网络空间安全专业规划教材

总主编◎杨义先　　执行主编◎李小勇

网络空间安全基础

Fundamentals of Cyberspace Security

彭海朋　编著

北京邮电大学出版社
www.buptpress.com

网络空间安全专业规划教材

总主编　杨义先　　执行主编　李小勇

网络空间安全基础

彭海朋　编著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

本书是网络空间安全学科的基础教材，围绕网络空间安全学科的主要研究方向及网络空间安全基础理论和密码学及应用两部分内容合理组织知识结构，其中第2章（基础知识）、第4章（大数据安全）、第5章（复杂网络安全）、第6章（网络安全博弈）、第7章（虚拟资产安全）和第8章（安全通论）等内容对应于网络空间安全基础理论的主要研究方向及内容，第3章（新型密码技术）则对应于密码学及应用。本书立足于网络空间安全的基本知识，并竭力把握好知识的深度和广度，为网络空间安全学科的后续课程及后续研究奠定一定的知识基础。

本书适合作为网络空间安全、信息安全、网络工程等相关专业本科、研究生的专业基础教材，也可作为计算机科学与技术、软件工程、电子商务等专业的选修教材。

图书在版编目(CIP)数据

网络空间安全基础 / 彭海朋编著. -- 北京 : 北京邮电大学出版社, 2017.8
ISBN 978-7-5635-5091-3

Ⅰ.①网… Ⅱ.①彭… Ⅲ.①互联网络－安全技术 Ⅳ.①TP393.408

中国版本图书馆 CIP 数据核字（2017）第 099755 号

书　　名：网络空间安全基础
著作责任者：彭海朋　编著
责 任 编 辑：刘　佳
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号（邮编：100876）
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：保定市中画美凯印刷有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：18
字　　数：444 千字
版　　次：2017 年 8 月第 1 版　2017 年 8 月第 1 次印刷

ISBN 978-7-5635-5091-3　　定　价：39.00 元

Prologue 序

Prologue

作为最新的国家一级学科，由于其罕见的特殊性，网络空间安全真可谓是典型的“在游泳中学游泳”。一方面，蜂拥而至的现实人才需求和紧迫的技术挑战，促使我们必须以超常规手段，来启动并建设好该一级学科；另一方面，由于缺乏国内外可资借鉴的经验，也没有足够的时间纠结于众多细节，所以，作为当初“教育部网络空间安全一级学科研究论证工作组”的八位专家之一，我有义务借此机会，向大家介绍一下2014年规划该学科的相关情况；并结合现状，坦诚一些不足，以及改进和完善计划，以使大家有一个宏观了解。

我们所指的网络空间，也就是媒体常说的赛博空间，意指通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间。它已成为继陆、海、空、太空之后的第五空间。网络空间里不仅包括通过网络互联而成的各种计算系统（各种智能终端）、连接端系统的网络、连接网络的互联网和受控系统，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种数据或信息。与其他四个空间不同，网络空间没有明确的、固定的边界，也没有集中的控制权威。

网络空间安全，研究网络空间中的安全威胁和防护问题，即在有敌手对抗的环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施，以及网络和系统本身的威胁和防护机制。网络空间安全不仅包括传统信息安全所涉及的信息保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。

网络空间安全一级学科，下设五个研究方向：网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。

方向1，网络空间安全基础，为其他方向的研究提供理论、架构和方法学指导；它主要研究网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等内容。

方向2，密码学及应用，为后三个方向（系统安全、网络安全和应用安全）提供密码机制；它主要研究对称密码设计与分析、公钥密码设计与分析、安全协议

设计与分析、侧信道分析与防护、量子密码与新型密码等内容。

方向3，系统安全，保证网络空间中单元计算系统的安全；它主要研究芯片安全、系统软件安全、可信计算、虚拟化计算平台安全、恶意代码分析与防护、系统硬件和物理环境安全等内容。

方向4，网络安全，保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全；它主要研究通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等内容。

方向5，应用安全，保证网络空间中大型应用系统的安全，也是安全机制在互联网应用或服务领域中的综合应用；它主要研究关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等内容。

从基础知识体系角度看，网络空间安全一级学科主要由五个模块组成：网络空间安全基础、密码学基础、系统安全技术、网络安全技术和应用安全技术。

模块1，网络空间安全基础知识模块，包括：数论、信息论、计算复杂性、操作系统、数据库、计算机组成、计算机网络、程序设计语言、网络空间安全导论、网络空间安全法律法规、网络空间安全管理基础。

