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

网络空间安全导论

郭启全　张海霞　张　潮　荆继武　雷灵光
杨正军　魏　薇　景慧昀　吴云坤　刘　健　编著
王新猛　张　征　肖新光　王耀华　崔宝江

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

内 容 简 介

本书共 12 章，围绕“网络空间安全导论”这一主题，系统介绍网络空间安全的基本制度、基础知识、基本理论、基本技术。其中，第 1 章概括性介绍网络空间安全，第 2 章介绍网络安全保护制度与实施，第 3 章介绍网络安全建设与运营，第 4 章介绍商用密码应用技术，第 5 章介绍数据安全管理与技术，第 6 章介绍人工智能安全治理与技术，第 7 章介绍网络安全事件处置与追踪溯源技术，第 8 章介绍网络安全检测评估技术，第 9 章介绍数字勘查与取证技术，第 10 章介绍网络威胁情报分析与挖掘技术，第 11 章介绍恶意代码分析与检测技术，第 12 章介绍漏洞挖掘与渗透测试技术。

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，可做为高等院校基础课教材，适合所有专业大学生系统学习网络空间安全的基本制度、基础知识、基本理论、基本技术，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

网络空间安全导论 / 郭启全等编著. -- 北京 : 电子工业出版社, 2025. 7. -- ISBN 978-7-121-50081-7

Ⅰ. TP393.08

中国国家版本馆 CIP 数据核字第 20258QL265 号

责任编辑：刘御廷　　文字编辑：路　越

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：21　　字数：537.6 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）88254569，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

网络空间安全是一门综合数学、计算机科学与技术、密码学、信息与通信工程、软件工程、控制科学与工程等学科的交叉学科，包含网络安全法律、政策、标准、制度、管理、技术、情报、勘查取证等内容。习近平总书记指出：“没有网络安全就没有国家安全”，网络安全是保护我国经济健康发展，维护国家安全、社会秩序和公共利益的重要保障，与政治安全、经济安全、国土安全、社会安全共同构成了我国总体国家安全观。

进入新时代，网络安全最显著的特征是技术对抗，应树立新理念，采取新举措，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“打造一支攻防兼备的队伍，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，建立完善网络安全综合防御体系，大力提升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和方法，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需要，郭启全组织成立编委会，共同编著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，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，并对内容严格把关，以期贡献给读者最高水平、最强实战的网络安全、数据安全、人工智能安全等重要内容和技术。

《网络空间安全导论》一书由郭启全等编著，从第 1 章到第 12 章分别由张海霞、郭启全、张潮、荆继武、杨正军、魏薇、段晓光、刘健、王新猛、张征、肖新光、崔宝江编著。该书主要介绍网络空间安全的基本制度、基础知识、基本理论、基本技能，包括网络空间安全有关概念、网络空间安全技术体系、网络安全主要产品、网络安全态势分析、网络攻防技术对抗、网络空间地理学基础理论和技术实践、网络安全保护制度与实施、网络安全建设与运营、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、数据勘查与取证技术、网络威胁情报分析与挖掘技术、恶意代码分析与检测技术、漏洞挖掘与渗透测试技术，内容全面丰富。本书是高等院校基础课教材，也可以做为培训教材使用。

书中不足之处，敬请读者指正。

作者

目录 CONTENTS

第1章

网络空间安全概述

第 2 章

网络安全保护制度与实施

第 7 章

网络安全事件处置与追踪溯源技术

第 8 章

网络安全检测评估技术

第 9 章

数字勘查与取证技术

第 12 章

漏洞挖掘与渗透测试技术

第 1 章 网络空间安全概述

本章对网络空间安全进行概括性介绍，包括网络空间安全基本概念、基础知识、基本技术和研究内容、网络安全主要产品、国内外网络空间安全战略，以及网络空间安全技术体系框架等，为本书后续章节的学习奠定基础。

1.1 基本概念

1.1.1 网络空间

网络空间（Cyberspace）一词是控制论（Cybernetics）和空间（Space）两个词的组合，直译就是“赛伯空间”，我国学者将其翻译成“网络空间”“网域空间”等。由于其内涵和外延都不断在发展，不同的国家或机构和不同的人从不同的角度都有不同的理解。

