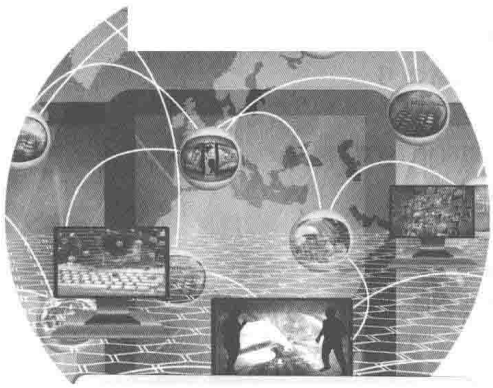
网络空间安全技术基础

陈启安　滕　达　申　强　◎主编

厦门大学出版社
XIAMEN UNIVERSITY PRESS
国家一级出版社
全国百佳图书出版单位

网络空间安全技术基础

主　编：陈启安　滕　达　申　强
参　编：周政杰　林远进　蔡菲娜　钟双琴
　　郭智旺　费　嘉　林文水



厦门大学出版社 XIAMEN UNIVERSITY PRESS
国家一级出版社
全国百佳图书出版单位

图书在版编目(CIP)数据

网络空间安全技术基础/陈启安，滕达，申强主编. —厦门：厦门大学出版社，2017.12
ISBN 978-7-5615-6669-5

Ⅰ.①网… Ⅱ.①陈…②滕…③申… Ⅲ.①网络安全 Ⅳ.①TN915.08

中国版本图书馆 CIP 数据核字(2017)第 225529 号

出 版 人 蒋东明
策　　划 宋文艳
责任编辑 郑　丹　李峰伟
封面设计 蒋卓群
技术编辑 许克华

出版发行 厦门大学出版社
社　　址 厦门市软件园二期望海路 39 号
邮政编码 361008
总 编 办 0592-2182177　0592-2181406(传真)
营销中心 0592-2184458　0592-2181365
网　　址 http://www.xmupress.com
邮　　箱 xmupress@126.com
印　　刷 厦门市金凯龙印刷有限公司

开本 787mm×1092mm　1/16
印张 25.25
字数 586 千字
版次 2017 年 12 月第 1 版
印次 2017 年 12 月第 1 次印刷
定价 43.00 元

厦门大学出版社
微信二维码

厦门大学出版社
微博二维码

内容简介

本书全面、系统地介绍了网络空间安全的相关知识，是一本网络空间安全技术基础的指导性书籍，它从网络空间安全的基本概念、相关法律法规和基础知识着手，着重介绍了网络空间安全防护技术、网络空间治理技术、网络渗透技术、电子数据勘查取证技术、计算机取证分析技术及移动终端取证技术。书中提供了许多编者在实际工作中的应用实例及相关案例，并在各章节最后给出了练习题，这些应用实例均可在相关平台进行练习实践，既突出了网络空间安全技术的实践教学和应用特点，又满足了读者的不同需要。

本书的特点是内容新、覆盖面广、通俗易懂且实用性强，在实例中使用了大量图片辅助讲解、图文并茂，便于初学者掌握网络空间安全技术的应用与开发，它可作为高校网络空间安全技术课程的基础性教材，也可作为网络空间安全技术研究和开发人员的参考书。

序

信息技术的广泛应用和网络空间的兴起发展，极大促进了经济社会繁荣进步，同时也带来了新的安全风险和挑战。信息作为一种战略资源，其安全问题也成为关系国家安全、经济发展和社会稳定的战略性问题。网络空间安全事关人类共同利益，事关世界和平与发展，事关各国国家安全。维护我国网络空间安全是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措，是实现“两个一百年”奋斗目标、实现“中国梦”的重要保障。

党中央、国务院高度重视我国网络空间安全保障体系的建设。国家互联网信息办公室于2016年发布了《国家网络空间安全战略》，在其中阐明了中国关于网络空间发展和安全的重大立场，用以指导中国网络空间安全工作，维护国家在网络空间的主权、安全、发展利益。2017年6月1日起实施的《中华人民共和国网络安全法》也在法律层面对维护网络空间安全提出了明确要求，明确国家及各级政府应加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，实行网络安全等级保护制度，支持企业、研究机构、高等学校等参与国家网络安全技术创新项目。