模块2，密码学基础理论知识模块，包括：对称密码、公钥密码、量子密码、密码分析技术、安全协议。

模块3，系统安全理论与技术知识模块，包括：芯片安全、物理安全、可靠性技术、访问控制技术、操作系统安全、数据库安全、代码安全与软件漏洞挖掘、恶意代码分析与防御。

模块4，网络安全理论与技术知识模块，包括：通信网络安全、无线通信安全、IPv6安全、防火墙技术、入侵检测与防御、VPN、网络安全协议、网络漏洞检测与防护、网络攻击与防护。

模块5，应用安全理论与技术知识模块，包括：Web安全、数据存储与恢复、垃圾信息识别与过滤、舆情分析及预警、计算机数字取证、信息隐藏、电子政务安全、电子商务安全、云计算安全、物联网安全、大数据安全、隐私保护技术、数字版权保护技术。

其实，从纯学术角度看，网络空间安全一级学科的支撑专业，至少应该平等地包含信息安全专业、信息对抗专业、保密管理专业、网络空间安全专业、网络安全与执法专业等本科专业。但是，由于管理渠道等诸多原因，我们当初只重点考虑了信息安全专业，所以，就留下了一些遗憾，甚至空白，比如，信息安全心

理学、安全控制论、安全系统论等。不过幸好，学界现在已经开始着手，填补这些空白。

北京邮电大学在网络空间安全相关学科和专业等方面，在全国高校中一直处于领先水平；从20世纪80年代初至今，已有30余年的全方位积累，而且，一直就特别重视教学规范、课程建设、教材出版、实验培训等基本功。本套系列教材，主要是由北京邮电大学的骨干教师们，结合自身特长和教学科研方面的成果，撰写而成。本系列教材暂由《信息安全数学基础》《网络安全》《汇编语言与逆向工程》《软件安全》《网络空间安全导论》《可信计算理论与技术》《网络空间安全治理》《大数据服务与安全隐私技术》《数字内容安全》《量子计算与后量子密码》《移动终端安全》《漏洞分析技术实验教程》《网络安全实验》《网络空间安全基础》《信息安全管理(第3版)》《网络安全法学》《信息隐藏与数字水印》等20余本本科生教材组成。这些教材主要涵盖信息安全专业和网络空间安全专业，今后，一旦时机成熟，我们将组织国内外更多的专家，针对信息对抗专业、保密管理专业、网络安全与执法专业等，出版更多、更好的教材，为网络空间安全一级学科，提供更有力的支撑。

杨义先

教授、长江学者、杰青

北京邮电大学信息安全中心主任

灾备技术国家工程实验室主任

公共大数据国家重点实验室主任

2017年4月，于花溪

前言

Foreword

近年来，随着社会信息化的不断加深，我国迅速成长为信息化大国，是目前全球范围内互联网用户最多、普及最广泛的国家。随着人们对互联网依赖度的逐渐提高，网络空间已经成为继陆、海、空、太空之后的第五空间，成为各国角逐权利的新战场。国际上围绕网络空间安全的斗争愈演愈烈，我国网络空间安全受到的冲击也越来越大。2014 年 2 月 27 日，中央成立网络安全与信息化领导小组，着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。

习近平指出，“没有网络安全就没有国家安全，没有信息化就没有现代化。”建设网络强国，要有自己过硬的技术；要有丰富全面的信息服务、繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济；要有高素质的网络安全和信息化人才队伍；要积极开展双边、多边的互联网国际交流合作。建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进。

为实施国家安全战略，加快网络空间安全高层次人才培养，2015 年 6 月国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。

网络空间安全学科培养学生掌握密码和网络空间安全基础理论和技术方法，掌握信息系统安全、网络基础设施安全、信息内容安全和信息对抗等相关专门知识，并具有较高网络空间安全综合专业素质、较强的实践能力和创新能力，能够承担科研院所、企事业单位和行政管理部门网络空间安全方面的科学研究、技术开发及管理工作。

网络空间安全一级学科的理论方法和方法论基础涉及数学、信息论、计算复杂理论、控制论、系统论、认知科学、博弈论、管理学等。网络空间安全涉及数学、计算机科学与技术、信息与通信工程等多个学科，已形成了一个相对独立的

教学和研究领域。

网络空间安全主要研究网络空间中的安全威胁和防护问题，即在有敌手的对抗环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施以及网络和系统本身的威胁和防护机制。网络空间安全不仅仅包括传统信息安全所研究的信息的保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。

