高等院校网络空间安全专业实战化人才培养系列教材

郭启全　丛书主编

网络空间安全技术

连一峰　郭启全　张海霞　石拓　编著

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

内 容 简 介

本书共11章，围绕“网络空间安全技术”这一主题，第1章为概述，第2章为安全防护技术，第3章为监测感知技术，第4章为攻防对抗技术，第5章为安全检测评估技术，第6章为网络安全等级保护制度中的关键技术，第7章为关键信息基础设施安全保护制度中的关键技术，第8章为数据安全保护制度中的关键技术，第9章为新技术领域安全保护中的关键技术，第10章为人工智能与大数据技术在网络安全中的应用，第11章为大模型研究在网络安全中的应用。

本书是高等院校网络空间安全专业实战化人才培养系列教材之一，可作为网络空间安全专业的专业课教材，适合网络空间安全专业、信息安全专业以及相关专业的大学生、研究生系统学习，也适合各单位各部门从事网络安全工作者、科研机构和网络安全企业的研究人员阅读。

图书在版编目（CIP）数据

网络空间安全技术 / 连一峰等编著. -- 北京 : 电子工业出版社, 2025. 7. -- ISBN 978-7-121-50116-6

Ⅰ. TP393.08

中国国家版本馆CIP数据核字第2025YQ4122号

责任编辑：刘御廷　　文字编辑：张萌萌

印　　刷：

装　　订：

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：15　　字数：346千字

版　　次：2025年7月第1版

印　　次：2025年7月第1次印刷

定　　价：69.00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：（010）88254059，lyt@phei.com.cn。

高等院校网络空间安全专业
实战化人才培养系列教材

编委会

序 FOREWORD

在数字化智慧化高速发展的今天，网络和数据安全的重要性愈发凸显，直接关系到国家政治、经济、国防、文化、社会等各个领域的安全和发展。网络空间技术对抗能力是国家整体实力的重要方面，面对日益复杂的网络安全威胁和挑战，按照“打造一支攻防兼备的队伍，开展一组实战行动，建设一批网络与数据安全基地”的思路，培养具有实战化能力的网络安全人才队伍，已成为国家重大战略需求。

一、培养网络安全实战化人才的根本目的

在网络安全“三化六防”（实战化、体系化、常态化；动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控）理念的指引下，网络安全业务越来越贴近实战。实战行动和实战措施都离不开实战化人才队伍的支撑。培养网络安全实战化人才的根本目的，在于培养一批既具备扎实的理论基础，又掌握高新技术和前沿技术、具备攻防技术对抗能力，还能灵活运用各种技术措施和手段，应对各种网络安全威胁的高素质实战化人才，打造“攻防兼备”和具有网络安全新质战斗力的队伍，支撑国家网络安全整体实战能力的提升。

二、培养网络安全实战化人才的重大意义

习近平总书记强调：“网络空间的竞争，归根结底是人才竞争”，“网络安全的本质在对抗，对抗的本质在攻防两端能力较量”。要建设网络强国，必须打造一支高素质的网络安全实战化人才队伍。我国网络安全人才特别是实战化人才严重缺乏，因此，破解难题，从网络安全保卫、保护、保障三个方面加强实战化人才教育训练，已成为国家重大战略需求。

当前，国家在加快推进数字化智慧化建设，本质是打造数字化生态，而数字化建设面临的最大威胁是网络攻击。与此同时，国家网络安全进入新时代，新时代网络安全最显著的特征是技术对抗。因此，新时代要求我们要树立新理念、采取新举措，从网络安全、数据安全、人工智能安全等方面，大力培养实战化人才队伍，加强“网络备战”，提升队伍的技术对抗和应急处突能力，有效应对新威胁和新技术带来的新挑战，为国家经济发展保驾护航。

三、构建新型网络安全实战化人才教育训练体系

为全面提升我国网络安全领域的实战化人才培养能力和水平，按照“理论支撑技术、技术支撑实战”的理念，创新高等院校及社会差异化实战人才培养的思路和方法，建立新型实战化人才教育训练体系。遵循“问题导向、实战引领、体系化设计、督办落实”四项原则，认真落实“制定实战型教育训练体系规划、建设实战型课程体系、建设实战型师资队伍、建设实战型系列教材、建设实战型实训环境、以实战行动提升实战能力、创新实战

型教育训练模式、加强指导和督办落实”八项重大措施，形成实战化人才培养的“四梁八柱”，有力提升网络安全人才队伍的新质战斗力。

四、精心打造高等院校网络空间安全专业实战化人才培养系列教材

在有关部门的大力支持下，具有 20 多年网络安全实战经验的资深专家统筹规划和整体设计，会同 20 多位部委、高等院校、科研机构、大型企业具有丰富实战经验和教学经验的专家学者，共同打造了 14 部技术先进、案例鲜活、贴近实战的高等院校网络空间安全专业实战化人才培养系列教材，由电子工业出版社出版，以期贡献给读者最高水平、最强实战的网络安全重要知识、核心技术和能力，满足高等院校和社会培养实战化人才的迫切需要。

网络安全实战化人才队伍培养是一项长期而艰巨的任务，按照教、训、战一体化原则，以国家战略为引领，以法规政策标准为遵循，以系统化措施为抓手，政府、高校、企业和社会各界应共同努力，加快推进我国网络安全实战化人才培养，为筑梦网络强国、护航中国式现代化贡献我们的智慧和力量！

郭启全

前言 PREFACE

网络安全关键技术包括安全防护技术、监测感知技术、攻防对抗技术、安全检测评估技术等。掌握网络安全关键技术极为重要，能否在网络空间领域有效维护国家安全、促进经济社会健康发展、保障人民群众的根本利益，关键看是否具备网络安全实战能力。

