国家级特色专业立项教材
国家重点研发计划资助出版

网络空间安全原理、技术与工程

◎ 闫怀志　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国家级特色专业立项教材
国家重点研发计划资助出版

网络空间安全原理、技术与工程

闫怀志　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书以重视理论基础、加强理论与工程交叉为指导原则，以培养“网络空间安全保障体系”构建能力为目标，围绕网络空间安全的理论、技术和工程三方面，系统、全面地介绍网络空间安全领域知识和最新研究进展。

全书共 14 章，分为 3 部分。原理部分主要包括网络空间安全概述、网络空间安全体系基本概念、现代密码体制和认证技术等；技术部分包括传统防火墙和下一代防火墙、入侵检测和入侵防护、安全漏洞和恶意代码、网络安全协议、信任管理和可信计算、网络内容安全和舆情监控等；工程部分讲述信息安全风险评估和安全测评，存储备份和灾难恢复、软件安全性和软件安全工程，信息安全管理、法律法规和标准体系，网络空间典型信息系统的安全防护与测评等内容。网络空间安全原理、技术与工程这三个层次的内容相互联系、融合和支撑，构成了完整的网络空间安全知识结构体系。

除讨论传统信息系统安全外，本书重点论述物联网、云计算、三网融合、工业控制系统和网络等新兴领域的信息安全保障问题，既让读者把握本领域的基础知识和核心技能，又充分反映本领域的技术前沿和发展趋势。

本书可作为高校网络空间安全、信息安全、信息对抗、信息工程以及计算机技术、软件工程类专业高年级本科生和研究生的教材和教学参考用书，也可作为相关培训教材，还可供相关技术和管理人员参考。

图书在版编目（CIP）数据

网络空间安全原理、技术与工程 / 闫怀志编著. —北京：电子工业出版社，2017.7

ISBN 978-7-121-30776-8

Ⅰ. ① 网… Ⅱ. ① 闫… Ⅲ. ① 计算机网络－信息安全 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字（2016）第 322896 号

策划编辑：章海涛
责任编辑：章海涛　　特约编辑：邢　颖　张　玉
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：21.75　字数：600 千字
版　　次：2017 年 7 月第 1 版
印　　次：2017 年 7 月第 1 次印刷
定　　价：49.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：192910558（QQ 群）。

前　言

信息技术在人类生产生活中日益发挥着至关重要的作用，信息作为一种战略资源，其安全问题也成为了关系国家安全、经济发展和社会稳定的战略性问题。国际上，围绕夺取“信息控制权”的斗争愈演愈烈，各国政府、学术界及产业界都对网络空间安全高度重视，在相关基础理论、关键技术及工程实施方面大力投入，取得了丰硕的成果；同时，网络空间安全事关国家主权和国家安全，作为国家安全的重要组成部分，持续并深刻影响着国家的政治安全、军事安全、经济安全、文化安全等方面。为了保证网络空间安全，必须坚持“自主可控”的原则，建立健全完善的网络空间安全保障体系。2017年6月1日起实施的《中华人民共和国网络安全法》更是在法律层面对此做出了明确要求。

与其他行业相比，网络空间安全行业具有鲜明的知识密集型特点。网络空间安全是攻防双方的高技术博弈与对抗，究其本质是人与人之间的对抗。因此，网络空间安全行业发展中的一切问题归根结底都是人才问题。解决网络空间安全人才问题的关键又在于高层次创新型人才的培养。国家教育部明确指出，“不断加强信息安全学科、专业建设，尽快培养高素质的网络空间安全人才队伍，成为我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。”《中华人民共和国网络安全法》对网络空间安全学科的建设和人才培养提出了更高要求。

近年来，为适应国家和社会对网络空间安全人才的迫切需求，国内近百所高校（特别是全国重点高校）依托不同的学科背景，设置了信息安全/网络空间安全类专业，还有更多的高校开设了网络空间安全方向的课程。2015年，我国适时设立了“网络空间安全”一级学科。随着对网络空间安全学科认识的不断深入，并经过多轮人才培养实践检验，业界越来越深刻地意识到，网络空间安全人才培养的关键在于抓住课程体系和教材建设这个“纲”。在构建面向层次化需求的网络空间安全学科课程体系的同时，编写定位准确、特色鲜明的适用教材成为网络空间安全人才培养的当务之急。

