 并且提出了许多方案。这些方案在理论上是正确的。但是, 由于运算器纠错码

的时间消耗会明显降低运算器的效率, 因而至今没有得到广泛应用。后来, 学者又研究同态密码, 希望提高运算的保密性, 这给我们带来了希望。近来, 由于云计算和大数据处理的迫切需求, 同态密码的研究形成热潮。但运算器纠错码的经验教训告诉我们, 安全高效是同态密码成功的关键。

上面从信息的形态是否变化对信息的存储、传输和处理 3 种状态下的信息安全问题做了简单的理论分析, 为深刻理解和解决信息安全问题提供了一种新视角。

必须指出, 由于信息技术的发展和应用的请求, 现在已经很少有单纯的存储、传输和处理系统。现在的信息系统几乎是综合存储、传输和处理的综合系统。例如, 计算机系统中有信息处理, 也有传输和存储; 通信系统中有传输, 也有存储和处理。又因为是系统, 所以存在信息系统的设备、数据、行为、内容 4 层安全问题, 因此安全问题就更加复杂。

重温信息论的基本观点, 哪里有信息哪里就存在信息安全问题, 信息安全是信息的影子。据此可知, 没有信息就没有信息安全问题。又因为信息只有存储、传输和处理 3 种状态, 所以信息安全问题是伴随信息的存储、传输和处理 3 种状态而存在的。没有信息的存储、传输和处理, 就没有信息安全问题。这就告诉我们, 网络空间安全学科是伴随计算机、通信、电子信息等学科共同存在和共同发展的。就信息安全技术而言, 只有融入计算机、通信、存储、电子等信息系统中, 才能发挥实际作用, 否则是不能发挥实际作用的。但是, 由于信息安全问题的广泛性以及学科内涵、研究方向及内容、理论基础和方法论基础的特殊性, 网络空间安全学科是计算机、通信、电子等任何一个学科所不能包含的。因此, 网络空间安全学科是一个一级学科。网络空间安全学科作为一个独立的学科存在和发展, 不仅可对确保我国

网络空间安全发挥重要的作用，而且还可推动计算机、通信、电子等学科加速发展。

2 网络空间安全学科的主要研究方向及研究内容

当前，网络空间安全学科的主要研究方向有密码学、网络安全、系统安全、内容安全与信息对抗^[4,9-11]。可以预计，随着网络空间安全科学技术的发展和应用，一定还会产生新的网络空间安全研究方向，网络空间安全学科的研究内容将更加丰富。

下面分别介绍这5个研究方向的研究内容。

2.1 密码学

密码学由密码编码学和密码分析学组成，其中密码编码学主要研究对明文信息进行编码以实现信息隐蔽，而密码分析学主要研究通过密文获取对应的明文信息^[13-15]。密码学研究密码理论、密码算法、密码协议、密码技术以及密码应用等科学技术问题。其主要研究内容如下。

- ①对称密码。
- ②公钥密码。
- ③Hash 函数。
- ④密码协议。
- ⑤新型密码：生物密码、量子密码、混沌密码等。
- ⑥密钥管理。
- ⑦密码应用。

2.2 网络安全

网络安全的基本思想是，针对不同的应用在网络的不同层次和范围内采取防护措施，以便能够对各种网络安全威胁进行检测发现，并采取相应的响应措施，确保网络设备安全、网络通信链路安全和网络的信息安全。其中，防护、检测和响应都需要基于一定的安全策略和安全机制^[16]。网络安全的研究包括网络安全威胁、网络安全理

论、网络安全技术和网络安全应用等。其主要研究内容如下。

- ①网络安全威胁。
- ②通信安全。
- ③协议安全。
- ④网络防护。
- ⑤入侵检测与态势感知。
- ⑥应急响应与灾难恢复。
- ⑦可信网络。
- ⑧网络安全管理。

2.3 系统安全

这里的系统是指以计算机为中心的各种实际信息系统。而第1.3节中的信息系统是一种抽象的系统，它包含所有的信息系统。两者的区别是明显的。

在以计算机为中心的各种实际信息系统中，有些系统是规模较小的。例如，它可能是一台计算机和一些应用软件。但许多系统是复杂庞大的。例如，电子商务系统、电子政务系统、云计算系统、大数据处理系统等都是复杂庞大的计算机信息系统。