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，包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统。

2014 年，俄罗斯发布的《网络安全战略构想》草案中指出：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、保障其运行的技术基础设施，以及直接使用这些渠道和设施的任何形式人（个人、组织、国家）活动的领域。

德国发布的《网络安全战略》中给出网络空间的定义：网络空间是指在全球范围内，在数据层面上链接的所有信息技术（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，可以用其他数据网络补充及扩展，孤立的虚拟空间中的 IT 系统并非是网络空间的一部分。

2016 年，我国《国家网络空间安全战略》中指出，网络空间由“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”。

通过上述这些定义，结合国内外学者对网络空间的理解和认识，本书中沿用以下定

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，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[1]。网络空间实际上是一个虚实结合的特殊宇宙空间，在这个空间中，物联网使得虚拟世界与物理世界加速融合，云计算使得网络资源与数据资源进一步集中，泛在网保证人、设备和系统通过各种无线或有线手段接入整个网络，各种网络应用、设备、系统和人逐渐融为一体。

1.1.2 网络空间安全

网络空间安全，顾名思义，是指“网络空间”的“安全”，已有许多关于网络空间安全（Cybersecurity）的定义，典型的定义如下。

（1）美国国家标准技术研究所（NIST）在 2014 年发布的《增强关键基础设施网络安全框架》（1.0 版）中给出的定义：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。该框架提出的网络安全风险管理生命周期五环论，期望用“最佳行为指南”为私营部门管理网络安全风险提供指引。由识别、保护、检测、响应、恢复 5 个环节组成的框架核心，包含 22 类活动，并进一步细分为 98 个子类。

（2）2014 年，俄罗斯发布的《网络安全战略构想》中给出的定义：网络空间安全是所有网络空间组成部分处在避免潜在威胁及其后果影响的各种条件的总和。

（3）2009 年，英国发布的《网络安全战略》中给出的定义：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。一个安全、可靠和富有活力的网络空间可以让所有人受益，无论是公民、企业还是政府，无论是国内还是海外，均应携手合作，理解和应对风险，打击犯罪和恐怖分子利益，并利用网络空间带来的机遇提高英国的总体安全和防御能力。

（4）2011 年，法国发布的《信息系统防和安全战略》中给出的定义：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并且可能对系统提供的或能够实现的存储、处理、传递的数据和相关服务的可用性、完整性或机密性造成损害的情况。

（5）2011 年，德国发布的《网络安全战略》中给出的定义：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限度。

（6）2011 年，新西兰发布的《网络安全战略》中给出的定义：网络空间安全是由网络构成的网络空间，要尽可能保证其安全，防范入侵，保持信息的机密性、可用性和完整性，检测确实发生的入侵事件，并及时响应和恢复网络。

（7）2023 年，《信息安全技术 网络安全事件分类分级指南》[2] 中给出的定义：网络安全是通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以保障数据的完整性、保密性、可用性的能力。

基于上述这些定义，结合国内外学者对网络空间安全的理解和认识，本书中沿用以下《中华人民共和国网络安全法》中的定义。

网络空间安全指通过采取必要措施，防范对网络安全攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力[3]，也指通过识别、保护、检测、响应和恢复等环节保护信息、设备、系统或网络等的过程。在这个过程中，其核心是基于风险管理理念，动态实施连续协作的五环论，即识别、保护、检测、响应、恢复。识别环节评估组织理解和管理网络空间安全风险的能力，包括系统、网络、数据等的风险；保护环节采取适当的防护技术和措施保护信息、设备、系统和网络等的安全，或者确保系统和网络服务正常；检测环节识别发生的网络空间安全事件；响应环节对检测到的网络空间安全事件采取行动或措施；恢复环节完善恢复规划、恢复由网络空间安全事件损坏的能力或服务[1]。

1.1.3　安全属性

属性是指事物所具有的性质、特点。网络空间的安全属性就是指网络空间或网络空间中的信息、信息系统所具有的安全性质、安全特点。网络安全可被理解为网络与信息系统抵御意外事件或恶意行为的能力，这些意外事件和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与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。以上这六个属性被普遍认为是网络安全的基本属性。其具体含义如下。

