HZ BOOKS
华章教育

网络空间安全学科规划教材

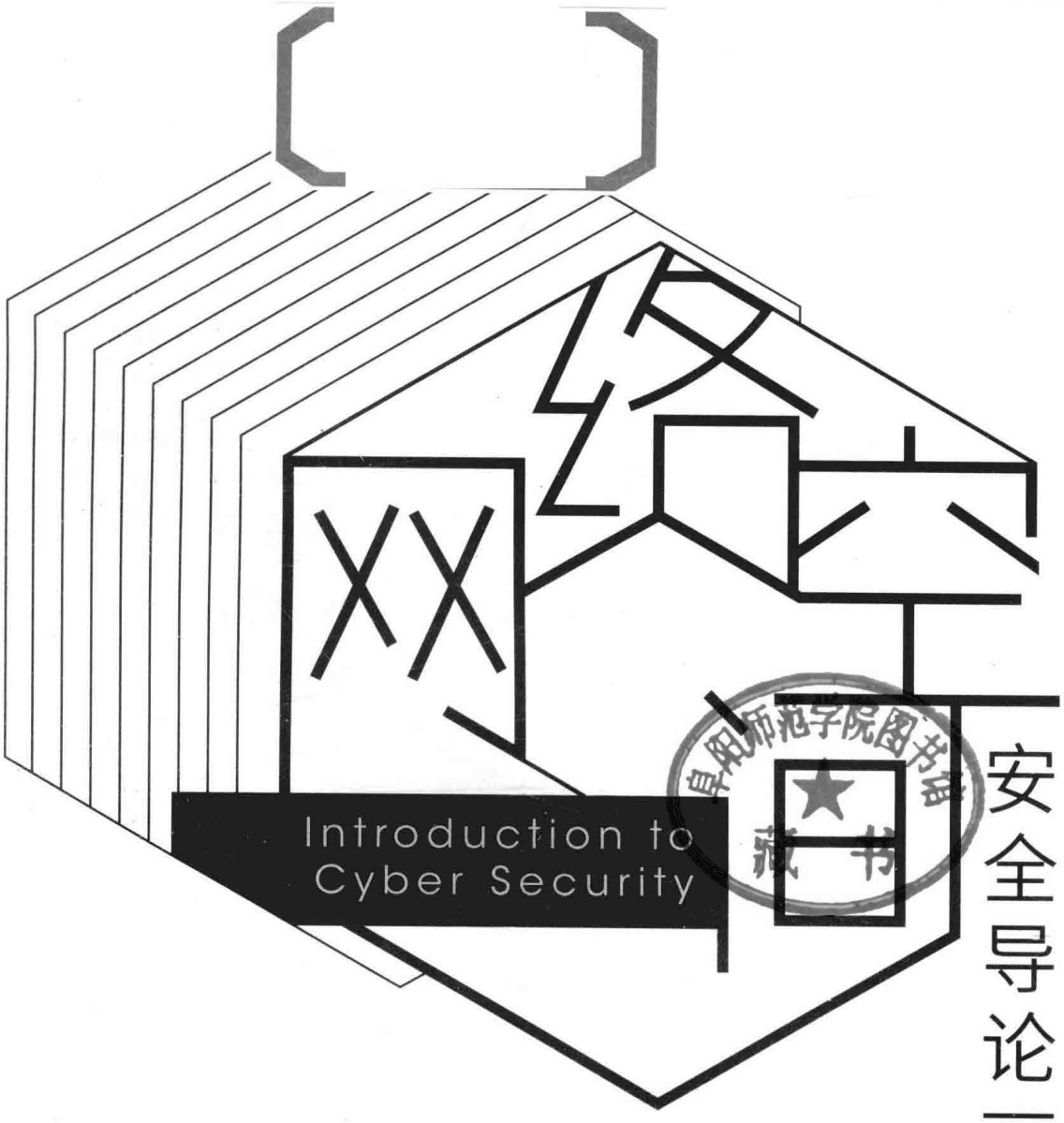
网络空间安全导论

Introduction to Cyber Security

蔡晶晶 李炜◎主编
侯孟佺 孙维隆 赵永 张光义◎参编

机械工业出版社
China Machine Press

网络空间安全学科规划教材



蔡晶晶 李炜◎主编
侯孟伶 孙维隆 赵永 张光义◎参编

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络空间安全导论 / 蔡晶晶，李炜主编 . —北京：机械工业出版社，2017.6
（网络空间安全学科规划教材）