进入新时代，网络安全最显著的特征是技术对抗，因此应树立新理念，采取新举措，立足有效应对大规模网络攻击，认真落实“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施，按照“打造一只攻防兼备的队伍，开展一组实战演习行动，建设一批网络与数据安全基地”这条主线，加强战略谋划和战术设计，建立完善的网络安全综合防御体系，大力提高综合防御能力和技术对抗能力。从创新角度出发，按照“理论支撑技术、技术支撑实战”的理念，加强理论创新和技术突破，实施“挂图作战”；从“打造一支攻防兼备的队伍”出发，创新高等院校和企业差异化网络安全人才培养思路与方法，建立实战型人才教育训练体系，加强教育训练体系规划，强化课程体系、师资队伍、系列教材、实训环境建设和培养模式创新，培养网络安全实战型人才。

为了满足培养网络安全实战型人才的需要，郭启全组织成立编委会，共同编写高等院校网络空间安全专业实战化人才培养系列教材，包括《网络安全保护制度与实施》《网络安全建设与运营》《网络空间安全技术》《商用密码应用技术》《数据安全管理与技术》《人工智能安全治理与技术》《网络安全事件处置与追踪溯源技术》《网络安全检测评估技术与方法》《网络安全威胁情报分析与挖掘技术》《数字勘查与取证技术》《恶意代码分析与检测技术》《恶意代码分析与检测技术实验指导书》《漏洞挖掘与渗透测试技术》《网络空间安全导论》。全套教材由郭启全统筹规划和整体设计，并组织具有丰富的网络安全实战经验和教学经验的专家、学者撰写这套高等院校网络空间安全专业教材，且对内容严格把关，以期贡献给读者较高水平、较强实战的网络安全、数据安全、人工智能安全等方面的重要内容。

《网络空间安全技术》全面系统地介绍了安全防护技术、监测感知技术、攻防对抗技术、安全检测评估技术四类技术，以及云计算、大数据、物联网、工业互联网、移动互联网、卫星互联网、人工智能等新技术、新应用，并围绕网络安全制度建设的体系化要求，包括网络安全等级保护、关键信息基础设施安全保护、数据安全保护三项重要制度，以及新技术领域安全保护工作等，分别对其技术要求进行阐述，介绍如何利用网络空间安全技术达到相应的体系化安全要求。

本书由连一峰、郭启全、张海霞、石拓编著，第 1、2、4、6、8、9 章由连一峰撰写，第 3、5、7 章由张海霞撰写，第 10、11 章由石拓撰写。全书由郭启全设计、组织和统稿。

本书得到了国家重点研发计划（课题编号：2023YFB3107203）的支持，展现了作者长期从事网络安全领域管理、科研和教学的工作成果。本书的撰写工作得到了网络空间地理学实验室和中国科学院软件研究所相关科研、教学人员及研究生的帮助，在此一并表示感谢。

由于作者水平有限，书中不当之处在所难免，恳请读者批评指正！

作者

目录 CONTENTS

第 11 章

大模型研究在网络安全中的应用

第 1 章 概　述

本章讲述网络空间安全技术的总体概况，分析网络安全问题产生的历史背景，定义网络安全的基本属性，介绍网络空间安全技术发展的重要阶段，描述各个阶段典型的安全模型，并给出通用的网络空间安全技术体系框架，为本书后续章节的学习奠定基础。本章重点内容：网络安全的六项基本属性、网络安全模型和网络安全技术体系。

1.1 技术背景

信息安全问题在人类社会几千年的发展过程中始终以不同的形式存在。在政治活动、军事战争、社会生产、商业贸易、科学研究、技术竞争，以及个人活动中，出于保护个人、家庭、家族、群体、机构、单位、组织、地区、行业、国家利益的目的，常常希望其他人或其他群体不能获取、知悉、掌握、篡改某些重要信息，或希望保证信息内容在知悉范围内真实可信。

自古以来，信息的保密问题一直受到重视。公元前 431 年至公元前 404 年，雅典和斯巴达之间发生了历史上著名的伯罗奔尼撒战争。战争过程中，斯巴达军队抓获了一名雅典信使，从他身上搜出一条写满了希腊字母的腰带。这些看似杂乱无章的希腊字母引起了斯巴达军队统帅的注意。当他把腰带呈螺旋形缠绕在剑鞘上时，那些字母竟然在特定位置组成了文字，原来这是雅典间谍送回的军事情报。斯巴达军队根据情报迅速调整了作战计划，从而获得了这场战争的最终胜利，这就是斯巴达密码棒的典故。斯巴达密码棒如图 1-1 所示，它属于典型的移位加密方法，通过改变文本中字母的阅读顺序来达到对信息文本加密的目的。

图 1-1　斯巴达密码棒

另一个经典的密码是恺撒密码，如图 1-2 所示，它来源于古罗马时期著名的统治者——恺撒大帝。据说为了在战争中秘密传递情报和命令，恺撒大帝自行设计了一种密码机制，将情报和命令中的每个字母都用顺序推后 3 位的字母来替换，例如，将字母 A 替换为字母 D，将字母 E 替换为字母 H，这就形成了加密的情报和命令。解密时只需要将接收到的加密信息反过来替换就可以获知原文信息。恺撒密码属于典型的替换密码方法，通过将原文中的字母用其他字母替换来达到加密的目的。

图 1-2　恺撒密码

太平洋战争期间，情报信息的保密和破译工作同样至关重要。1942 年 6 月 4 日，日美两国海军主力舰队在中途岛周边海域展开激烈搏杀。踌躇满志的日军对此战志在必得，结果战役结束时，日军 4 艘航母被毁，太平洋战争的战略局势顿时逆转。中途岛战役真正激烈的战斗过程仅十余个小时，却留下很多传奇故事。在这场扭转局势的战役中，有一个默默无闻的群体，虽然不上战场奋勇拼杀，却在幕后做出了特别贡献，那就是以约瑟夫·罗彻福特为代表的美军太平洋舰队情报部密码破译组，他们成功破译了日本海军的密码，在战前准确掌握日军动向，使情报工作成为美军赢得此战的关键因素之一。