1. 机密性（Confidentiality）

能够确保敏感或机密数据的传输和存储不遭受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）

能够保障被传输、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，在被篡改的情况下能够发现篡改的事实或者篡改的位置。

3. 可用性（Availability）

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

4. 非否认性（Non-repudiation）

能够保证网络与信息系统的操作者或信息的处理者不能否认其行为或者处理结果，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）身份或者信息、信息来源的真实性。

6. 可控性（Controllability）

能够保证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。

除此之外，网络空间安全属性还包括隐私性、公平性、匿名性，从信息归属、交互对等性、不被泄露性方面体现了网络空间安全活动的特点。

从工程角度而言，一个安全的网络与信息系统是指“一个按预期方式运作的可靠系统”。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方式？这些都是在工程实践中需要解决的问题。

1.1.4 安全威胁

安全威胁是指对系统、网络、数据的安全使用可能造成潜在危害的因素，如某人、物、组织、方法或概念等。通常把可能威胁安全的行为称为攻击，行为的完成者或行为完成的主体称为攻击者。常见的安全威胁大致可分为四类，分别是暴露、欺骗、打扰和占用。

（1）暴露是指导致对信息进行非授权访问的因素，例如窃听、截收、人员疏忽等。

（2）欺骗是致使信息系统接收错误数据或做出错误判断的因素，例如篡改、重放、假冒、否认等。

（3）打扰是指干扰或打断信息系统执行的因素，例如网络攻击、灾害、故障等。

（4）占用是指非授权使用信息或信息系统的因素，例如利用恶意代码。

安全威胁是可能会危及网络空间安全属性的因素，不同的安全威胁可能会危及网络空间安全一种或多种不同的安全属性，例如网络攻击会破坏网络或系统的可用性，恶意代码可能会破坏网络空间的可用性、机密性和可控性。

1.1.5 安全策略

安全策略是指组织或企业为保障网络、系统、数据或资产而制定的一系列的规则和程序，或者说是为了达到网络空间安全目标，或确保网络空间要素始终处于安全状态，或防止网络空间要素进入安全状态，而对允许做什么、禁止做什么的一种规定。安全策略明确了安全目标、权责等，是网络安全管理的基础。

在专业领域，安全策略通常描述的是网络空间要素的安全需求和安全属性，涉及网络空间要素，包括但不限于硬件、软件、用户、访问、连接、网络等。安全策略表述通常不涉及实现过程，其具体实现往往通过某种技术或管理机制达成，而不需要在安全策略自身表述中限定。安全策略可用来指导网络安全体系结构的规划设计、产品选型、系统开发、运营维护等。

1.1.6　安全机制

安全机制是为了实施安全策略、实现安全功能或提供安全服务而采用的方法，常见的安全机制如加密、数字签名、访问控制、完整性校验、路由控制、安全审计、入侵检测、病毒防范、安全操作手册等。

1.1.7　安全保障

保障的英文单词是 Assurance，在英文中解释为“确信、确保、信心、保障”等；安全保障的英文为 Security Assurance，通常在中文中翻译为安全确信、安全确保、安全保证，也就是说，确保安全策略落地 [1]。安全保障通过一定的安全保障技术而获得，在相关安全保障技术的支持下，能够获取证据来说明系统的实现和运行能够满足安全策略中定义的安全需求。安全保障的目标是确保系统从实现到运行的整个生命周期都满足其安全需求。

安全保障技术包括开发过程的技术、设计分析和测试中所用到的技术方法等，包括策略、设计、实现、运行等安全保障技术。策略安全保障技术确保策略中的安全需求是完整的、一致的，并在技术上是可行的；设计安全保障技术确保系统设计满足策略中的安全需求；实现安全保障技术确保系统实现与策略中的安全需求是一致的；运行安全保障技术确保系统安装、配置和日常运行的过程中仍然与策略中的安全需求是一致的。安全验证、安全测试、安全评估、安全审查等属于安全保障技术范畴，通过在生命周期的某个阶段消除可能破坏安全属性的疏忽或错误。

1.1.8　漏洞或脆弱性

漏洞（Vulnerability），又称脆弱性，是指在硬件设计、软件开发、通信协议执行或系统安全配置中存在的弱点或缺陷，可以被恶意用户（也成为攻击者）利用，以未经授权的方式访问、篡改或破坏系统资源，从而对系统的安全性、完整性和可用性造成威胁。