系统是信息的载体，因此系统应当确保存在于其中的信息的安全。系统安全的特点是从系统的底层和整体上考虑信息安全威胁并采取综合防护措施^[17]。它研究系统的安全威胁、系统安全的理论、系统安全的技术和应用。其主要具体研究内容如下。

- ①系统的安全威胁。
- ②系统的设备安全。
- ③系统的硬件子系统安全。
- ④系统的软件子系统安全。
- ⑤访问控制。
- ⑥可信计算。
- ⑦系统安全等级保护。
- ⑧系统安全测评认证。

⑨应用信息系统安全。

2.4 内容安全

信息内容安全简称内容安全。它是信息安全在政治、法律、道德层次上的要求。我们要求信息内容是安全的,即信息内容在政治上是健康的,在法律上是符合我国法律法规的,在道德上是符合中华民族优良的道德规范的。因此,信息内容安全是信息在语义层次上的安全^[18]。

1995年,西方七国信息会议首次提出“数字内容产业”(digital content industry)的概念。我国将“数字内容产业”定义为基于数字化、网络化,利用信息资源创意、制作、开发、分销、交易的产品和服务的产业。显然,数字内容产业需要信息内容安全来保障。若不能确保信息内容的安全,将不能确保数字内容产业的健康发展。

目前学术界对内容安全的认识尚不一致。广义的内容安全既包括信息内容在政治、法律和道德方面的要求,也包括信息内容的保密、知识产权保护、隐私保护等诸多方面。我们这里主要强调内容安全中的基本理论、基本技术和基本应用。其主要研究内容如下。

- ①内容安全的威胁。
- ②内容的获取。
- ③内容的分析与识别。
- ④内容安全管理。
- ⑤信息隐藏。
- ⑥隐私保护。
- ⑦内容安全的法律保障。

2.5 信息对抗

随着计算机网络的迅速发展和广泛应用,信息领域的对抗从电子对抗发展到信息对抗。

信息对抗是从对方信息系统中获取有用信息,削弱、破坏对方信息设备和信息的使用效能,保障己方信息设备和信息正常发挥效能而采取的综合战术、技术措施,其实质是斗争双方利用电

磁波和信息的作用来争夺电磁频谱和信息的有效使用和控制权。

信息对抗研究信息对抗的理论、信息对抗技术和应用。其主要的研究内容如下。

- ①通信对抗。
- ②雷达对抗。
- ③光电对抗。
- ④计算机网络对抗。

3 网络空间安全学科的理论基础

网络空间安全学科是在计算机、通信、电子、数学、物理、生物、法律、管理和教育等学科的基础上交叉融合发展而来的,其理论基础和方法论基础也与这些学科相关,但在学科的形成和发展过程中又丰富和发展了这些理论,从而形成了自己的学科理论基础,特别是具有一些自己独特的理论基础^[4,9-11]。

3.1 数学

数学是一切自然科学的理论基础,当然也是网络空间安全学科的理论基础^[19]。

现代密码可以分为两类:一类是基于数学的密码;另一类是基于非数学的密码。虽然某些基于非数学的密码技术开始走向应用,如基于量子物理的量子密钥分发技术已经走向实际应用。但基于非数学的密码总体上还处在发展的初期阶段。目前广泛实际应用的密码仍然主要是基于数学的密码。

对于基于数学的密码,设计一个密码本质上就是设计一个数学函数,破译一个密码本质上就是求解一个数学难题。这就清晰地阐明了数学是密码学的理论基础。作为密码学理论基础之一的数学主要有代数、数论、概率统计等。

协议是网络的核心,因此协议安全是网络安全的核心。作为网络协议安全理论基础之一的数学主要有逻辑学等。

因为网络空间安全领域的斗争本质上是对抗双方之间的斗争,因此数学中的博弈论(game theory)成为网络空间安全的基础理论之一。

博弈论是现代数学的一个分支,是研究具有对抗或竞争性质行为的理论与方法^[20]。一般称具有对抗或竞争性质的行为为博弈行为。在博弈行为中,参加对抗或竞争的各方各自具有不同的目标或利益,并力图选取对自己最有利的或最合理的方案。博弈论研究的就是博弈行为中对抗各方是否存在最合理的行为方案,以及如何找到这个最合理的方案。博弈论考虑对抗双方的预期行为和实际行为,并研究其优化策略。博弈论的思想古已有之,我国古代的《孙子兵法》不仅是一部军事著作,而且是最早的一部博弈论专著。博弈论已经在经济、军事、体育和商业等领域得到广泛应用。网络空间安全领域的斗争无一不具有这种对抗性或竞争性。例如,网络的攻与防、密码的加密与破译、病毒的制毒与杀毒、信息的隐藏与提取等。因为网络空间安全领域的斗争,本质上都是人与人之间对抗性质的斗争,因此博弈论成为网络空间安全的基础理论之一。遵循博弈论的指导原则,我们将在网络空间安全的斗争中,避免被动,掌握主动,立于不败之地。