网络空间安全学科主要研究方向有5个：网络空间安全基础理论、密码学及应用、系统安全、网络安全、应用安全。网络空间安全基础理论方向为其他方向提供理论、架构和方法学指导；密码学及应用方向为其他方向提供密码体制机制；系统安全方向保证网络空间中单元计算系统安全、可信；网络安全方向保证连接计算机的网络自身安全和传输信息安全；应用安全方向保证网络空间中大型应用系统安全。

本书是网络空间安全学科的基础教材，围绕网络空间安全学科的主要研究方向及网络空间安全基础理论和密码学及应用两部分内容合理组织知识结构，其中第2章(基础知识)、第4章(大数据安全)、第5章(复杂网络安全)、第6章(网络安全博弈)、第7章(虚拟资产安全)和第8章(安全通论)等内容对应于网络空间安全基础理论的主要研究方向及内容，第3章(新型密码技术)则对应于密码学及应用。本书立足于网络空间安全的基本知识，并竭力把握好知识的深度和广度，为网络空间安全学科的后续课程及后续研究奠定一定的知识基础。

本书由北京邮电大学彭海朋编著，在内容规划和撰写过程中得到了北京邮电大学杨义先教授和李丽香教授、四川大学李涛教授、西南大学赖红副教授、青岛大学王震、孙菲等老师的大力支持和帮助，在此向他们表示衷心的感谢！也感谢陈自刚、陈川、郑明文、陈永刚等博士及陈晨、冯翠翠、侯敬宜、林茹、沈如辉、樊晓彤等同学的帮助。

本书的出版得到了国家自然科学基金(项目编号：61472045、61573067)和国家重点研发计划“网络空间安全”重点专项(项目编号：2016YFB0800602)的支持，北京邮电大学出版社为本书出版做了大量编辑和组织工作，特在此致谢！

限于水平，书中难免有错误与不妥之处，恳请读者批评指正。

彭海朋

目录

Contents

第1章

绪　论

近年来，互联网的高速发展给人们生活的方方面面带来了翻天覆地的变化，李克强总理在政府工作报告中提出，“制定‘互联网＋’行动计划，推动移动互联网、云计算、大数据、物联网等与现代制造业结合，促进电子商务、工业互联网和互联网金融健康发展，引导互联网企业拓展国际市场。”“互联网＋”的战略使得互联网应用进入一个全新的阶段，许多传统产业借助互联网平台焕发出了新活力。

1.1　网络空间

网络空间(Cyberspace)是指通过全球互联网和计算系统进行通信、控制和信息共享的动态(不断变化)虚拟空间。目前，继陆、海、空、太空之后，网络空间已成为世界第五大空间。这个巨大的虚拟空间不但包括通过网络互连而成的各种计算系统和智能终端，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种巨大数据或信息。网络空间就是虚拟世界的神经系统，有着极其重要的作用，其最为显著的特点是没有明确、固定的边界，也没有集中的控制权。网络空间包含着事关国计民生的关键信息基础设施，例如金融网、能源网、交通网等以及事关国家安全的国防信息基础设施的各类军网。

1.2　网络空间的积极意义

随着经济全球化和信息化的发展，以互联网为基础的信息基础设施对整个国家和社会的正常运行发展起着关键作用，它和电力、能源、交通等基础设施一样，在国民经济发展的各个领域处于基础地位，甚至其他传统基础设施的运行也逐渐依赖互联网和相关信息系统的正常运行。正如习近平总书记所言，“没有信息化就没有现代化”。

1.3　网络空间的安全威胁

随着社会对网络和信息系统依赖性的增加，网络空间面临的威胁也与日俱增。网络和信息安全牵涉国家安全和社会稳定。

从国际上看，国家或地区在政治、经济、军事等各领域的冲突都会反映到网络空间。与陆、海、空、太空等领域相比，网络空间这个虚拟世界有其无可比拟的特点，对国家安全构成威胁。第一，网络空间没有明确、固定的边界，资源分配不均衡，导致网络空间的争夺异常复

杂；第二，网络空间没有集中的控制权，网络武器（如计算机病毒）极易扩散；第三，网络空间具有极强的隐蔽性，发动者可以藏身于一个无人知晓的地方发动门槛极低的网络攻击，且不留下任何可被追踪的痕迹；第四，网络空间包含事关国计民生的关键信息基础设施，以及事关国家安全的国防信息基础设施，也就是说，网络空间安全事关国计民生和国家安全。网络空间作为“第五大空间”已经成为各国角逐权力的新战场，世界主要国家为抢占网络空间制高点，已经开始积极部署网络空间安全战略及网战部队。