漏洞可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误，也可能来自业务在交互处理过程中的设计缺陷或逻辑流程上的不合理之处。这些缺陷、错误或不合理之处可能被有意或无意地利用，从而对一个组织地资产或运行造成不利影响。如信息系统被攻击或控制，重要资料被窃取，用户数据被篡改，系统被作为入侵其他主机系统的跳板。

网络安全漏洞（Cybersecurity Vulnerability）是指网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程中，无意或有意产生的、有可能被利用的缺陷或薄弱点。这些缺陷或薄弱点以不同形式存在于网络产品和服务的各个层次和环节中，一旦被恶意主体所利用，就会对网络产品和服务的安全造成损害，从而影响其运行。

在网络安全领域，漏洞通过采用 *x*day 的方式来表示其曝光程度，*x* 通常为 0、1、*n*，0day 漏洞指那些已经被攻击者发现掌握并开始利用，但还没被包括受影响软件厂商在内的公众所知的漏洞，这类漏洞的危害极高；1day 漏洞指漏洞已公开但仍未发布补丁的漏洞，此类漏洞的危害仍然较高；*n*day 漏洞是指已经发布官方补丁的漏洞，此类漏洞只需更新补丁即可，但由于种种原因，大量漏洞补丁更新不及时，漏洞利用方式已经公开，仍然具有一定危害，它是未达到一定水平的黑客最为常用的漏洞。

1.1.9 恶意软件

恶意软件（Malware）是指设计用于破坏、非法访问或干扰网络或系统运行的恶意程序，通常包括病毒（Virus）、蠕虫（Worm）、特洛伊木马（Trojan Horse）、间谍软件（Spyware）。病毒是一种能够自我复制并传播的恶意软件，它能够附加到其他合法程序上，随程序的运行执行恶意操作；蠕虫是一种能够自我复制并通过网络自动传播的恶意软件，不需要附加到其他程序上，且可在没有用户操作的情况下传播；特洛伊木马是一种伪装成合法程序的恶意软件，当用户运行它时，可能会执行恶意操作；间谍软件是一种隐蔽地收集用户信息并发送给攻击者的恶意软件，它可以记录键盘输入、截屏、监控网络活动等，通常用于窃取敏感信息。

近年来，出现了一种危害极高的恶意软件——勒索软件（Ransomware），它是一种通过加密受害者的文件，要求支付赎金才能解密的恶意软件，通常通过钓鱼邮件和漏洞利用攻击传播。

1.1.10 僵尸网络

僵尸网络（Botnet）是指黑客采用一种或多种传播手段，致使大量主机感染僵尸程序病毒，被感染的主机（Bot）通过控制协议接收黑客的指令，从而在黑客和被感染主机之间形成的可一对多控制的网络，往往被黑客用来发起大规模的网络攻击。黑客即监视网络的控制者，能够控制僵尸网络上的主机；跳板主机是用户控制僵尸主机的计算机，黑客通过跳板主机下发控制指令，实现对僵尸网络中大片僵尸主机的控制；控制协议是僵尸网络控制者用来控制僵尸主机的媒介；僵尸主机指已经被黑客控制的主机，可以在远程操纵下执行恶意任务。常见的利用僵尸网络发动的攻击行为包括：发动分布式拒绝服务攻击、僵尸网络挖矿、发送海量垃圾邮件。

1.1.11 网络攻击

在网络空间安全领域，攻击（Attack）指企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用系统或网络资产的行为，攻击的发起人通常称为攻击者，指故意利用

技术或非技术安全控制的脆弱性，以窃取或损害信息系统和网络，或者损害合法用户对信息系统和网络资源可用性为目的的任何人。攻击通常利用网络或针对网络实施，又常被人们称为网络攻击。