我国古代著名的军事家孙武在《孙子兵法》中写道：“能而示之不能，用而示之不用，近而示之远，远而示之近。”这显示了孙武对军事信息保密的重视，也代表了我国古代对于信息安全这一领域的初步认知。随着人类存储、处理和传输信息方式的变化和进步，网络安全的内涵和实践不断深化、延拓。从政府、军队专享的通信保密，发展到后来的数据保护、系统安全、信息保障，网络安全的概念已经不局限于信息内容的保密和保护，而是对支撑国家和社会发展运行的网络、信息系统、数据、平台及基础设施等的全方位安全保护，包含了防护、监测、感知、评估、处置、对抗等各个环节。

1.2 基本属性

网络安全可被理解为网络和信息系统抵御意外事件或恶意行为的能力，这些意外事件或恶意行为将危及所存储、处理或传输的数据，或者将危及经由这些网络和信息系统所提供的服务的机密性、完整性、可用性、非否认性、真实性和可控性。以上六项属性被普遍认为是网络安全的基本属性[1-2]，其具体含义如下。

1. 机密性（Confidentiality）

机密性能够确保敏感或机密数据的传输和存储不出现未授权的浏览或访问，甚至可以做到不暴露保密通信的事实。

2. 完整性（Integrity）

完整性能够保证被传输、接收或存储的数据，以及网络和信息系统内的软件、程序等内容是完整的和未被篡改的，且在被篡改的情况下能够发现被篡改的事实或被篡改的位置。

3. 可用性（Availability）

可用性是指即使在突发事件下，依然能够保障数据和服务的正常使用，例如，面对网络攻击、计算机病毒感染、系统崩溃、战争破坏、自然灾害等突发事件时。

4. 非否认性（Non-repudiation）

非否认性能够保证网络和信息系统的操作者或信息的处理者不能否认其行为或处理结果，这可以防止参与某次操作或通信的一方事后否认该事件曾发生过。

5. 真实性（Authenticity）

真实性也称为可认证性，能够确保实体（如人、进程或系统）身份或信息、信息来源的真实性。

6. 可控性（Controllability）

可控性能够掌握和控制网络系统的基本情况，可对网络系统的使用实施可靠的授权、审计、责任认定、传播源追踪和监管等控制措施。

从工程角度而言，一个安全的网络和信息系统是指“一个按预期运作方式进行的可靠系统”。这意味着系统不会出现超预期的运作方式，也意味着系统的所有状态和运行数据都是可预期的。在这种情况下，这个系统是可以受到信赖的。那么，这种信赖程度可以计量吗？所谓的预期运作方式是如何确定的？如何检验和判断系统是否出现了超出预期的运作方式？这些都是在工程实践中需要解决的问题。

网络安全是理论与实践紧密结合的学科领域。网络安全首先应建立在理论基础之上。研究人员创造或设计了针对网络和信息系统的安全模型，并用数学方法描述其安全属性，且证明了模型的安全性。此外，网络安全也注重解决实际问题。研究人员围绕安全漏洞、

网络攻击、攻击检测、技术对抗等领域开展了大量工作，极大地拓展和丰富了网络安全领域的技术体系与应用范围。

网络安全是典型的交叉学科，数学、物理学、电子学、计算机科学是其学科发展的基础，数论、微积分、数理统计、信息论、图论、操作系统、网络协议、计算方法、软件工程、电子工程、通信技术等各领域的基础理论和专业技术都会在网络安全中得到应用。随着各类新型信息技术的不断涌现，网络安全更进一步拓展出了云计算/云服务安全、物联网安全、工业控制系统安全、移动互联网安全、卫星互联网安全等各类新型的细分领域。

1.3 发展历程

网络安全包括针对数据的保护、鉴别、验证、审计、修复，以及针对产生、处理、存储、传输、使用、修改、更新、删除数据的网络和信息系统的保护、鉴别、验证、审计、修复。同时，识别针对网络和信息系统的攻击、渗透、入侵、篡改、破坏等行为，以及用于应对上述攻击等行为所需要的监测、感知、还原、刻画、处置、阻断、预警、反制等技术，也都属于网络安全的范畴。另外，由于网络安全工作依赖人员和组织机构的密切参与，因此网络安全领域也包含管理、运营等非技术因素。

1. 网络安全发展阶段

网络安全是一个古老而又年轻的学科领域。网络安全之前的发展主要围绕信息保密的问题。在全球政治、军事、经济、科技等多领域的驱动下，网络安全的发展步入了快车道，其内涵不断延伸。网络安全已经由原先依靠经验和灵感的一门“技艺”发展成为依靠理论体系和关键技术的“科学”。纵观网络安全的发展，可以将其划分为以下五个阶段[3]。

第一阶段：通信安全

20 世纪 60 年代之前，网络安全领域关心的是通信过程中数据的机密性。最初，人们仅以实物或特殊符号传递机密，后来出现了一些朴素的信息伪装方法。

北宋年间，曾公亮与丁度合著的《武经总要》反映了北宋军队对军令的伪装方法。按现在的观点，它综合了基于密码本的加密和基于文本的信息隐藏：先将全部 40 条军令编号合并成密码本，以 40 字诗对应位置上的文字代表相应编号。在通信中，代表某编号的文字被隐藏在一个普通文件中，但接收方知道该文字在 40 字诗中的位置，这样可以通过查找它该位置获得编号，再通过密码本获得军令。

在古代欧洲，代换密码和隐写术得到了较多的研究和应用[4]。德国学者 Trithemius 于 1499 年完成了《隐写术》的撰写。该书于 1606 年才得以正式出版，它记载了古代欧洲人在文本中进行信息隐藏的方法。

自 19 世纪 40 年代发明电报后，安全通信主要面向保护电文的机密性，且密码技术成为保护机密性的核心技术[4]。在两次世界大战中，各发达国家均研制了自己的密码算法和密码机，例如，第二次世界大战中德国的 ENIGMA 密码机、日本的 PURPLE 密码机，但