3.2 信息论、控制论和系统论

信息论、控制论和系统论是现代科学的理论基础,也是网络空间安全学科的理论基础。

信息论是香农为解决现代通信问题而建立的,控制论是维纳在解决自动控制问题中建立的,系统论是为了解决现代化大科学与工程项目的组织管理问题而建立的。在开始时,它们都是独自形成的独立的科学理论。但由于它们之间具有紧密的联系,因此在后来的应用和发展中互相渗透、互相作用,出现了趋向综合统一、形成统一学科的趋势。这些理论,特别是信息论构成了网络空

间安全学科的理论基础。

信息论对信息源、密钥、加密和密码分析进行了数学分析,用不确定性和唯一解距离来度量密码体制的安全性,阐明了密码体制、完善保密、纯密码、理论保密和实际保密等重要概念,把密码置于坚实的数学基础之上,标志着密码学作为一门独立学科的形成。因此,信息论成为密码学的重要的理论基础之一^[21]。

从信息论角度看,信息隐藏(嵌入)可以理解为在一个宽带信道(原始宿主信号)上用扩频通信技术传输一个窄带信号(隐藏信息)。尽管隐藏信号具有一定的能量,但分布到信道中任意特征上的能量是难以检测的。隐藏信息的检测是一个有噪信道中弱信号的检测问题。因此,信息论构成了信息隐藏的理论基础之一^[22]。

控制论是研究机器、生命社会中控制和通信的一般规律的科学。它研究动态系统在变化的环境条件下如何保持平衡状态或稳定状态。控制论中把“控制”定义为,为了改善受控对象的功能或状态,获取一些信息,并以这种信息为基础施加作用到该对象上。由此可见,控制的基础是信息,信息的获取是为了控制,任何控制又都依赖于信息反馈^[23-24]。

保护、检测、反应策略是确保信息系统安全和网络安全的基本策略。在信息系统和网络系统中,系统的安全状态是系统的平衡状态或稳定状态。恶意软件的入侵打破了这种平衡和稳定。检测到这种入侵便获得了控制的信息,进而杀灭这些恶意软件,使系统恢复安全状态。

系统论是研究系统的一般模式、结构和规律的科学^[25]。系统论的核心思想是整体观念。任何一个系统都是一个有机的整体,不是各个部件的机械组合和简单相加。系统的功能是各部件在孤立状态下所不具有的。系统论的能动性不仅在于认识系统的特点和规律,更重要的是在于利用这

些特点和规律去控制、管理、改造或创建一个系统,使它的存在和发展符合人的需求。

信息安全遵从“木桶原理”,“木桶原理”正是系统论的思想在信息安全领域的体现。

确保信息系统安全是一个系统工程,只有从系统的软硬件底层做起,从整体上综合采取措施,才能比较有效地确保信息系统的安全。这也是系统论的思想在信息安全领域的具体体现。

以上策略和观点经过信息安全的实践检验,证明是正确的,是行之有效的。它们符合控制论和系统论的基本原理。这表明控制论和系统论是信息系统安全和网络安全的理论基础之一。

3.3 计算理论

网络空间安全学科的许多问题是计算安全问题,因此计算理论也是网络空间安全学科的理论基础之一。这里主要包括可计算性理论和计算复杂性理论等。

可计算性理论是研究计算的一般性质的数学理论^[26]。它通过建立计算的数学模型,精确区分哪些问题是可计算的,哪些问题是不可计算的。对于判定问题,可计算性理论研究哪些问题是可判定问题,哪些问题是不可判定问题。

计算复杂性理论使用数学方法对计算中所需的各种资源的耗费做定量的分析,并研究各类问题之间在计算复杂程度上的相互关系和基本性质^[27]。计算复杂性理论是计算理论在可计算性理论之后的又一个重要发展。可计算性理论研究区分哪些问题是可计算的,哪些问题是不可计算的,这里的可计算是理论上的可计算,或原则上的可计算。而计算复杂性理论则进一步研究现实的可计算性,如研究计算一个问题类需要多少时间,多少存储空间。研究哪些问题是现实可计算的,哪些问题虽然是理论可计算的,但因计算复杂性太大而实际上是无法计算的。