从学科的角度来讲，网络空间安全是综合数学、通信、计算机、电子、物理、管理、法律和教育等学科，发展演绎而形成的新兴交叉学科。网络空间安全学科与上述各学科既联系紧密，又有本质区别，它以网络空间安全主体、客体及其相互作用构成的复杂动力系统为对象，以数学、信息SCI论（即信息论、控制论和系统论）、计算理论为理论基础，以系统工程观点和复杂系统理论为方法论，主要研究信息获取、信息存储、信息传输和信息处理中的安全威胁和安全保障问题，形成了自己的理论、技术和工程应用体系，从而构成了一个相对独立的新兴学科，内容涵盖原理、技术与工程三个基本层次。

本书在深刻领会教育部教改精神的基础上，结合“卓越工程师教育培养计划”，以重视理论基础、加强理论与工程交叉为指导原则，根据培养学生“构建网络空间安全保障体系”的

能力这条主线，围绕网络空间安全理论、技术和工程三方面组织知识点和技能点，借鉴国内外的先进教学理念和知识框架，结合实际教学需求，开发了新的教学内容和教学组织方法，着力培养学生的系统思维和创新意识。考虑到网络空间安全学科自身在不断地发展变化，所以本书力求既让读者把握本领域的基础知识和核心技能，又充分反映本领域的前沿技术，实现先进性和成熟性的统一。在教学实践中，教师可根据不同专业课程设置需求以及自身办学特色来选取教学内容。

全书共14章，分为3部分，以原理、技术与工程为主线，系统、全面地介绍网络空间安全领域知识。原理部分介绍网络空间安全的基本原理，涉及网络空间安全学科理论基础和方法论基础，这是一切网络空间安全技术与工程共同需要的理论基础，具体内容主要包括网络空间安全概述和网络空间安全体系基本概念、现代密码体制与认证技术等。技术部分包括传统防火墙和下一代防火墙、入侵检测和入侵防护、安全漏洞和恶意代码、网络安全协议、信任管理和可信计算、网络内容安全和舆情监控等。工程部分讲述信息安全风险评估和安全测评，存储备份和灾难恢复，软件安全性和软件安全工程，信息安全管理、法律法规和标准体系，网络空间典型信息系统的安全防护与测评等。网络空间安全原理、技术与工程这三个层次的内容相互联系、融合和支撑，构成了完整的网络空间安全知识结构体系。

除了讨论传统信息系统安全外，本书还将重点论述物联网、云计算、三网融合、工业控制系统和网络等新兴领域的信息安全保障问题。

本书为教育部高等学校国家级特色专业建设、研究生教育研究课题（教改项目）立项项目，同时得到了国防特色紧缺专业建设项目的支持，并受国家重点研发计划项目资助。北京理工大学将本书列为“重点规划教材”，电子工业出版社对本书的出版给予了大力支持。书稿曾经数年多轮试用，这次成书吸收了同行和学生提出的诸多宝贵意见和建议。本书编写过程中，得到了北京大学、清华大学、中国科学院大学、上海交通大学、北京航空航天大学、北京理工大学、武汉大学、中国科学院信息工程研究所、中国航天第710研究所、公安部第一研究所、中国信息安全测评中心、国家信息中心等单位同行专家的大力帮助和支持。本书在编写过程中参阅了大量的国内外专著、教材、论文和网络资料，在此一并致谢。如有引用未能尽录，请联系作者再版补救。

在本书的编写过程中，曾佳、卢道英、闫振民、曾永岐、边霞等人做了大量文字校对工作，一并致谢！

本书可作为高校网络空间安全、信息安全、信息对抗、信息工程以及计算机技术、软件工程类专业高年级本科生和研究生的教材和教学参考用书，也可作为相关培训教材，还可供相关技术与管理人员参考。

由于作者水平有限，虽已尽力避免不足，难免仍有疏漏，恳请广大读者将意见和建议发至yhzhi@bit.edu.cn，不胜感激。

作　者

目　录

第 1 章　网络空间安全概述

信息、信息系统与人类社会的发展相伴相生，它们的安全问题也由来已久。信息技术发展到今天，网络和计算机成为了信息系统最重要的载体，网络空间也已经成为人类社会发展的新支柱和国家安全的新领域。网络空间的国际战略竞争日趋激烈，其安全对抗程度也在不断增强，网络空间安全已经成为国家安全的核心内容之一。本章将结合网络空间安全的技术架构来介绍网络空间安全的基本范畴，具体内容包括信息、信息系统、网络空间及网络空间安全的基本概念，涉及网络空间安全原理、技术与工程之间的关系、网络空间安全的知识体系等。