当时的密码技术本身并未摆脱主要依靠经验的设计方法，且在技术上缺乏安全可靠的密钥（密码本）分发方法，因此在两次世界大战中对战双方均有大量的密码通信被破解。以上密码技术缺乏完整的理论基础，因此被统称为古典密码。

1949 年，著名的信息论创始人香农发表论文《保密系统的通信理论》[5]，提出了著名的香农保密通信模型，明确了密码设计者需要考虑的问题，并用信息论阐述了保密通信的原则，这为对称密码学奠定了理论基础，从此密码学发展成为一门科学。

第二阶段：计算机安全

计算机的出现是 20 世纪的重大事件，它深刻改变了人类处理和使用信息的方法，网络安全的内涵也逐步扩展到了计算机和信息系统安全。

20 世纪 60 年代出现了多用户操作系统，由于需要解决多用户间的安全共享问题，人们对网络安全的关注点在数据机密性的基础上扩展到了用户的访问控制与认证，并开始关注系统的可用性。1965 年至 1969 年间，美国军方和科研机构组织开展了有关操作系统安全的研究。1972 年，Anderson 提出了计算机安全涉及的主要问题与模型 [6]。

进入 20 世纪 80 年代后，随着密码技术和其他类型安全技术的不断发展，人们在计算机安全方面开始了标准化和商业应用的进程。1985 年，美国国防部发布了可信计算机系统评估准则（Trusted Computer System Evaluation Criteria，TCSEC），推进了计算机安全的标准化和测试评估工作。人们逐渐认识到保护计算机系统（不仅限于保护单台计算机）的重要性。Anderson 最早提出了入侵检测系统（Intrusion Detection System，IDS）的概念 [6]，详细阐述了主机入侵检测的概念和架构，这标志着网络安全领域诞生了一项新的技术类型——入侵检测。

在密码学方面，Diffie 和 Hellman 于 1976 年发表了论文《密码编码学新方向》[7]，指出通信双方不直接传输加密密钥的保密通信是可能的，并提出了非对称公钥加密的设想；美国国家标准技术研究所（National Institute of Standardization and Technology，NIST）于 1977 年首次通过公开征集的方法制定了当时应用上急需的“数据加密标准”（Data Encryption Standard，DES），推动了分组密码的发展。这两个事件标志着现代密码学的诞生。1978 年，Rivest、Shamir 与 Adleman 设计了著名的 RSA 公钥密码算法 [8]，实现了 Diffie 和 Hellman 提出的公钥思想，使数字签名和基于公钥的认证成为可能。

第三阶段：信息安全

随着信息技术越来越广泛的应用，20 世纪 80 年代中期至 20 世纪 90 年代中期，政府机关、军事部门、学术界、产业界对信息和信息系统的安全越来越重视。人们所关注的安全问题逐渐扩大到 1.2 节描述的网络安全六个基本属性。在这一时期，密码学、安全协议、计算机安全、安全评估等理论和技术得到了较大发展，尤其是互联网的普及大大促进了安全技术的发展与应用。这一时期不但学术界提出了很多新观点和新方法，如椭圆曲线密码（Ellipse Curve Cryptography，ECC）、密钥托管和盲签名等，标准化组织与产业界也制定了大量的算法标准和实用协议，如数字签名标准（Digital Signature Standard，DSS）、因特网安全协议（Internet Protocol Security，IPSec）、安全套接字层（Secure Socket Layer，

简称 SSL）协议等。此外，安全多方计算、形式化分析、零知识证明等均取得了进展，一些理论成果也逐渐得到应用。

自美国国防部发布 TCSEC 起，世界各国根据自己的实际情况相继发布了一系列安全评估准则和标准：英国、法国、德国、荷兰于 20 世纪 90 年代初发布了信息技术安全评估准则（Information Technology Security Evaluation Criteria，ITSEC）；加拿大于 1993 年发布了可信计算机产品评价准则（Canadian Trusted Computer Product Evaluation Criteria，CTCPEC）；加拿大、法国、德国、荷兰、英国和美国的 NIST 与美国国家安全局（National Security Agency，NSA）于 20 世纪 90 年代中期提出了信息技术安全性评估通用准则（Common Criteria，CC）。

随着计算机网络的发展，这一时期的网络攻击行为逐渐增多，传统的安全保密措施难以抵御黑客入侵及有组织的网络攻击。学术界和产业界先后提出了基于网络的 IDS（NIDS）、分布式 IDS（DIDS）、防火墙等网络系统防护技术。1989 年美国国防部资助卡内基梅隆大学建立了世界上第一个计算机应急小组及协调中心（Computer Emergency Response Team/Coordination Center，CERT/CC），标志着网络安全从静态防护阶段过渡到主动防护阶段。

第四阶段：信息保障

20 世纪 90 年代中期以来，随着信息安全越来越受到各国的高度重视及信息技术本身的发展，人们更加关注信息安全的整体发展及在新型应用下的安全问题。人们也开始深刻认识到安全是建立在完整过程的基础上的，这包括“预警、保护、检测、响应、恢复、反制”整个过程。信息安全的发展也越来越多地与国家战略结合在一起。欧洲委员会从信息社会技术（Information Society Technology，IST）规划中出资 33 亿欧元，启动了“新欧洲签名、完整性与加密计划（New European Schemes for Signature, Integrity, and Encryption，NESSIE）”项目，对分组密码、流密码、杂凑函数、消息认证码、非对称加密、数字签名等算法进行了广泛征集。日本、韩国等国家也先后启动了类似的计划。美国的 NIST 先后组织制定、颁布了一系列的网络安全标准，并用高级加密标准（Advanced Encryption Standard，AES）取代 DES 成为新的分组密码标准。我国也先后颁布了一系列与安全相关的标准，并于 2004 年 8 月颁布了《电子签名法》。

在电子商务和电子政务等应用的推动下，公钥基础设施（Public Key Infrastructure，PKI）逐渐成为国民经济的基础，它为需要密码技术的应用提供基础支撑。在这一时期，新型网络、新型计算和新型应用环境下的算法和协议设计也逐渐成为热点问题，主要包括移动网络、传感器网络或 Ad-Hoc 网络下的算法和安全协议、量子密码及其协议，信息隐藏、数字版权保护和电子选举等。