众所周知,授权是计算机信息系统访问控制

的核心。计算机信息系统是安全的,其授权系统必须是安全的。可计算性的理论告诉我们:一般意义上,给定的授权系统是否安全这一问题是不可判定问题,但一些“受限”的授权系统的安全问题又是可判定问题^[28]。由此可知,一般操作系统的安全问题是一个不可判定问题,而一些具体的操作系统的安全问题却是可判定问题。又例如,著名的“停机问题”是不可判定问题,而许多具体程序的停机问题却是可判定的。由此可知,一般计算机病毒的检测是不可判定问题,而许多具体软件的计算机病毒检测又是可判定问题。与计算复杂性类似,可判定问题也存在判定复杂性问题。有些问题虽然是理论可判定的,但因判定复杂性太大而实际上是无法判定的。这说明可计算性理论是信息系统安全的理论基础之一。

本质上,密码破译就是求解一个数学难题,如果这个难题是理论不可计算的,则这个密码就是理论上安全的。如果这个难题虽然是理论可计算的,但是由于计算复杂性太大而实际上不可计算,则这个密码就是实际安全的,或计算上安全的。“一次一密”密码是理论上安全的密码,其余的密码都只能是计算上安全的密码。根据计算复杂性理论的研究,NP问题是一类困难计算的问题,NPC问题是NP问题中最难计算的一类问题。公钥密码的构造往往基于一个NPC问题,以使密码是计算上安全的^[8]。例如,McEliece密码基于纠错码的一般译码是NPC问题;背包密码基于求解一般背包问题是NPC问题;多变量密码基于多变量二次非线性方程组的求解问题是NPC问题等。这说明计算复杂性理论是密码学的理论基础之一。

3.4 密码学理论

虽然信息论奠定了密码学的基础。但是,密码学在其发展过程中已经超越了传统信息论,形

成了自己的一些新理论^[14],如单向陷门函数理论、公钥密码理论、零知识证明理论、安全多方计算理论以及部分密码设计与分析理论。

从应用角度看,密码技术是网络空间安全的一种共性技术,许多网络空间安全领域都要应用密码技术。因此,密码学理论是网络空间安全学科的理论基础之一,而且是网络空间安全学科特有的理论基础。

3.5 访问控制理论

访问控制是信息系统安全的核心问题。访问控制的本质是,允许授权者执行某种操作、获得某种资源;不允许非授权者执行某种操作、获得某种资源^[17]。信息系统中的身份认证是一种最基本的访问控制。本质上,许多网络空间安全技术都可看成是访问控制。例如,密码技术也可以看成是一种访问控制。这是因为,在密码技术中密钥就是权限,拥有密钥就可以正确执行相应密码操作并获得需要的信息。没有密钥,就不能正确执行相应密码操作、不能获得需要的信息。只给合法用户分配密钥,不给非法用户分配密钥,就实现了访问控制。

访问控制理论包括访问控制模型及其安全理论。现在已有许多访问控制模型,如矩阵模型、BLP模型、BIBA模型、中国墙模型、基于角色的模型(RBAC)、基于属性的访问控制模型等。

从应用角度看,访问控制技术也是网络空间安全的一种共性技术,许多网络空间安全领域都要应用访问控制技术。因此,访问控制理论是网络空间安全学科的理论基础之一,而且是网络空间安全学科所特有的理论基础。

综上所述,数学、信息论、控制论、系统论、可计算性理论、计算复杂性理论、密码学理论、访问控制理论等是网络空间安全学科的理论基础。

4 网络空间安全学科的方法论基础

4.1 方法论的概念

笛卡尔在1637年出版了著作《方法论》,研究论述了解决问题的方法,对人类的思维方式和科学研究方法产生了极大的影响。笛卡尔在书中把研究的方法划分为4步。

1) 永不接受任何自己不清楚的真理。对自己不清楚的东西,不管是什么权威的结论,都可以怀疑。

2) 将要研究的复杂问题,尽量分解为多个比较简单的小问题,一个一个地解决。

3) 将这些小问题从简单到复杂排序,先从容易解决的问题入手。

4) 将所有问题解决后,再综合起来检验,看是否完全,是否将问题彻底解决了。

按不同层次,方法论分为哲学方法论、一般科学方法论和具体科学方法论。其中,研究认识世界、改造世界最一般的方法论是哲学方法论;研究各科学门类,具有一定普遍意义、适用于各科学门类的方法论是一般科学方法论;研究某一具体科学,涉及这一具体科学的方法论是具体科学方法论。三者之间的关系是相互依存,互相影响,互相补充的对立统一的关系。哲学方法论在一定意义上具有决定性作用,是最一般的方法论,对一般科学方法论和具体科学方法论具有指导意义^[29-30]。