就社会生活而言，网络空间的安全威胁涉及网络漏洞、个人信息安全、网络冲突与攻击、网络犯罪等。网络漏洞是无授权的攻击者利用计算机系统软硬件、网络协议、系统安全方面存在的缺陷对数据进行窃取、操控，进而破坏网络系统。服务商、员工人为泄露客户信息，黑客通过黑客技术盗取信息数据，导致个人信息安全受到严重威胁。除了国家之间的网络冲突与攻击之外，企业间或者利益集团间也存在着网络冲突与攻击。网络信息窃取、互联网金融诈骗、网上洗钱、色情服务、虚假广告等网络犯罪频率也呈现出快速上升的趋势，同时其智能性、隐蔽性和复杂性使得取证更加困难。网络空间的安全威胁也影响社会稳定。

网络空间的安全威胁按照行为主体的不同，可划分为黑客攻击、有组织网络犯罪、网络恐怖主义以及国家支持的网络战这四种类型。

网络空间安全已经是国家安全战略的重要组成部分。以互联网为基础的信息系统几乎构成了整个国家和社会的中枢神经系统，它得以安全可靠运行是整个社会正常运转的重要保证。如果这个系统的安全出了问题（如受到入侵或瘫痪），必将影响整个社会的正常运转，造成大面积的瘫痪或恐慌。

党中央、国务院历来重视我国信息安全保障体系的建设，新一届中央领导集体高度重视网络安全工作。2014 年 2 月 27 日，中央成立网络安全与信息化领导小组，习近平总书记亲自担任组长。习总书记在第一次会议上强调指出：“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展。”“网络安全和信息化是一体之两翼、双轮之驱动，必须统一谋划、统一部署、统一推进、统一实施。”“没有网络安全，就没有国家安全；没有信息化，就没有现代化。”这一科学论断阐述了网络安全与国家信息化之间的紧密联系，使我们认识到网络安全为国家信息化建设提供安全保障的极端重要性。

充分利用互联网对经济发展的推动作用，保护公民和企业的合法权益，同时又要控制它威胁国内社会稳定的负面影响，此外，还要立足网络空间安全，维护国家安全。

1.4 网络空间安全

网络空间安全的对抗是人与人的对抗，无论是国家安全、企业安全、个人安全，还是社会的治理都是如此。培养网络空间安全人才是当务之急。

然而，由于网络空间安全学科建设缺乏系统性、规模小，远远满足不了信息安全产业发展对高层次专门人才的需要，导致我国信息安全关键技术整体上比较落后。据统计，信息安全人才连续几年一直被列为最急需的人才之一，信息安全人才问题已经成为当前严重制约信息安全产业发展的瓶颈。

为实施国家安全战略，加快网络空间安全高层次人才培养，2015 年 6 月国务院学位委

员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科。

从信息论角度来看，系统是载体，信息是内涵，网络空间是所有信息系统的集合，是人类生存的信息环境，人在其中与信息相互作用、相互影响。因此，网络空间存在更加突出的信息安全问题，其核心内涵仍是信息安全。

网络空间安全主要研究网络空间中的安全威胁和防护问题，即在有敌手的对抗环境下，研究信息在产生、传输、存储、处理各个环节中所面临的威胁和防御措施以及网络和系统本身的威胁和防护机制。网络空间安全不仅包括传统信息安全所研究的信息保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。

网络空间安全学科主要研究方向有5个，如图1.1所示。网络空间安全基础理论方向为其他方向提供理论、架构和方法学指导；密码学及应用方向为其他方向提供密码体制机制；系统安全方向保证网络空间中单元计算系统安全、可信；网络安全方向保证连接计算机的网络自身安全和传输信息安全；应用安全方向保证网络空间中大型应用系统安全。

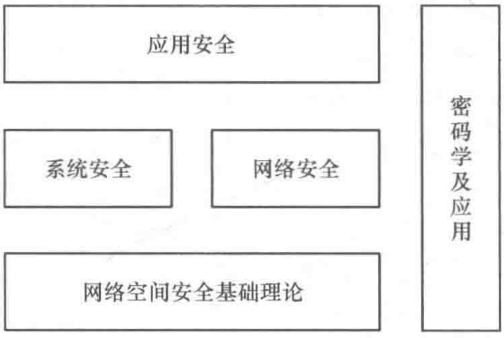

图1.1 网络空间安全学科主要研究方向

网络空间安全一级学科的理论方法和方法论基础涉及数学、信息论、计算复杂理论、控制论、系统论、认知科学、博弈论、管理学等。网络空间安全涉及数学、计算机科学与技术、信息与通信工程等多个学科，已形成了一个相对独立的教学和研究领域。