为了保护日益庞大和重要的网络系统，信息保障的重要性被提到空前的高度。1995 年美国国防部提出了“保护—监测—响应”的动态模型，即 PDR 模型，后来增加了恢复环节，成为 PDRR（Protection, Detection, Reaction, Restore）模型。1998 年 10 月，NSA 颁布了信息保障技术框架（Information Assurance Technical Framework，IATF），以后

又分别于 1999 年、2000 年和 2002 年颁布了改进的版本。自 2001 年 9 月发生“9.11”事件以来，美国政府以“国土安全战略”为指导，出台了一系列信息保障策略，将信息保障体系纳入国家战略中，如 2003 年 2 月通过了“保护网络安全的国家战略”。一些具有国际影响力的国家也高度重视信息安全战略，如欧盟于 2007 年 3 月颁布了“信息社会安全战略”，以期全面建立信息保障机制。日本提出了“防卫力量配备计划”，以防止遭受信息武器的突袭和对国内信息网络的突发事件保持警惕。俄罗斯发表了《国家信息安全学说》，成立了国家信息安全与信息对抗领导机构，组建了特种信息战部队。在我国，国家信息化领导小组于 2003 年出台了“国家信息化领导小组关于加强信息安全保障工作的意见”（中办发〔2003〕27 号文），是我国信息安全领域的指导性和纲领性文件。

第五阶段：网络空间安全

网络安全最新的发展阶段被称为“网络空间安全”。空间是与时间相对的一种物质的客观存在形式，两者密不可分。时间是物质的延续性、间隔性和顺序性的表现，空间是物质的广延性和伸张性的表现。按照宇宙大爆炸理论，宇宙从奇点爆炸之后，由初始状态分裂开来，从而有了存在形式、运动状态等方面的差异。物与物的位置差异度量称为“空间”。空间由长度、宽度、高度、大小等参量表现出来。空间是一个相对概念，既包含宇宙空间、物理空间、地理空间、建筑空间等实体空间的范畴，也包含思维空间、逻辑空间、数字空间、社会空间、网络空间等虚拟空间的范畴。

网络空间是一种依托于实体空间存在的新型空间形态，是在计算技术、网络技术、虚拟化技术等信息技术的支撑下，物理空间和社会空间在虚拟世界的投影。网络空间关系到政治、经济、文化、军事、科技、教育等社会生产生活的方方面面。国内外学者对网络空间概念进行了研究和阐述。基于不同应用需求及研究领域，网络空间被赋予了不同的内涵和外延：有些概念强调网络空间的物质属性，认为网络空间依附于软硬件设备等物质基础，是互联网与万维网的近似概念；有些概念强调网络空间的社会属性，认为网络空间是人基于互联网技术与社交行为结合产生的“空间感”，并将网络空间视为人在再现的空间中对社会的感知，认为社会性的交互行为比技术内容更能体现网络空间的本质内涵；还有一些概念则强调网络空间中的操作和活动，认为网络空间是创造、存储、调整、交换、共享、提取、使用和消除信息与分散的物质资源的全球动态领域 [9]。

2. 网络空间基本含义

从上述描述中可以看出，网络空间具有物质属性 (软硬件等基础设施) 和社会属性 (人的交互行为及其操作)。早期的定义从不同角度强调了网络空间中的某种组成要素，但是均未全面、系统地对网络空间的要素进行概括和描述。不同的国家或机构从不同的角度对网络空间进行了定义。

（1）2003 年美国总统国家安全令给出的定义：“网络空间是一个关联信息技术基础设施的网络，包括互联网、电信网、计算机系统及关键产业中的嵌入式处理器和控制器。通常该术语在使用时，也代表信息虚拟环境及人们之间的相互影响。”

（2）2006 年美军参谋长联席会议出台的《网络空间国家军事战略》给出的定义：“网络空间是一个作战领域，其特征是通过互联的信息系统和相关的基础设施，利用电子技术和电磁频谱产生、存储、修改、交换和利用数据。通俗地说，网络空间与陆、海、空、天一样，是由电磁频谱、电子系统及网络基础设施组成的一个作战领域。”

（3）2014 年俄罗斯公布的《俄罗斯联邦网络安全战略构想（草案）》给出的定义：“信息空间是指与形成、创建、转换、传递、使用、保存信息活动相关的，能够对个人和社会认知、信息基础设施和信息本身产生影响的领域。网络空间是指信息空间中基于互联网和其他电子通信网络沟通渠道，包括保障这些渠道运行的技术基础设施，以及在这些渠道和设施上进行活动的任何形式的领域（包括个人、组织、国家）。”

（4）2009 年英国《网络安全战略》给出的定义：“网络空间包括各种形式的网络化和数字化活动，其中，包括数字化内容或通过数字网络进行的活动。网络空间的物理基础是计算机和通信系统，因此，以前在纯物理世界中不可以采取的行动，如今在这里都可以实现。”

（5）2011 年法国《信息系统防御和安全战略》给出的定义：“网络空间是由数字资料自动化处理设备在全世界范围内相互连接构成的交流空间。网络空间是分享世界文化的新场所，是传播思想和实时资讯的光缆，是人与人之间交流的平台。”

（6）2011 年德国《网络安全战略》给出的定义：“网络空间是指在全球范围内，在数据层面上的所有信息技术（IT）系统的虚拟空间。网络空间的基础是互联网。互联网是可公开访问的通用连接与传输网络，可以由其他数据网络补充及扩展得到。孤立的虚拟空间中的 IT 系统并非网络空间的一部分。”

（7）2011 年新西兰《网络安全战略》给出的定义：“网络空间是由相互依赖的信息技术基础设施、电信网络和计算机处理系统组成的，即时在线通信的全球性网络。”