笛卡尔的方法论强调了把复杂问题分解成一些细小的问题分别解决,是一种分而治之的思想。但是它忽视了各个部分的关联和彼此影响。近代科学的发展使科学家发现,许多复杂问题无法分解,或分解后的细小问题的性质之和并不能反映原问题的性质,因此必须用整体的思想和方法来处理,由此导致系统工程的出现。方法论由传统的方法论发展到系统性的方法论。系统工程的出

现推动了环境科学、气象学、生物学、人工智能和软件工程的快速发展。

4.2 网络空间安全学科的方法论基础

网络空间安全保障体系是由信息基础设施、安全防御体系、技术规范与标准、法律法规和组织管理等组成。而网络空间安全保障体系的实施必须以人为核心,这就成为一个复杂的巨系统。因此,解决网络空间安全领域的问题必须遵循一套科学的方法论,否则是不行的。人们在网络空间安全保障的长期实践中逐渐形成了自己的方法论^[9]。

网络空间安全学科的方法论是,以解决网络空间安全问题为目标、以适应网络空间安全需求为特征的具体科学方法论。它既包含分而治之的传统方法论,又包含综合治理的系统工程方法论,而且将这两者有机地融合为一体。网络空间安全学科的方法论与数学或计算机科学与技术等学科的方法论既有联系又有区别。具体概括为以下4个步骤。

- 1) 理论分析。
- 2) 逆向分析。
- 3) 实验验证。
- 4) 技术实现。

其中,逆向分析是网络空间安全学科所特有的方法论。这是因为网络空间安全领域的斗争,本质上都是攻防双方的斗争。网络空间安全学科的每一分支都具有攻和防两个方面,因此必须从攻和防两个方面进行分析研究。例如,密码设计必须遵循公开设计原则,即假设对手知道密码算法、掌握足够的明密文数据资源、拥有足够的计算资源,在这样的条件下仍要确保密码是安全的。这就要求我们在进行密码设计时,必须了解密码破译的理论和技術,否则就无法设计出安全的密码。反过来,在进行密码破译时,必须了解密码设计的理论和技術,否则就无法有效破译密码。

在进行信息系统安全和网络安全设计时,首先要进行安全威胁分析和风险评估,必须了解系统攻击和网络攻击的技術和方法,否则就无法设计出安全的信息系统和安全的网络系统。这些做法就是逆向分析方法论的具体应用,并且已被实践证明是正确的和有效的。

在运用网络空间安全学科的方法论分析和解决网络空间安全问题时,这4个步骤既可以独立运用,也可以结合运用。通常需要循环往复多次,才能较好地解决网络空间安全问题。

在运用网络空间安全学科的方法论分析和解决网络空间安全问题时,还应当注意以下几点。

1) 坚持“以人为核心”。这是因为,网络空间安全领域的对抗,本质上是人与人之间的对抗。毛泽东主席曾经指出:“武器是战争的重要因素,但不是决定因素,决定的因素是人不是物”。因此,不考虑人的因素,是不可能有效解决网络空间安全问题的。例如,当人们用一个杀病毒软件去查杀一个病毒时,表面上是杀病毒软件与病毒软件之间的斗争,但实际上是编写杀病毒软件的人与编写病毒软件的人之间的斗争。

众所周知,在确保网络空间安全的工作中,人是最积极的因素。但同时必须指出,人也是一个薄弱因素。这是因为人是有思想和情感的、人是会疲劳的。许多网络空间安全事件都是由于人的思想出了问题而造成的。因此,对人进行有效的政治思想教育和管理,是十分必要的。