21世纪的竞争是人才的竞争，人才的竞争归根到底是教育的竞争。国家教育部明确指出“要不断加强信息安全学科建设，尽快培养高素质的信息安全人才队伍，将其作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”。为适应国家和社会对网络空间安全人才的迫切需求，国内众多高校开设了网络空间安全类专业，也有很多学校将网络空间安全技术基础课程作为全校性的公选课。2015年，我国设立了“网络空间安全”一级学科。在构建更加合理的课程体系的同时，编写一本专业知识扎实，针对性强，实用、好用的网络空间安全教材便成为人才培养的当务之急。

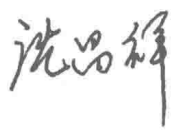
网络空间安全学科是一门涉及计算机、信息安全、通信技术、数学、法律等多学科的综合性交叉学科，内容比较庞杂，有关知识、技术和应用更新迅速。厦门大学陈启安老师等主编的《网络空间安全技术基础》和《网络空间安全技

术实验》从网络空间安全设备及相关技术着手，除了对网络空间安全防护技术、治理技术、渗透技术的基础知识进行细致讲解外，还在电子数据勘查取证技术、计算机取证分析技术、移动终端取证技术方面结合最新技术对主流的方法和工具进行了介绍，同时在案例分析中注重相关法律知识的渗透，构建了完整的网络空间安全知识结构体系。

产学研合作教育是培养新兴学科人才和紧缺技术人才的有效方法，可以打破以理论教学为主导、实践教学为辅助的教学模式的束缚，创造出更多、更广泛的教学实践条件和方法，进而提高学生的学习热情，培养学生的技能和实践能力，尤其是将学习到的专业知识应用于实践中的能力。《网络空间安全技术基础》和《网络空间安全技术实验》由高校从事教学的一线教师和企业研发骨干人员合作编写，内容既符合学生课程设置的要求，又与技术发展的前沿紧密联系，反映出网络空间安全领域的新趋势、新成果。特别值得一提的是，书中案例的选取体现“典型性”“真实性”和“针对性”，既有对网络空间安全热点事件的专题报告，也有我国自主研发工具的实际运用操作讲解，内容新颖翔实，流程讲解图文并茂，使学生在学习时避免了“纸上谈兵”，真正做到学以致用。

信息化是世界经济和社会发展的必然趋势，网络空间安全关乎每个人的切身利益。不仅相关专业教师、学生，相关领域技术工作者需要学习网络空间安全知识，我们每一个人都应该学习网络空间安全知识，成为维护网络空间安全的参与者，而不是旁观者。相信这套教材定能对我国网络空间安全相关领域的教育发展和教学水平的提高有所裨益，成为所有想学习网络空间安全技术知识的读者的有益读物，对推动我国信息化人才的培养做出贡献。

教育部高等学校信息安全专业教指委名誉主任、中国工程院院士



前 言

网络空间是人运用信息技术通信系统进行交互的空间。其中信息技术通信系统包括各类互联网、电信网、广电网、物联网、在线社交网络，计算系统、通信系统、控制系统，电子或数字信息处理设施等；交互是指人与人之间的信息通信技术活动。网络空间是一个新事物，关系到人类未来的生存及生活模式，网络空间安全已成为近年来国内外关注的焦点之一。

习近平同志指出：网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题；没有网络安全就没有国家安全，没有信息化就没有现代化。为实施国家安全战略，加快网络空间安全高层次人才培养，国务院学位委员会、教育部于2015年增设“网络空间安全”一级学科。目前，已有几十所高校获准建立该学科的一级学科博士点。这些足以说明网络空间安全课程建设的重要性。

网络空间安全也和我们的生活息息相关。今天的社会已经完全迈入“互联网＋”时代。在我们享受着快速发展的信息技术给我们带来的便利生活的同时，也要警惕它可能带给我们的伤害。象牙塔中的大学生应该充分利用学校提供的软硬件设施提高自己的网络安全意识，了解网络安全基本知识，懂得基本防护技巧，让自己远离网络侵权、网络暴力、网络诈骗、网络攻击，共同创建和维护一个净化的网络环境。