常见的网络攻击包括网络钓鱼（Phishing）、中间人攻击（Man-In-The-Middle attack，MITM）、拒绝服务攻击（Denial-of-Service attack，DoS）、分布式拒绝服务攻击（Distributed Denial-of-Service attack，DDoS）等。网络钓鱼是一种社会工程攻击，通过伪装称可信实体来欺骗用户透露敏感信息（如用户名、密码、信用卡信息等），常见方式包括伪造电子邮件、网站和短信。中间人攻击是指攻击者在通信双方之间插入自己，拦截并篡改通信内容。拒绝服务攻击是指通过向目标系统发送大量请求，使其无法正常提供服务。分布式拒绝服务攻击是指通过多个受控计算机同时向目标系统发送大量请求，从而使其无法正常提供服务，分布式拒绝服务攻击比拒绝服务攻击更具破坏性。

根据攻击造成的危害程度不同，攻击层次由浅入深依次划分为：简单拒绝服务、本地用户获得非授权读权限、本地用户获得非授权写权限、远程用户获得非授权账号信息、远程用户获得特权文件的读权限、远程用户获得特权文件的写权限、远程用户拥有了系统管理员的权限。根据攻击位置不同可以将攻击划分为远程攻击、本地攻击、临近攻击和伪远程攻击。攻击的分类有很多种，包括基于攻击术语的分类、基于攻击过程的分类、基于攻击效果评估的分类等，这里不再一一列举，读者要深入了解网络攻击的内容，可参考本系列教材中的其他教材。

1.1.12　网络安全事件

本书中沿用国家标准《信息安全技术　网络安全事件分类分级指南》（GB/T 20986—2023）对网络安全事件（Cybersecurity incident）的定义。网络安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或者其中的数据和业务应用造成的危害，对国家、社会、经济造成负面影响的事件[2]。常见的网络安全事件包括：恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件等。

1.1.13　高可持续性威胁

高可持续性威胁（Advanced Persistent Threat，APT）攻击指由有组织地攻击者针对特定目标进行长期、复杂的攻击。APT 攻击具有高水平和持续性，难以检测和防御。本书中将 APT 攻击理解为针对目标攻击的有组织和有计划的攻击。APT 攻击通常包含三个主要元素：高级，强调使用复杂的恶意程序或利用系统中的高级漏洞；可持续性，强调监控攻击目标的持久性；威胁，强调具有蓄意和严重影响的复杂网络攻击。APT 攻击通常具有高度隐蔽性，可以穿透受害者的网络，停留时间长，缓慢而隐蔽地移动，以达到攻击意图。

APT 攻击者花费更多时间选择目标、准备攻击模式、发现漏洞以及自定义恶意工具和恶意软件来执行攻击。攻击周期包括信息收集、武器定制、有效载荷投送、初始入侵、安装和操作、C&C 通道的建立和攻击实现。

1.2 网络空间安全基础知识

网络空间安全学科是一个综合了计算机科学与技术、数学、信息与通信工程、软件工程、控制科学与工程、生物管理、法律等的交叉学科，因此其技术体系基于各学科相关理论技术构建，与密码学共同构成了网络空间技术体系的基础。

1.2.1 网络空间安全理论基础

1. 数学

目前网络空间安全领域广泛应用的密码仍然是基于数学的密码。对于基于数学的密码，密码学界普遍认为设计一个密码就是设计一个数学函数，而破译一个密码就是求解一个数学难题，这就从本质上清晰地阐明了数学是密码学的理论基础。作为密码学理论基础之一的数学分支主要有代数、数论、概率统计、组合数学等。协议安全是网络安全的核心，作为协议安全理论基础之一的数学主要有逻辑学等 [4]。

博弈论是现代数学的一个分支，是研究具有对抗或竞争性质的行为的理论与方法。一般称具有对抗或竞争性质的行为为博弈行为。在博弈行为中，参加对抗或竞争的各方各自具有不同的目标或利益，并力图选取对自己最有利的或最合理的方案。博弈论研究的就是博弈行为中对抗各方是否存在最合理的行为方案，以及如何找到这个合理方案。博弈论考虑对抗双方的预期行为和实际行为，并研究其优化策略。信息安全领域的斗争无一不具有这种对抗性或竞争性。例如，网络的攻与防、密码的加密与破译、病毒的制毒与杀毒、信息隐藏与分析、信息对抗，等等。因为信息安全领域的斗争，本质上都是人与人之间的攻防斗争，因此博弈论便成为网络空间安全学科的基础理论 [4]。