2) 强调底层性和系统性。即从系统的软硬件底层和系统整体上分析信息安全问题,从系统的软硬件底层和系统整体上综合采取措施来解决信息安全问题。

3) 实行综合治理。这是因为网络空间安全学科是多学科交叉融合形成的交叉学科,网络空间安全问题大都涉及多方面的问题,而且信息系统具有设备安全、数据安全、行为安全和内容安全

多层次的安全问题。因此,必须综合采取法律、管理、教育、技术多方面的措施,综合治理,才能较好地解决网络空间安全问题。千万不能忽视法律、管理、教育的作用,许多时候它们的作用大于技术。“七分管理,三分技术”是信息安全领域的一句行话,这是人们在长期的信息安全工作中总结出来的经验。就技术措施而言,每一种信息安全技术都有自己的优势,同时也有自己的弱势,没有一种信息安全技术能够解决所有信息安全问题。而且,任何一种信息安全技术,只有融入信息系统中,才能发挥实际作用,否则是不能发挥实际作用的。因此,综合采用多种信息安全技术,将其融入信息系统中,共同发挥最大实际效能,是解决信息安全问题的有效方法。

综上所述,我们应当遵循网络空间安全学科的方法论,坚持“以人为核心”,强调底层性和系统性,实行综合治理。在解决具体网络空间安全问题时,坚持理论联系实际,运用定性分析与定量分析相结合、注意量变会引发质变、局部治理与综合治理相结合、追求整体效能。只有这样,才能较好地解决网络空间安全中的理论、技术和应用问题。

本文是作者在制定我国信息安全专业规范(第二版)的过程中形成的,其草稿得到许多教师的阅读和帮助。作者向阅读过本文草稿和帮助过作者的教师致谢!

参考文献:

- [1] 中国科学院信息领域战略研究组.《中国至2050年信息科技发展路线图》[M].北京:科学出版社,2009.
Strategic research group in the field of information. Chinese academy of sciences. Information science & technology in China: a Roadmap to 2050 [M]. Beijing: Science Press, 2009.
- [2] 李国杰.信息科学技术的长期发展趋势和我国的战略取向[J].中国科学:信息科学,2010,40(1):128-138.
LI G J. The strategic orientation of 21 century development of science and technology information[J]. Scientia Sinica Informations, 2010, 40(1): 128-138.
- [3] GIBSOB W. Burning chrome[M]. Harper Crollins UK,1982.
- [4] 张焕国,韩文报,来学嘉,等.网络空间安全综述[J].中国科学:信息科学,2016,46(2):125-164.
ZHANG H G, HAN W B, LAI X J, et al. Survey on cyberspace security[J]. Scientia Sinica Informations, 2016, 46(2):125-164.
- [5] ZHANG H G, HAN W B, LAI X J, et al. Survey of Syberspace Security[J]. Science China: Information Sciences, 2015, 58(11): 43.
- [6] 沈昌祥,张焕国,冯登国,等.信息安全综述[J].中国科学(E集:信息科学),2007,37(2):129-150.
SHEN C X, ZHANG H G, FENG D G, et al. Information security review [J]. Science in China(Series E: Information Sciences), 2007, 37(2):129-150.
- [7] SHEN C X, ZHANG H G, FENG D G, et al. Survey of information security[J]. Science in China Series F, 2007, 50(3): 273-298.
- [8] 张焕国,王后珍,杨昌,等.抗量子计算密码[M].北京:清华大学出版社,2015.
ZHANG H G, WANG H Z, YANG C, et al. Post quantum cryptography[M]. Beijing: Tsinghua University Press, 2015.
- [9] 信息安全类专业教学指导委员会信息安全专业规范项目组.信息安全专业指导性专业规范[M].北京:清华大学出版社,2014.
Information security professional instruction committee information security professional speciation project group. Information security majority instructive specication[M]. Beijing: Tsinghua University Press, 2014.
- [10] 张焕国,王丽娜,杜瑞颖,等.信息安全学科体系结构研究[J].武汉大学学报理学版,2010,56:614-620.
ZHANG H G, WANG L N, DU R Y, et al. Information security discipline system structure research[J]. Journal Wuhan University, 2010, 56: 614-620.
- [11] 张焕国,杜瑞颖,傅建明,等.论信息安全学科[J].网络安全,2014,56:619-620.
ZHANG H G, WANG L N, DU R Y, et al. Information security discipline system structure research[J]. Network Security, 2010, 56: 614-620
- [12] 张焕国,赵波,王骞,等.可信云计算基础设施关键技术[M].北京:机械工业出版社,2019.
ZHANG H G, ZHAO B, WANG Q, et al. Trusted cloud computing infrastructure[M]. Beijing: China Machine Press,2019.
- [13] SHANNON C E. A mathematical theory of communication [J]. Bell System Technical Journal, 1948, 27(4): 623-656..
- [14] SHANNON C E. Communication theory of secrecy system[J]. Bell System Technical Journal, 1949, 28(4): 656-715.
- [15] 张焕国,唐明.密码学引论(第三版)[M].武汉:武汉大学出版社,2009.
ZHANG H G,TANG M. Introduction to cryptography(third edition)[M]. Wuhan: Wuhan University Press, 2009.
- [16] 刘建伟,王育民,网络安全——技术与实践(第三版)[M].北京:清华大学出版社,2017.
LIU J W, WANG Y M. Network security technology and practice (third edition)[M]. Beijing: Tsinghua University Press, 2017.
- [17] 石文昌,梁朝晖.信息系统安全概论[M].北京:电子工业出版社,2008.
SHI W C, LIANG Z H. Introduction to information system security[M]. Beijing: Publishing House of Electronic Industry, 2008.
- [18] 周学广,任延珍.信息内容安全[M].武汉:武汉大学出版社,