1.1　信息

信息（Information）是自然与人类社会普遍存在的现象，无处不在、无时不有，在自然和人类生活各领域中的应用非常广泛。信息既存于自然界，也存于人类社会；既可以来自物质世界，也可以来自精神领域。人类很早就实现了信息的记录、存储和传输，上古“结绳记事”就是用麻绳和筹码作为信息载体来记录和存储信息。虽然发展到现代社会，信息的内涵和外延变得十分丰富，并在人类社会的生产生活中扮演着重要角色，可以从不同角度去理解和利用，但是目前尚无一个通用的定义。在自然与人类社会中，信息是与物质、能量并列的三大要素之一，是社会生产力出现飞跃的新质。人们从信息的本质、用途和表示等方面给出了不同的定义，这些定义因信息的发展阶段、研究领域而各有不同。本节将重点讨论与信息相关的基本概念。

1.1.1　系统论、控制论、信息论与信息

人类社会很早就产生了信息的概念，但在我们所关注的科学技术领域，信息最早见于 1928 年美国贝尔电话实验室哈特莱（R. V. Hartley）发表的《信息传输》一文，文中给出了“信息是指有新内容、新知识的消息”的观点，并首次提出“信息定量化”的基本思想，采用对数来度量信息，将一条信息包含的信息量定义为它可能取值个数的对数。哈特莱由此开启了现代信息论的研究，这是人类对信息的理解和表达具有现代意义的开端。经过近百年的发展，信息至今已成为自然科学和社会科学的主要研究对象。特别是自 20 世纪 70 年代以来，微电子技术革命为信息的数字化表达和建构提供了崭新的手段，信息和信息系统具有了新的内涵，从而引发了一场信息革命，人类开始进入真正的信息社会。信息社会是继农业社会、工业社会之后的第三次伟大的科技革命与社会变革，系统论、控制论和信息论成为信息社会最为基础的理论体系。

系统论创始人美籍奥地利理论生物学家和哲学家贝塔朗菲（Ludwig Von Bertalanffy）早在 20 世纪上半叶就提出了系统论的思想，但直到 60～70 年代才受到人们的重视。系统论认为，系统是由若干相互联系的基本要素构成的、具有确定的特性和功能的有机整体，其研究对象

是系统的模式、性能、行为和规律，这种思想为人们认识各种系统的组成、结构、性能、行为和发展规律提供了一般方法论的指导。信息在系统论中被认为是系统内部联系的特殊形式，系统论考察的是物质、能量、信息的交换、流动，以及系统的状态、内部结构的分布随时间的变化规律。

1948 年，美国应用数学家诺伯特·维纳（Norbert Wiener）发表了专著《控制论—关于在动物和机器中控制和通信的科学》（*Cybernetics or Control and Communication in the Animal and the Machines*），开创了控制论学科，研究的是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的一般规律，其思想和方法至今被几乎所有的自然科学和社会科学领域所广泛采用。所谓控制，是指为“改善”某个或某些受控对象的功能或发展，需要获得并使用信息，基于这种信息选出的施加于该对象上的作用。因此可以说，控制的根基是信息，一切信息传递的目的都是为了实现控制，任何控制又都需要依赖信息反馈来实现。这里的信息反馈是指由控制系统输出信息，又将其作用结果返回，以影响信息的再输出，制约系统行为以达到预定目的。需要注意的是，尽管一般系统具有质量、能量和信息三要素，但控制论仅研究系统的信息变换和控制过程，即着眼于信息来研究系统的行为方式，而不关注系统质量和能量的变化。因此，维纳将信息描述为“人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容和名称”。