可以看出，上述定义有些强调网络空间的物质属性，有些侧重网络空间的社会属性，也有些两者兼顾。参考上述定义，结合国内外研究机构对网络空间的理解和认识，研究人员给出了网络空间的定义：网络空间是一个由相关联的基础设施、设备、系统、应用和人等组成的交互网络，利用电子方式生成、传输、存储、处理和利用数据，并通过对数据的控制，实现对物理系统的操控并影响人的认知和社会活动 [10]。

3. 网络空间安全的定义

针对网络空间安全的概念，不同的国家或机构也对其进行了定义，典型的有：

（1）2014 年美国推出的《增强关键基础设施网络安全框架》（1.0 版）给出的定义：“网络空间安全是通过预防、检测和响应攻击以保护信息的过程。”该框架提出网络空间安全风险管理生命周期五环论，由识别、保护、检测、响应、恢复组成，并进一步细分为 22 类活动、98 个子类。

（2）2014 年《俄罗斯联邦网络安全战略构想（草案）》给出的定义：“网络空间安全是指网络空间的所有组成部分均处于能够防范潜在威胁及其后果影响的状态。”

（3）2009 年英国《网络安全战略》给出的定义：“网络空间安全包括在网络空间对英国利益的保护和利用网络空间带来的机遇，实现英国安全政策的广泛化。”

（4）2011 年法国《信息系统防御和安全战略》给出的定义：“网络空间安全是信息系统的理想模式，可以抵御任何来自网络空间的威胁，这些威胁可能损害系统存储、处理或传递的数据和相关服务的可用性、完整性或机密性。”

（5）2011 年德国《网络安全战略》给出的定义：“网络空间安全是大家所期待实现的 IT 安全目标，即将网络空间的风险降到最低。”

（6）2011 年新西兰《网络安全战略》给出的定义：“网络空间安全是指由网络构成的网络空间要尽可能保证其安全，防范入侵，且保持信息的机密性、可用性和完整性，能够检测确实发生的入侵事件，并即时响应和恢复网络。”

参考上述定义，结合国内外研究机构对网络空间安全的理解和认识，研究人员给出了网络空间安全的定义：网络空间安全是通过识别、保护、检测、响应和恢复等环节，以保护信息、设备、系统或网络免受威胁和损害 [10]。

1.4　网络安全模型

网络安全模型是关于网络和信息系统在何种环境下会遭受威胁，且如何实现网络安全的一般性描述。在一些文献中，网络安全模型也被称为威胁模型或敌手模型。明确网络安全模型有助于说明和了解网络空间安全技术原理。

1. 网络安全模型的发展

早期的网络安全模型主要侧重于保密通信领域，包括：香农提出了保密通信系统的模型 [5]，该模型描述了保密通信的收发双方通过安全信道获得密钥、通过可被窃听的线路传递密文的场景，确定了收发双方和密码分析者的基本关系和所处的技术环境；Simmons 面向认证系统提出了无仲裁认证模型 [11]，它描述了认证方和被认证方通过安全信道获得密钥、通过可被窃听的线路传递认证消息的场景；Dolve 和 Yao 针对一般的网络安全体系提出了 Dolve-Yao 威胁模型 [12]，它定义了攻击者在网络和系统中的攻击能力，被密码系统的设计者广泛采用；随着密码技术研究的深入，很多学者认为密码系统的设计者应该将攻击者的能力估计得更高一些，例如，攻击者可能会有控制加密设备或在一定程度上接近、欺骗加密操作人员的能力。

后续的网络安全模型重点针对访问控制领域，典型的有：Harrison、Ruzzo 和 Ullman 提出的基于访问控制矩阵（HRU）的模型，这是一种基本的自主访问控制（Discretionary Access Control，DAC）模型；Bell 和 LaPadula 于 1973 年至 1976 年间提出的强制访问控制模型即 Bell-LaPadula（BLP）模型，主要用于解决面向保密性的访问控制问题；Biba 等人在 1977 年提出的 BIBA 模型，是 BLP 模型的变体，目的是保护数据的完整性；Dion 于 1981 年提出同时面向保护机密性和完整性的 Dion 模型，它结合了 BLP 模型和 BIBA 模

型，但只提供强制性策略。访问控制模型将在本书的第 2 章中进行详细介绍。

在互联网时代，信息系统跨越了公用网络和组织机构的内部网络，网络安全的内涵在不断扩展。保密通信、安全认证、访问控制是满足机密性、完整性、真实性和非否认性的主要手段，但可用性和可控性的要求不能完全依靠它们解决。因此，进入信息保障阶段后，网络安全模型不再局限于保密通信、访问控制等具体细分领域的安全问题，而是开始关注网络和信息系统的整体安全保护。如美国国防部提出的“保护—监测—响应（PDR）”动态模型、增加了恢复环节（Restore）的 PDRR 模型、增加了安全策略（Policy）的 PPDR 模型，以及进一步增加了预警（Warning）和反击（Counter attack）的 WPDRRC 模型等。预警、监测、响应、反击等技术环节的加入，表明这一阶段的网络安全模型开始考虑网络对抗环境下的动态安全问题。例如，某单位使用的网络包括内部网和外部网两部分。典型的网络安全模型中包含的安全措施应包括主机内部网络安全构件、网络防护设施和网络安全机构。其中，主机内部网络安全构件主要指主机内部与网络安全相关的模块（如主机审计模块、用户认证模块、访问控制模块等）；网络防护设施主要包括防火墙、IDS 或防病毒网关等独立运行的安全设备；网络安全机构是专门负责实施安全措施的机构，它可以是由第三方或单位自行设立的，主要用于完成密钥管理、资产管理、用户管理、权限管理、安全策略管理等功能。在该模型下，攻击者不能在内部或外部通信网中的任何一点上截获数据或进行消息收发，也不能从一台被控制的计算机上发动网络攻击，还不能基于一个系统中的账号发动系统攻击等。网络安全的实施者主要通过以上网络安全构件和相应的管理制度形成动态的安全防御能力。