2012.
ZHOU X G, REN Y Z. Information content security[M]. Wuhan: Wuhan University Press, 2012.
- [19] 覃中平, 张焕国, 乔秦宝, 等. 信息安全数学基础[M]. 北京: 清华大学出版社, 2006.
QIN Z P, ZHANG H G, QIAO Q B, et al. Mathematical basis of information security[M]. Beijing: Tsinghua University Press, 2006.
- [20] 张维迎. 博弈论与信息经济学[M]. 上海: 上海人民出版社, 2004.
ZHANG W Y. Game theory and information economics[M]. Shanghai: Shanghai People's Publishing house, 2004.
- [21] 王育民, 李晖, 梁传甲. 信息论与编码理论[M]. 北京: 高等教育出版社, 2005.
WANG Y M, LI H, LIANG C J. Information theory and coding theory [M]. Beijing: Higher Education Press, 2005.
- [22] 王育民, 张彤, 黄继武. 信息隐藏——理论与技术[M]. 北京: 清华大学出版社, 2006.
WANG Y M, ZHANG T, HUANG J W. Information hiding —— theory and technology[M]. Beijing: Tsinghua University Press, 2006.
- [23] WIENER N. Cybernetics or control and communication in the animal and the machine[M]. New York: Wiley, 1948.
- [24] 维纳. 控制论(或关于在动物和机器中控制和通信的科学)(第二版) [M]. 北京: 科学出版社, 2009.
WIENER. Cybernetics (or the science of control and communication in animals and machines) (2nd edition)[M]. Beijing: Science Press, 2009.
- [25] 李喜先. 工程系统论[M]. 北京: 科学出版社, 2007.
LI X X. Engineering systems theory[M]. Beijing: Science Press, 2007.
- [26] 杨东屏. 可计算理论[M]. 北京: 科学出版社, 1999.
YANG D P. Computability theory [M]. Beijing: Science Press, 1999.
- [27] 陈志东, 徐宗本. 计算数学-计算复杂性理论与 NPC/NP 难问题求解[M]. 北京: 科学出版社, 2001.
CHEN Z D, XU Z B. Computational mathematics-computational complexity theory and solving NPC/NP hard problems [M]. Beijing: Science Press, 2001.
- [28] 周锡龄. 计算机数据安全原理[M]. 上海: 上海交通大学出版社, 1987.
ZHOU X L. Principles of computer data security [M]. Shanghai: Shanghai Jiaotong University Press, 1987.
- [29] 张伟刚. 科研方法论[M]. 天津: 天津大学出版社, 2006.
ZHANG W G. Research methodology[M]. Tianjin: Tianjin University Press, 2006.
- [30] 金观涛. 控制论与科学方法论[M]. 北京: 新星出版社, 2005.
JIN G T. Cybernetics and scientific methodology [M]. Beijing: Xinxing Press, 2005.

[作者简介]



张焕国 (1945—), 男, 河北保定人, 武汉大学教授、博士生导师, 主要研究方向为信息安全、密码学、可信计算和容错计算。



杜瑞颖 (1964—), 女, 河南新乡人, 博士, 武汉大学教授、博士生导师, 主要研究方向为网络安全、隐私保护。