20 世纪 40 年代，信息论也获得了重要进展，信息自此成为一个科学概念，被广泛应用于自然科学和社会科学的诸多领域。时任贝尔实验室研究员的美国数学家香农（Claude E Shannon）相继发表了《通信的数学理论》（*A Mathematical Theory of Communication*，1948 年）、《噪声下的通信》（*Communication in the Presence of Noise*，1949 年）两篇论文，由此奠定了现代信息论的基础（后人称之为香农信息论）。香农将信息描述为“用来消除不确定性的东西”，也就是说，以“确定接收者因接收到消息而消除的对信息源所存的疑义（不定度）”来度量信息所含的信息量。如果将信息视为随机事件，则可以运用概率来实现其不确定性的测度。香农提出了通信系统的整套数学理论，特别是创造性地采用概率论来研究信息传导问题，进一步对信息赋予科学的定量描述，从而创立了信息论。后人在此基础上采用数理统计方法来研究信息的度量、传递和变换规律，通过研究通信和控制系统中普遍存在的信息传递的共同规律以及研究信息的获取、度量、变换、存储和传递等问题的最优方案，发展成为成熟的现代信息论。香农提出的通信模型更是为信息等一般概念的界定奠定了基础。在现代信息论中，信息被视为可以获得、变换、传递、存储、处理、识别和利用的一般对象。到目前为止，信息论早已成为现代通信系统发展的核心基础理论，而不断发展完善的通信系统理论也已经成为现代信息技术最重要的基础理论之一。

20 世纪 40 年代末，随着科学技术的发展，各科学研究领域不断分化同时彼此渗透，几乎同时应运而生的系统论、控制论、信息论这三门边缘学科对科学技术和思维的发展起到了巨大的推动作用，为多门现代学科的出现奠定了坚实的基础，现代科学技术的基本理论体系都是以信息为核心或重要内容的。这三大理论特别是信息论也是网络空间安全学科的方法论基础。比如，网络空间安全保障是一项系统工程，系统论是系统工程的理论基础；信息安全动态防御和主动防御策略，体现了控制论的基本思想；信息论则奠定了信息保密学和信息隐藏学的基础，密码学和信息隐藏学的发展都属于信息论范畴。

1.1.2　信息的定义及其基本特征

要研究信息的安全问题，必须首先搞清楚信息的概念及其基本特征。下面将介绍信息的定义、信息的基本特征以及数据、信息与知识的区别和联系。

1. 信息的定义

“信息”作为信息学科中最重要、最基本的概念，被广泛应用于自然科学和社会科学的诸多领域，成为哲学、信息论、系统论、控制论、管理学等诸多学科（特别是技术科学中）共同探讨和使用的重要概念之一。与此同时，各学科领域基于自己认识世界和具体研究的需要，对“信息”的概念和定义的认识又多种多样，这个问题不但是学术界长期争论的焦点，而且至今尚未达成统一认识。这种争论的原因在于，“信息”一词应用的场合不同，其含义也不相同。

从技术科学的角度来讲，信息作为研究对象内部结构与外部联系运动的状态与方式，究其本质，它是物质的一种本质属性，可以脱离原来的研究对象而被获取、传输、处理和利用。也就是说，信息是从记录客观事物（物质和精神）的运动状态和方式（状态改变）的数据中提取出来的、对人们的决策提供有益帮助的一种特定形式的数据。信息的外延广泛，自然信息反映的是自然界各种事物状态和运动规律；社会信息反映的是人类社会各种事物状态和运动规律。

2. 信息的基本特征

信息主要具有可识别性、可传载性、可共享性、可度量性等基本特征。

① 可识别性。首先，信息应该是可以识别的，又可分为直接识别和间接识别两种方式。直接识别是指通过生物感官（如听觉、嗅觉、视觉、味觉等）来识别，间接识别是指通过各种测试手段来识别，如使用压力计来识别压力、使用 GPS 来识别位置、使用网络流量计来识别网络流量等。在对不同的信息源进行识别时，可以使用对应的传感装置来实现不同的识别方法。在信息安全领域，可识别性多针对的是可间接识别的对象。

② 可传载性，又称为可存储性。信息本身只是一些抽象符号，必须借助各种方法（即媒介或载体）才能实现存储。常见的信息表现形式可以是语音、文字、图像、视频等，媒介或载体则可以是磁盘、声波、电波、光波等，从而实现处理和存储。存储媒介或载体并不是信息本身，如光盘上的数据，认知主体首先接触到的是光盘本身，然后才能通过光盘读取设备来感知光盘上所存储的数据信息。