2. 网络空间与物理空间的关系

随着网络空间与物理空间的逐步融合，网络空间与物理空间之间呈现出复杂的关系形态，两者既相互区别，又密切联系。物理空间是人类通过自身感官可以直观感受到的实体空间，例如，通过视觉观察到的日月星辰、山川河流、建筑物、动植物等各类物体，通过听觉观察到的鸟鸣虫吟、语言音乐等自然界和人类社会发出的声音。网络空间的信息则通过计算机网络进行传输和处理，并经由信息终端以文字、图形、图像、音频、视频或其他虚拟现实方式进行呈现。与传统物理空间相比，虽然网络空间具有虚拟特性，但物理空间的时空关系仍旧是网络空间不可或缺的关键要素。网络空间所依托的信息基础设施和网民都是物理实体，本身也具有地理位置和地域性的差异，这取决于其中事物与现实物体的映射关系、信息所蕴含的物理属性和对现实空间的真实作用。网络空间与物理空间的关系主要体现在以下方面。

1）网络空间依赖物理空间的物质基础

网络空间是通过在真实物理空间中部署一系列的信息基础设施而逐步构建起来的。网络空间的信息基础设施主要包括网络基础设施、服务器、信息转换器和上网工具四部分 [17]。网络基础设施是网络空间构建的底层基础设施，由骨干网、城域网和局域网通过有线或无线传输方式层层搭建而成；服务器是指在网络环境下运行相应的应用软件，为网络用户提供共享信息资源和各种服务的一种高性能计算机；信息转换器是指在信息传输过

程中，负责信号转换和信息组织的设备，主要包括调制解调器、路由器、交换机和中继站；上网工具是网络空间的入口，是从现实世界进入虚拟世界的主要途径。

网络空间以物理空间为真实载体。网络空间的各项要素（信息系统、网络服务、虚拟身份、操作行为、网络通信、连通关系、数据交互关系、安全漏洞、网络攻击等）在本质上都依赖物理空间的物质基础而存在。由于网络资源的供给和部署在地理分布上往往是不均衡的，即总是倾向于人口和经济活动聚集的地方，因此，全球网络空间资源分布情况在空间上具有明显的不均衡性，这对网络空间的体系架构、空间格局和空间可达性造成了影响。

2）网络空间与物理空间同样存在地域性差异

网络空间的发展导致了人类通信方式的变革，例如，Facebook、微博、微信、抖音等，加速了互联网虚拟社区与现实社会的交互。在传统的社会交往中，由于地理上的邻近性、社会文化的较强认同感，周边生活、工作的群体往往成为人们最主要的社会交往对象。然而，在网络空间中，虽然信息技术压缩了时空距离，扩展了人们社会交往与联系的范围，但本地域的信息联系强度仍然远远大于与其他地域的信息联系强度，表现出本地域的信息联系在网络信息空间中占据主体地位的特征。

同时，网络空间是人类借助互联网媒体在整合多种信息与通信技术基础上所构建的虚拟空间。网络空间的行为主体对应现实世界中的组织机构或人类个体。社交网络空间中的个体在物理空间上都对应某一特定的地理位置。因此，人作为网络空间的行为主体，具有明显的地域特征。

3）网络空间与物理空间具有密切的关联性和互动性

网络虚拟实体与物理实体存在动态映射关系。物理空间中的个人可能在网络空间中拥有多重的虚拟身份，而网络空间的计算服务也可能是由分布在不同区域的物理设备通过虚拟化方式组合形成的。因此，网络虚拟实体与物理实体存在多对多的映射关系，且这种映射关系会受经济活动、社会发展、技术革新、法律法规、管理制度等多重因素的影响而发生动态变化。

此外，网络空间的信息流分布格局与地理距离和经济社会发展水平密切相关。例如，城市对外的网络信息不对称度与其经济社会发展水平具有相对一致性，经济社会发展水平越高，其在网络空间中的影响力相对就越强。城市之间的网络信息不对称度与它们之间的地理距离和经济社会发展水平密切相关，且随着地理距离的增加呈现出衰减的特性 [18]。

3. 构建网络空间安全模型的四个要素

网络空间安全的覆盖范围广泛，涉及专业领域众多，包含多维度、多品类、多层次的安全要素，构建网络空间的安全模型时，可以考虑以下四个层次的要素。

（1）网络环境要素是指各类网络空间要素形成的节点和链路，即网络结构、资源及拓扑关系。网络环境要素包括楼层、机房、机柜等网络设备所处的物理环境；网络拓扑和网络接入等逻辑环境；电商平台、网络论坛、社交媒体等网络场所；IP 地址、域名、网络服

务等网络资源。

（2）行为主体要素是指各类网络实体角色的真实身份和网络身份。行为主体要素包括行业、单位、人员及人员组织对应的邮箱、社交账号、联系方式等。行为主体要素主要关注网络实体的交互行为及其社会关系。

（3）业务环境要素是指重点关注的网络空间安全业务对象。例如，需要开展的网络安全等级保护、关键信息基础设施安全保护、网络安全监测、态势感知、事件研判、攻击溯源、应急处置、攻击阻断、威胁情报分析挖掘等业务工作内容。

（4）地理环境要素是指各类网络空间要素依附的地理载体，强调网络空间要素的地理属性。地理环境要素包括网络空间实体的行政区划、道路、设施等基础地理信息，交通管理设施、治安管理设施等公共安全地理信息，图像、音视频、建筑物三维模型等信息。这主要涉及设备及相关实体的距离、尺度、区域、物理边界、空间映射等概念。

因此，当网络安全发展到当前的网络空间安全阶段时，网络安全模型将呈现出多空间融合交汇的显著特点，通过在地理环境层、网络环境层、行为主体层和业务环境层中对网络空间安全相关的实体、属性及其关系进行交叉映射和融合，能充分反映出网络空间、物理空间和社会空间存在的多层次、多维度、跨空间的关联关系，由此构成了新时代下网络空间安全涵盖的综合体系。