网络空间安全技术涉及多种交叉学科，知识覆盖面广，网络空间安全领域需要的人才多种多样，包括立法人才、治理人才、战略人才、技术和理论研发人才、安全规划人才、宣传和教育人才、运维人才、防御人才等多层次的复合型人才。因此，除计算机相关专业的学生外，非计算机专业的学生学习网络空间安全知识，也能从自己的专业特长出发，对维护网络空间安全做出法律、管理、宣传等全方位的贡献。

网络空间安全是一门实践性很强的学科。在教学中应当重视实践应用环节，与相关企事业单位进行联合教学，加强对新知识、新技术的学习，理论联系实际地培养出高素质的网络空间安全人才。正是基于这一目的，我们组织了厦门大学教学经验丰富的一线教师和厦门美亚柏科信息股份有限公司的骨干

人员，结合自身多年的工作及教学经验完成了本书的编写。

编者在本书编写中力求做到科学性与实用性、先进性与针对性相统一；做到循序渐进、由浅入深、简明易懂；着重于基本概念、基本方法的理解应用，特别注意对学生动手能力的培养。本书和与本书配套的实验教材《网络空间安全技术实验》对每一种设计或分析方法都安排有步骤完整、过程详细的实例予以说明，各章都配备有习题供读者练习。

全书共分 7 章，参考学时数为 60 学时，其中实验学时数为 20～24 学时。各章内容如下：第 1 章，网络空间安全设备及相关技术；第 2 章，网络空间安全防护技术；第 3 章，网络空间治理技术；第 4 章，网络渗透技术基础；第 5 章，电子数据勘察取证技术；第 6 章，计算机取证分析技术；第 7 章，移动终端取证技术。目录中标有“*”号的章节提供给有一定相关技术基础的读者学习，其他读者可以略过。

网络空间安全是一门新的学科，新技术的发展总是日新月异，相关知识更新很快。在本书编写过程中，编者虽做了很大努力，但限于水平，难免有错误和疏漏之处，敬请读者批评指正。另外在编写过程中，编者参阅了大量的文献，包括专业书籍、论文、报告等，借此机会向文献的作者表示衷心的感谢！

网络空间安全是一个系统工程，涉及领域繁多。我们真诚期望本书能够尽可能多地展现出网络空间安全的丰富内涵，使其成为读者掌握网络空间安全知识与技能的有益参考书，同时热烈期望同学们在学习中能够有所收获！

编者

2017 年 11 月

目 录

注：带“*”号标记的章节供计算机相关专业的学生学习，其他专业学生不做要求。

第 1 章

网络空间安全设备及相关技术

1.1 网络空间安全概述

1.1.1 定　义

网络空间是一个虚拟的空间，虚拟空间包含 3 个基本要素：第一个是载体，也就是通信系统；第二个是主体，也就是网民、用户；第三个是构造一个集合，用规则管理起来，我们称之为“网络空间”。

网络空间是人们运用信息通信系统进行交互的空间，其中信息技术通信系统包括各类互联网、电信网、广电网、物联网、在线社交网络、计算系统、控制系统等，电子或数字信息处理设施等。

“网络空间安全”的英文是 cyberspace security。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》中创造了 cyberspace 一词，意指由计算机创建的虚拟信息空间。cyberspace 在这里强调的是电脑爱好者在游戏机前体验到交感幻觉，体现了 cyberspace 不仅是信息的简单聚合体，而且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。除美国外，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。网络空间安全，即由互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的相关安全。网络空间安全涉及网络空间中的电子设备、电子信息系统、运行数据、系统应用中存在的安全问题，分别对应 4 个层面：设备、系统、数据和应用。这里面包括两个部分：

第一、防治、保护、处置包括互联网、电信网、广电网、物联网、工控网、在线社交网络、计算系统、通信系统、控制系统在内的各种通信系统及其承载的数据不受损害。

第二、防止对这些信息通信技术系统的滥用所引发的政治安全、经济安全、文化安全和国防安全。既要保护系统本身，也要防止利用信息系统带来的安全问题。针对这些风险，要采取法律、管理、技术、自律等综合手段来应对（图 1-1），而不能单一地说信息安全