③ 可共享性。我们常说“物质不灭”、“能量守恒”，而信息不满足“此得彼失”这个规律。信息作为可以脱离源事物相对独立地存在的一种资源，可被无限制地进行大量复制、长期保存、重复使用，供不同个体或群体在同一时间或不同时间享有。信息与物质和能量的这种显著区别给使用者带来的极大方便，也给信息安全带来了极大隐患。比如，攻击者通过非法手段复制获得信息后，信息所有者可能毫无察觉。

④ 可度量性。信息可采用某种测度或度量单位进行度量，并实现信息编码。香农采用了信息熵的概念来表征信源的不确定性，解决了信息的量化度量问题，而常用的二进制、十进制等数制其实就是一种简单的信息编码。

此外，信息还具有可压缩性、可转换性、可处理性、可利用性等特征。

1.1.3 数据、信息与知识的区别和联系

在信息技术领域，人们经常会遇到数据、信息与知识这三个术语，它们之间既有联系、又有区别，往往难以区分。

数据（Data）是载荷或记录信息的按照一定规则排列组合的物理符号，它是人们从自然现象和社会现象中搜集的原始材料，根据使用数据人的目的按一定的形式加以处理，实现对客观事物的数量、属性、位置及其相互关系的抽象表示，以适合用自然方式或人工方式进行存储、传递和处理，具有真实性、客观性的特点。数据既可以是数字、文字、图像，也可以是声音或程序代码等。例如，一个文件大小是 15 MB、网页响应时间是 0.5 s、程序代码是 500 行、应用服务器是 5 台、信息安全等级保护是 3 级等，其中的数据包括“文件大小”、“15 MB”、“网页响应时间”、“0.5 s”等原始材料，通过这些数据的描述，人们可以在大脑中形成对计算机网络这个客观世界的清晰印象。这些数据也可以通过编码被录入到计算机中。

信息是数据载荷的内容，是具有时效性的、有一定含义的、有逻辑的、经过加工处理的、对决策有价值的数据流，具有针对性、时效性、减少不确定性的特点。同一信息的数据表现形式可以多种多样，如某个文件大小是 1 MB，也可以表示为 1024 B。将“文件大小”与“1 MB”这两个数据关联处理成“文件大小是 1 MB”就构成了有用的信息。信息必然来源于数据，并且其抽象程度要高于数据本身。经过处理的数据可以更好地用于解释，只有经过关联和解释，数据才有意义，才称为信息。可以说，信息是经过加工后并对客观世界产生影响的数据。

知识是反映各种事物的信息经过信息接收者的提炼和推理而获得的正确结论，是人通过信息对自然界、人类社会以及思维方式与运动规律的认识和掌握，是人的大脑通过思维重新组合的、系统化的信息集合，具有规律性、本质性、系统性的特点。知识是由信息形成的，通过人们的参与，对信息进行归纳、演绎、比较等手段进行挖掘，使其有价值的部分沉淀下来，并于已存在的人类知识体系相结合，这部分有价值的信息就转变成了知识。例如，正常的网络 TCP 连接是三次握手，而 Syn 洪水攻击的 TCP 连接无法实现三次握手，出现大量的无效 Syn 连接请求。当安全研究人员对这些信息进行归纳和对比就会发现，实现三次握手的多是正常连接，大量的无效 Syn 连接请求可能代表出现了 Syn 洪水攻击，于是总结出网络是否遭受攻击的判断信息。因此，知识是沉淀并与已有人类知识库进行结构化的有价值信息。

所以，从性质上来说，数据、信息和知识都是社会生产活动中的一种基础性资源；从形态上来说，三者都可以采用数字、文字、符号、图形、声音、影视等表示。数据是信息加工处理的原材料，信息则是知识加工处理的原材料，因此从涵盖范围上来说，从大到小依次是数据、信息和知识。

1.2 信息系统

1.2.1 信息系统的概念与形态

信息论的基本原理告诉我们，信息不能脱离其载体而独立存在，这种载体就是信息系统。换言之，信息系统是获取、存储、传输和处理信息的载体。前面已经介绍，系统是由若干相互联系的基本要素构成的、具有确定的特性和功能的有机整体，那么信息系统可以被定义为：按一定结构组织的可以获取（收集）、存储、传输、处理和输出信息，以实现其目标的相互关联的元素和子系统的集合。