ISBN 978-7-111-57309-8

I. 网… II. ①蔡… ②李… III. 网络安全 - 教材 IV. TN915.08

中国版本图书馆 CIP 数据核字（2017）第 162079 号

本书面向初学者，以行业视角融合基本的网络空间安全理论体系来组织全书内容，按照网络空间安全的基本知识点、网络空间安全知识的应用场景及大型攻防案例的主线由浅入深地介绍网络空间安全的基础知识和技能。本书内容涵盖网络空间安全的技术架构、物理安全、网络安全、系统安全、应用安全、数据安全、舆情分析、隐私保护、密码学等，并对当前热点的大数据安全、物联网安全、云安全等内容进行了初步介绍，对网络空间安全相关的法律法规等也进行了系统梳理。通过网络攻防大赛的题目分析和企业安全压力测试的案例分析及实践，读者可综合应用相关知识解决实际问题。

本书适合作为高等院校信息安全、计算机、电子对抗及相关专业的教材，也适合作为理工科学生了解网络空间安全的参考书。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：朱　劼　　责任校对：李秋荣
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2017 年 8 月第 1 版第 1 次印刷
开　　本：185mm×260mm　1/16　　印　　张：17.75
书　　号：ISBN 978-7-111-57309-8　　定　　价：49.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

本书编委会

（按姓氏拼音顺序）

蔡晶晶（北京永信至诚科技股份有限公司）

崔　勇（清华大学）

李　炜（北京永信至诚科技股份有限公司）

李舟军（北京航空航天大学）

侯孟伶（北京永信至诚科技股份有限公司）

贾春福（南开大学）

马　丁（公安大学）

王　标（国际关系学院）

嵩　天（北京理工大学）

孙维隆（北京永信至诚科技股份有限公司）

徐文渊（浙江大学）

张光义（北京永信至诚科技股份有限公司）

张兆心（哈尔滨工业大学（威海））

赵　刚（北京信息科技大学）

赵　永（北京永信至诚科技股份有限公司）

序

网络空间安全是什么？

这是个值得我们思考的问题。

信息通信技术（ICT）的蓬勃发展，使得网络空间的边界在过去二十几年中变得无比广阔，它联结着地球上的每一台终端、每一个人、每一寸土地，甚至已经覆盖到广阔的宇宙当中，令人惊叹于技术的伟大。

从最初的几台计算机间的简单传输，到如今沟通万物、生机勃勃的精密网络，每一个进入网络空间的人既成为使用者，也成为这个巨大空间的构建者——就像在物理空间中一样。

然而，也正像这存在了几万年的人类文明一样，由人构建和使用的网络空间中也有善与恶的交锋，有建造与毁灭的平衡，网络空间的各种安全问题便由此产生。我们能够看到，随着互联网应用在深度和广度方面的不断拓展，如今的网络空间安全问题已经包含了越来越多的基础维度：设备安全、网络安全、应用安全、大数据安全等，包罗万象，影响着我们的日常学习、工作和生活的方方面面。从某种意义上来说，如何在网络空间中生存，已经是现代人必须要掌握的生存本领之一。

也许有人会说，从整个人类文明的角度来看，网络空间安全的各种理论和技术与数学、物理学、机械制造等经典学科或技术相比，还未脱懵懂；但互联网特有的高速进化能力让越来越多的不可能成为可能，就像刚刚在互联网上以全胜战绩击败了众多围棋大师的人工智能棋手 AlfaGo 一样。