主要是技术手段。

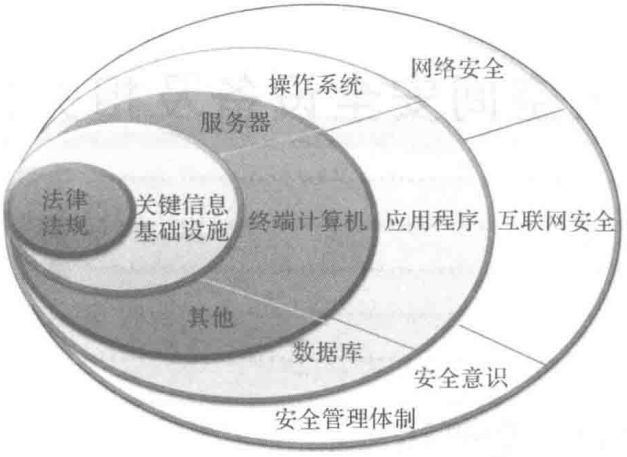


图 1-1　网络空间安全构成

中国的网民数量和网络规模世界第一，维护好中国网络空间安全，不仅是自身需要，而且对维护全球网络安全乃至世界和平都具有重大意义。中国致力于维护国家网络空间主权、安全、发展利益，促进网络空间和平利用和共同治理，推动互联网发展以造福人类。

网络安全的人才多种多样，包括立法人才、治理人才、战略人才、技术和理论研发人才、安全规划人才、宣传和教育人才、运维人才、防御人才等。网络空间安全专业的人才培养目标是：培养具有扎实的网络空间安全基础理论和基本技术，系统掌握信息内容安全、网络安全法律、网络安全管理的专业知识，政治素质过硬，较强的中英文沟通和写作能力，有技术、懂法律、会谈判的复合型人才。

为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证及国务院学位委员会学科评议组评议，报国务院学位委员会批准，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。目前，已有几十所高校获准建立该学科的一级学科博士点。

1.1.2　相关法律法规

1. 刑事法律依据

①《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》。

②《中华人民共和国刑法(修订)》。

③《中华人民共和国刑事诉讼法》。

④最高人民法院、最高人民检察院《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》。

⑤最高人民法院、最高人民检察院《关于办理网络淫秽色情犯罪的司法解释》。

⑥最高人民法院、最高人民检察院《关于办理网络淫秽色情犯罪的司法解释(二)》。

⑦最高人民法院、最高人民检察院《关于办理赌博刑事案件具体应用法律若干问题的

司法解释》。

⑧最高人民法院、最高人民检察院、公安部《关于办理网络赌博犯罪案件适用法律若干问题的意见》。

⑨最高人民法院、最高人民检察院《关于办理诈骗刑事案件具体应用法律若干问题的司法解释》。

⑩最高人民法院、最高人民检察院《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的司法解释》。

⑪最高人民法院、最高人民检察院、公安部《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》。

⑫《中华人民共和国国家安全法》。

⑬《中华人民共和国反恐怖主义法》。

⑭《中华人民共和国网络安全法》。

⑮最高人民法院、最高人民检察院、公安部《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》。

⑯最高人民法院、最高人民检察院、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》。

⑰最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》。

2. 行政法律依据/规范性文件

①《全国人民代表大会常务委员会关于加强网络信息保护的决定》。

②《治安管理处罚法》。

③《计算机信息系统安全保护条例》。

④《计算机信息网络国际联网安全保护管理办法》。

⑤《互联网上网服务营业场所管理条例》。

⑥《互联网信息服务管理办法》。

⑦《计算机病毒防治管理办法》。

⑧《互联网安全保护技术措施规定》。

⑨《信息网络传播权保护条例》。

⑩《“约谈十条”互联网新闻信息服务单位约谈工作规定》。

⑪《“账号十条”互联网用户账号名称管理规定》。

⑫《互联网信息搜索服务管理规定》。

⑬《移动互联网应用程序信息服务管理规定》。

⑭《互联网直播服务管理规定》。

⑮《互联网新闻信息服务管理规定》。

⑯《网络交易管理办法》。

3. 信息安全等级保护

①《关于信息安全等级保护工作的实施意见》(公通字〔2004〕66 号)。