1.5 技术体系

2015 年 6 月，“国务院学位委员会　教育部关于增设网络空间安全一级学科的通知”（学位〔2015〕11 号）内容如下：“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，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，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。”

围绕网络空间安全技术体系，研究人员提出了多种分类方式。例如，参考传统的网络安全等级保护技术标准，将网络空间安全技术分为物理安全、系统安全、网络安全、应用和数据安全等类型；或者将现有的网络空间安全技术归纳为五类，即核心基础安全技术（包括密码技术、信息隐藏技术等）、安全基础设施技术（包括标识与认证技术、授权与访问控制技术等）、基础设施安全技术（包括主机系统安全技术、网络系统安全技术等）、应用安全技术（包括网络与系统攻击技术、网络与系统安全防护与应急响应技术、安全审计与责任认定技术、恶意代码检测与防范技术、内容安全技术等）、支撑安全技术（包括安全测评技术、安全管理技术等）。

为了便于读者理解，在参考上述分类方法的基础上，本书按照网络空间安全实战的需求，将技术体系按照以下维度进行分类，如图 1-3 所示。

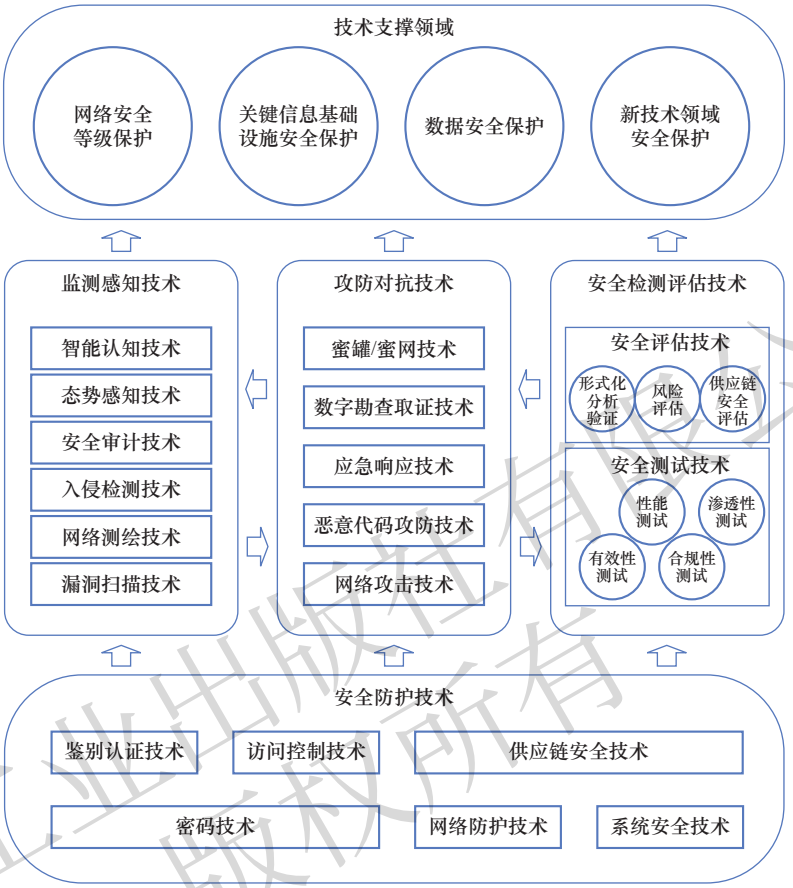

图 1-3　网络空间安全技术体系

1. 安全防护技术

安全防护技术侧重于传统的安全防护工作，主要目的是通过相应的技术手段，保障基础设施、系统、应用、数据的安全性，防范针对网络系统的未授权访问。它的具体内容包括密码技术、鉴别认证技术、访问控制技术、供应链安全技术、网络防护技术、系统安全技术等内容，将在本书的第 2 章详细介绍。

2. 监测感知技术

监测感知技术侧重于探测发现网络安全威胁行为，主要目的是通过相应的技术手段，监测、分析、感知网络中已经发生、正在发生或即将发生的威胁行为。它的具体内容包括漏洞扫描技术、网络测绘技术、入侵检测技术、安全审计技术、态势感知技术、智能认知技术等内容，将在本书的第 3 章详细介绍。

3. 攻防对抗技术

攻防对抗技术侧重于针对网络空间威胁的实战对抗，主要目的是掌握网络空间的攻击方式，例如，口令破解、后门攻击、拒绝服务（Denial of Service，DoS）、缓冲区溢出、APT 攻击、勒索病毒等，以便更好地开展处置响应工作。它的具体内容包括网络攻击技

术、恶意代码攻防技术、应急响应技术、数字勘查取证技术、蜜罐/蜜网技术等内容，将在本书的第 4 章详细介绍。

4. 安全检测评估技术

安全检测评估技术侧重于针对网络系统开展检测评估，以验证其安全合规情况和实际的安全保护能力。它的具体内容包括有效性测试、合规性测试、性能测试、渗透性测试、风险评估、供应链安全评估、形式化分析验证等内容，将在本书的第 5 章详细介绍。

在介绍完上述类型的关键技术后，为便于读者理解如何在实战中开展技术应用，本书在随后的第 6 章、第 7 章、第 8 章中分别围绕网络安全等级保护、关键信息基础设施安全保护、数据安全保护三项重要制度，阐述所包含的网络空间安全技术内容。在第 9 章中，重点针对新技术领域（云计算、算力网络、移动互联网、人工智能、量子计算等）的安全保护工作，分析目前所面临的安全挑战和技术思路。在第 10 章、第 11 章中本书介绍人工智能与大数据技术、大模型研究在网络安全中的应用及其发展趋势。

习　题

1. 简述网络安全的六项基本属性，分析六项基本属性的保护重点。
2. 简述网络空间安全当前发展阶段与历史阶段的主要区别。
3. 什么是网络空间？网络空间与物理空间的关系是什么？
4. 构建网络空间的安全模型时，可以考虑哪几个层次的要素？
5. 简述网络空间安全技术体系的分类。