就像狄更斯在《双城记》中所说：这是一个最好的时代，这是一个最坏的时代；这是一个智慧的年代，这是一个愚蠢的年代。网络空间的发展赋予了我们美好的生活，而各类网络威胁的存在也让我们有了守护这份安宁与美好的义务；智慧与愚蠢，在互联网时代只有一线之隔，所以前人积淀下的智慧才显得更为可贵。

我欣喜看到，国内有一批网络安全技术人才有着家国情怀，有热情、有理想，感恩于时代，也愿意为网安人才培养尽一份责任，他们愿意分享网安技术，为高校人才培养、课程体系尤其是实践教育提供平台支撑。永信至诚是其中的典型代表，经过近几年的发展，其提供的线上课程及实验深受师生欢迎，这次将课程整理成书，与高校师生分享，实在难能可贵。

这本书，相信可以在一定程度上向大家传递这种智慧。

未来，网络空间将迎来更多的建设者，蓬勃发展的互联网产业向我们证明了这一点。

未来，网络空间会涌现出更多的探索者，我们建造的这个世界还有很多领域等待开

拓，互联网的星辰大海正在召唤着我们。

未来，网络空间安全需要更多的守护者。

其路远，其路艰辛，其志笃定。

是为序。

封化民

教育部高等学校信息安全专业教学指导委员会秘书长

2017.5.8

于北京

前言

网络空间已经成为人类生存的“第五空间”，网络空间安全直接关系到国家安全、政治稳定、经济发展以及个人隐私安全，因此成为近年来国内外关注的焦点。保障网络空间安全，培养网络安全人才，这两项工作已经上升到国家战略的层面。

- 习近平总书记曾指出：“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 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上指出：“互联网主要是年轻人的事业，要不拘一格降人才。要解放思想，慧眼识才，爱才惜才。培养网信人才，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院。”
- 全国人民代表大会常务委员会于 2016 年 11 月 7 日发布《中华人民共和国网络安全法》，强调“支持培养网络安全人才，建立健全网络安全保障体系”。
- 国家互联网信息办公室于 2016 年 12 月 27 日发布并实施《国家网络空间安全战略》，指出要“实施网络安全人才工程，大力开展全民网络安全宣传教育，增强全社会网络安全意识和防护技能”。

有统计数字显示，当前，我国重要行业信息系统和信息基础设施需要各类网络空间安全人才约 70 万，预计到 2020 年，这个数字会增长到 140 万，并还会以每年 1.5 万人的速度递增。与之形成剧烈反差的是，我国高等学校每年培养的网络空间安全相关人才却不足 1.5 万人，远远不能满足行业发展对人才的需求。

2015 年，经教育部批准，网络空间安全一级学科正式设立，这标志着网络空间安全人才的培养进入新的阶段。网络空间安全领域需要多层次的复合型人才，他们不仅需要掌握坚实的理论知识，还要具备较强的实践能力，并掌握一定的领域知识，这样才能真正对抗不同领域面临的网络空间安全威胁。为此，除了高校根据网络空间安全一级学科的新要求进一步完善人才培养方案外，从事网络空间安全相关工作的企业也应加入人才培养的队伍中，与高校协作，在学校的教育阶段加强实践环节，帮助学生了解知识应用场景，从而培养出高素质的网络空间安全人才队伍。

本书正是基于上述背景，由高校一线教师和企业携手，结合编者多年网络安全工作经验及教学经验编写而成的，也是企业与高校共同进行网络空间安全专业课程建设的有益尝试。

网络空间安全涉及多学科交叉，知识结构和体系宽广，应用场景复杂，同时，相关知识更新速度快。作为一本导论课程教材，本书面向网络空间安全的初学者，力求为读者展示网络空间安全的技术脉络和基本的知识体系，为读者后续的专业课学习和深造打下基