网络空间安全学科培养学生掌握密码和网络空间安全的基础理论和技术方法，掌握信息系统安全、网络基础设施安全、信息内容安全和信息对抗等相关专门知识，并具有较高的网络空间安全综合专业素质、较强的实践能力和创新能力，能够承担科研院所、企事业单位和行政管理部门网络空间安全方面的科学研究、技术开发及管理工作。

信息安全、网络安全、网络空间安全三者既有互相交叉的部分，也有各自独特的部分。信息安全泛指各类信息安全问题，网络安全指网络所带来的各类安全问题，网络空间安全则特指与陆、海、空、太空并列的全球五大空间中的网络空间安全问题。

1.5 网络空间安全基础

网络空间的规模和复杂度都远超于传统计算机网络，网络空间安全的影响跨越物理域、逻辑域、社会域和认知域，传统的网络安全、信息安全理论和方法学必然无法满足研究需求，因此，需要新的网络空间安全理论。但同时由于网络空间安全是处于不断发展变化中的学科，其安全理论也必将随着时间的推移而不断发展成熟。

网络空间安全基础理论的研究内容包括网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略等。

本书是一本网络空间安全学科的基础教材，围绕图 1.1 网络空间安全学科主要研究方向及内容中的网络空间安全基础理论和密码学及应用两部分内容合理选择组织知识结构和内容，其中第 2 章(基础知识)、第 4 章(大数据安全)、第 5 章(复杂网络安全)、第 6 章(网络安全博弈)、第 7 章(虚拟资产安全)和第 8 章(安全通论)等内容对应于网络空间安全基础理论的主要研究方向及内容，第 3 章(新型密码技术)则对应于密码学及应用。本教材立足于网络空间安全的基本知识，并竭力把握好知识的深度和广度，为网络空间安全学科的后续课程及后续研究奠定一定的知识基础。

1. 基础知识

主要是对后文所用到的相关知识进行初步的介绍，内容包括抽象代数、信息论、博弈论、稳定性理论和复杂网络理论等。抽象代数给出一些有关群、环和域的相关概念，并不加证明地给出相关的重要定理，介绍数论中一些最基本的知识，包括简单模运算和欧拉定理；信息论主要介绍信息熵和信道容量；博弈论主要介绍博弈论中的有关术语、博弈类型以及纳什均衡；稳定性理论主要介绍解的稳定性，按线性近似判断稳定性，李雅普诺夫第二方法；复杂网络主要介绍复杂网络的主要术语、网络模型等。

2. 新型密码技术

首先，介绍传统的密码技术，主要包括对称密码、非对称密码、数字签名和密码协议；其次，介绍三种新型密码技术，主要包括混沌密码技术、量子密码技术、格密码和格密码技术。混沌密码技术主要介绍混沌保密通信系统、混沌密码学、混沌密码技术应用、混沌密码存在的问题等。量子密码技术主要介绍量子比特及属性、量子密码经典模型、量子密码应用等。格密码主要介绍格密码的基础知识、格上的一些困难问题、STP-GPV 算法及相应的仿真实验。

3. 大数据安全

主要介绍大数据概述、大数据安全、大数据安全保障技术以及大数据安全应用技术。大数据概述介绍大数据的时代背景、基本理论、机遇挑战和大数据与云计算。大数据安全主要介绍大数据安全的定义，不同领域的大数据安全要求以及大数据安全应用实例。大数据安全保障技术主要介绍数据采集安全技术、数据存储安全技术、数据挖掘安全技术以及数据发布安全技术。大数据安全应用技术主要介绍位置大数据隐私保护以及社交网络的隐私保护。

4. 复杂网络安全

主要介绍四部分内容。首先，介绍复杂网络安全面临的挑战；其次，介绍复杂网络安全模型，包括静态拓扑结构下复杂网络的鲁棒性、级联失效情况下单层网的鲁棒性分析、相互依存网络的鲁棒性分析等；然后，介绍复杂网络安全策略，包括带有应急恢复机制的网络级联动力学模型、相互依存网络上的鲁棒性增强策略等；最后，介绍复杂网络的病毒传播模型，包括两途径传播病毒的 SIR 传播模型、两层网络模型、邻居节点平均相似度与度相关性、传播临界值与传播规模及其仿真实验。

5. 网络安全博弈

主要介绍静态博弈理论、动态博弈与逆向归纳法、网络安全博弈应用和复杂网络演化博