础。因此，本书在内容组织和编写上，遵循以下理念：

1）发挥企业的优势，以行业视角融合基本的网络空间安全理论体系来组织全书内容，为读者展示从技术视角出发的网络空间安全知识体系。

2）以技术与管理为基础，按照“点—线—面”结合的方式组织具体的内容。点，是指网络空间安全领域的基本知识点；每一章在介绍基本知识点的基础上，通过案例、实际的应用场景，将这些知识点连接成一条线，使读者了解每一章（每个网络空间安全领域）的知识主线；有了每一章的知识主线，通过两个完整的大型案例，使读者理解如何应用网络安全技术和知识解决实际场景下的综合性问题，拓展知识面。最终，使学生全面掌握网络空间安全的基本技术架构。

3）突出前沿性和实用性。随着信息技术的发展，网络空间安全领域也出现了很多新问题，比如大数据安全、云安全、物联网安全等，本书对这些热点领域面临的安全问题和企业界现有的解决方案做了介绍，但限于篇幅以及领域的迅猛发展，本书无法介绍更多，读者可以根据自己的兴趣进一步学习与探究。同时，书中还引入编者实际工作中的很多案例，围绕其安全需求逐步展开，并给出完整的解决方案，使读者对常见的技术和工具有基本的认识和掌握。

4）突出安全思维的培养。网络空间安全从业人员与其他行业人员最大的不同在于其独有的一套思维方式。本书在介绍知识体系的同时，努力将网络空间安全领域分析问题、解决问题的思维方式和方法提炼出来，使读者学会从网络空间安全的角度思考问题，寻找解决方案。

5）丰富的学习和教学资源。为帮助高校教师使用本书进行教学，我们为教师配备了相关的教学辅助资源，读者可以通过教材及本书配套的学习和教学资源进一步深入学习。我们通过教材＋网络辅助学习资源的形式提供了完善的、贴近实际应用的课程体系，并提供大量配套的在线实操演练场景，面向广大个人用户提供便捷的网络安全实训服务，从而更加有效地辅助培养实践型网络安全人才。

本书从前期策划到最终成稿，得到了很多人的帮助和支持。教育部高等学校信息安全专业教学指导委员会秘书长封化民教授、清华大学崔勇教授、北京航空航天大学李舟军教授、公安大学马丁教授、浙江大学徐文渊教授、国际关系学院王标教授、北京信息科技大学赵刚教授、哈尔滨工业大学（威海）张兆心教授、南开大学贾春福教授、北京理工大学嵩天副教授在百忙之中对本书的编写进行了指导，对本书的内容框架和编写方针给出了极具价值的意见。

编者在编写本书的过程中参阅了大量的文献，其中包括大量专业书籍、学术论文、学位论文、国际标准、国内标准和技术报告等，在此向这些文献的原作者表示衷心的感谢和敬意！

由于网络空间安全学科还在飞速变化中，加之编者学识有限，书中难免有理解不准确或表述不当之处，恳请同行和各位读者不吝赐教，我们将不胜感激。

编者

2017 年 5 月

主编介绍

蔡晶晶 北京永信至诚科技有限公司创始人，董事长。从事网络安全相关工作17年，国内资深互联网安全专家之一。多年浸润攻防一线，培养出许多安全专家。中国国家信息安全漏洞库特聘专家，互联网网络安全应急专家组委员，2008年曾担任奥运安保互联网应急处置技术支援专家，并担任反黑客组组长。目前专注于网络空间安全学科人才的培养、企业安全能力的提高及公众安全意识的提升，创办的i春秋学院已成为国内影响力最大的信息安全教育机构，e春秋网络安全实验室已成为国内顶级信安赛事的支持平台。他相信信息安全技术是一种生存技能，并希望通过有温度的技术培育信息时代的安全感。

李炜 北京永信至诚科技有限公司副总裁，网络空间安全智能仿真和众测关键技术与服务北京市工程实验室主任。从事信息安全行业相关工作近15年，致力于安全架构、安全防护理念研究以及网络安全人才培养模式、框架、形式的探索和实践。中国网络空间安全协会竞评演练工作委员会委员，中国网络安全产业联盟人才培养工作组副组长，中国－欧盟第十九次中欧领导人峰会数字经济与网络安全专家工作组成员。参与梳理、设计实用型人才职业认定框架，与中国信息安全认证中心共同主导推出CISAW认证中“Web安全”“移动安全”两个全新的职业认证。具有“中国信息安全项目管理师”“微软MCSE认证专家”“Symantec SST”等资质。

学习建议

作为网络空间安全的入门教材，本书力求从技术和行业视角为读者展现网络空间安全的知识全景。网络空间安全知识体系宽广，技术更新速度快，实践要求高，我们建议读者在学习时遵循以下原则：

- 本书的每一章涉及网络空间安全的一个领域，建议学习过每一章之后，回顾各章的主题和要点，建立起网络空间安全的知识框架。这个知识框架对你后续深入学习和研究某一个安全领域至关重要。

- 由于是导论课程教材，因此本书每一章只给出某一领域概要性和框架性介绍。如果你对其中某个主题有兴趣，建议阅读该章最后列出的进一步学习材料或该主题相关的教材、参考书进一步学习。华章网站上会持续更新每一章相关的学习素材和资源，读者可定期关注并下载。

- 网络空间安全是一个实践性很强的学科，建议你在学习本书时尽量多动手实践。

- 在学习过程中向老师或他人请教和交流是很好的学习方式。建议你关注网络空间安全相关的技术、学习社区、公众号等，以获取技术和学习方法方面的更多建议。

读者可登录华章网站和i春秋学院获得本书更多的学习资源和信息。

封面设计：马天

目录

Chapter 1

第1章 网络空间安全概述

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，是一种基础资源。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、电视和手机等电子信息设备，人们将无法正常生活和工作。可以说，在信息时代，人们生存在物理世界、人类社会和信息空间组成的三维世界中。与此同时，网络空间安全变得前所未有地重要。

本章首先通过日常生活和工作中常见的一些网络安全问题案例让读者直观地感受网络空间安全实实在在地存在于我们身边，与我们的工作、生活息息相关。然后，通过引用三家国际机构的定义，引出网络空间安全的含义，深入地介绍网络空间安全包含的内容及当前面临的严峻形式。在介绍网络空间安全技术架构时，通过一张思维导图展示了网络空间安全中 12 个方面的内容及其之间的关系，这也是本书包含的主要内容。通过这张图，读者能初步了解从产业界角度所理解的网络空间安全都包含哪些内容、涉及哪些技术领域等。因为网络空间安全是一个崭新的领域，所以与工业革新、大数据一样，面临巨大的发展机会，能进一步促进新业态发展和技术变革。与此同时，我国在发展网络空间安全时还将面临攻击的高级性、威胁的多元性和危害的倍增性等诸多挑战。通过对网络空间安全的机遇与挑战的描述，可以看出网络空间安全的发展道路还很漫长，任重而道远。本章最后将通过一个案例和推荐的课外阅读材料让读者对

网络空间安全有更加深刻的认识，对这本书所列的技术架构有立体的认识，为学习后续章节的内容打下良好基础。

1.1 工作和生活中的网络安全

1.1.1 生活中常见的网络安全问题

一提到网络安全，很多人就会想到“黑客”，觉得网络安全很神秘，甚至离现实生活很遥远。但实际上，网络安全与我们的生活关系密切，网络安全问题屡有发生。比如，现实生活中，我们经常听到类似如下列举的安全事件。

1. QQ 账号密码被盗

不法分子通常在网络上购买病毒软件或者木马程序，再通过网络上各种信息搜集平台或工具，获得大量的用户邮箱信息，然后向这些邮箱群发伪装过且带有病毒或者木马的邮件，如用户无意中打开邮件，轻则会被不法分子盗取 QQ 密码，更严重的会被窃取隐私信息，给用户带来损失。

2. 支付宝账号被盗

经常有不法分子获得用户支付宝账户信息，导致用户支付宝内存款被转走，如果支付宝绑定了银行卡，还会出现银行卡被转账的情况。

3. 银行卡被盗刷

有时我们会收到陌生电话号码发来的短信，并含有很吸引人的图片或网络链接，如果我们没有注意，点击了短信中的图片或链接，就有可能被盗刷银行卡。此类事件在现实生活中已经层出不穷。

此外，我们还会遇到形形色色的网络安全事件，可见，网络安全问题已经渗透到我们的日常生活中。之所以出现这些网络安全问题，一方面是因为公众对网络安全问题的警惕性不高，另一方面也缺乏抵御网络安全威胁的知识，本书后面各章将陆续介绍防御这些网络威胁的技术和方法。

1.1.2 工作中常见的网络安全问题

在互联网时代，工作更多地依赖于互联网，因此，工作场景下也会遇到各类网络安全问题，下面给出了工作中常见的网络安全问题。

1. 网络设备面临的威胁

路由器是常用的网络设备，是企业内部网络与外界通信的出口。一旦黑客攻陷路由

器，那么就掌握了控制内部网络访问外部网络的权力，将产生严重的后果。

2. 操作系统面临的威胁

目前，我们常用的操作系统是 Windows 和 Linux，这两种系统也面临着网络安全威胁。一方面，操作系统本身有漏洞，黑客有可能利用这些漏洞入侵操作系统；另一方面，黑客有可能采取非法手段获取操作系统权限，对系统进行非法操作或破坏，因此操作系统的安全不容忽视。

3. 应用程序面临的威胁

计算机上运行着大量的应用程序，包括邮箱、数据库、各种工具软件等，这些应用程序也面临着严峻的网络安全问题。例如，邮箱因被攻击而无法正常提供服务，甚至导致邮件信息泄露，企业数据库被攻击会造成大量交易信息或用户信息泄露，等等。应用程序的安全与企业和用户的正常工作息息相关。

可见，工作场景下依然面临严峻的安全问题，随着本书的介绍，我们将学习到抵御这些风险和威胁的相关技术和手段。

1.2　网络空间安全的基本认识

通过上面的几个案例可以看出，伴随着互联网的不断普及和网络技术的快速发展，网络已经成为当今社会最广泛、最重要的基础设施之一，人们生活和工作日益离不开网络空间，随之而来的网络空间安全问题也日益增多。要想更好地避免和解决网络空间安全问题，首先需要了解什么是网络空间。

我们常说的网络空间，是为了刻画人类生存的信息环境或信息空间而创造的词。早在 1982 年，移居加拿大的美国科幻作家威廉·吉布森（William Gibson）在其短篇科幻小说《Burning Chrome》中创造了 Cyberspace 一词，意指由计算机创建的虚拟信息空间。在这里，Cyber 强调了电脑爱好者在游戏机前体验到的交感幻觉，表明 Cyberspace 不仅是信息的聚合体，也包含了信息对人类思想认知的影响。

后来，Cyberspace 一词逐渐被接受和熟悉，这也体现了网络空间概念的不断丰富和演化，与之相关的 Cybersecurity 一词开始进入大家的视野，被越来越多的人所提及。那么，什么是网络空间安全呢？

实际上，由于网络空间安全的内涵丰富，涉及领域广泛，且这些领域在飞速发展中，因此尚未有公认的、准确的定义，我们只能从与其相关的不同侧面来认识这一新兴领域。本书将列出 ISO/IEC 27032:2012、ITU（国际电联）以及荷兰安全与司法部的文件中关于网络空间安全的定义，供大家参考。