2. 信息论、系统论和控制论

信息论奠定了密码学和信息隐藏的基础。信息论对信息源、密钥、加密和密码分析进行了数学分析，用不确定性和唯一解距离来度量密码体制的安全性，阐明了密码体制、完善保密、纯密码、理论保密和实际保密等重要概念，把密码置于坚实的数学基础之上，标志着密码学作为一门独立的学科的形成。因此，信息论成为密码学的重要的理论基础之一 [4]。

系统论是研究系统的一般模式、结构和规律的科学，系统论的核心思想是整体观念。任何一个系统都是一个有机的整体，不是各个部件的机械组合和简单相加。系统的功能是各部件在孤立状态下所不具有的。

控制论是研究机器、生命社会中控制和通信的一般规律的科学，它研究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。控制论中把“控制”定义为，为了改善受控对象的功能或状态，获得并使用一些信息，以这种信息为基础施加到该对象上的作用。由此可见，控制的基础是信息，信息的传递是为了控制，任何控制又都依赖于信息反馈。

保护、检测、响应策略是确保信息系统和网络系统安全的基本策略，在信息系统和网络系统中，系统的安全状态是系统的平衡状态或稳定状态。恶意软件的入侵打破了这种平衡和稳定。检测到这种入侵，便获得了控制的信息，进而杀灭这些恶意软件，使系统恢复安全状态。确保信息系统安全是一个系统工程，只有从信息系统的硬件和软件的底层做起，从整体上综合采取措施，才能比较有效地确保信息系统的安全。这表明，系统论和控制论是信息系统和网络系统安全的基础理论[4]。

3. 可计算性与计算复杂性

可计算性理论是研究计算的一般性质的数学理论，它通过建立计算的数学模型，精确区分哪些是可计算的，哪些是不可计算的。计算复杂性理论使用数学方法对计算中所需的各种资源的耗费做定量的分析，并研究各类问题之间在计算复杂程度上的相互关系和基本性质，研究计算一个问题类需要多少时间，多少存储空间；研究哪些问题是现实可计算的，哪些问题虽然是理论可计算的，但因计算复杂性太大而实际上是无法计算的。

在网络空间安全中，授权是访问控制的核心。从可计算性的视角出发，一般意义上，对于给定的授权系统是否安全这一问题是不可判定问题，但是一些“受限”的授权系统的安全问题又是可判定问题。由此可知，一般操作系统的安全问题是一个不可判定问题，而具体的操作系统的安全问题却是可判定问题。又例如，密码破译就是求解一个数学难题，若这个难题是理论不可计算的，则这个密码就是理论上安全的；若这个难题虽然是理论可计算的，但是由于计算复杂性太大而实际上不可计算，则这个密码就是实际安全的，或计算上安全的。因此可以说，可计算性与计算复杂性是网络空间安全的理论基础之一[4]。

4. 密码学理论

虽然信息论奠定了密码学的基础，但密码学在其发展过程中已经超越了传统信息论，形成了自己的一些新理论，如单向陷门函数理论、公钥密码理论、零知识证明理论、多方安全计算理论、以及部分密码设计与分析理论。从应用角度看，密码技术是信息安全的一种共性技术，许多信息安全领域都要应用密码技术。因此，密码学理论是网络空间安全学科的理论基础，而且是网络空间安全学科特有的理论基础[4-6]。

1.2.2　网络空间安全方法论基础

1. 分而治之与系统工程相结合的方式是网络空间安全的方法论之一

传统针对复杂问题的解决思路通常是将其分解为一些细小的问题分别解决，是一种分而治之的思想，它为解决复杂问题提供了可行的途径；随着近代科学的发展，人们发现许

多复杂问题无法分解，分解之后的局部并不具有原来整体的性质，因此必须用整体的思想和方法来处理，由此导致系统工程的出现。网络空间安全学科既包含分而治之的传统方法论，又包含综合治理的系统工程方法论，应将这两者有机地融合为一体，从理论分析、逆向分析、实验验证、技术实现 4 个核心方面开展关键技术研究和工程系统建设，这四者既可以独立运用，也可以相互结合，指导解决网络安全问题，推动网络空间安全技术发展。

2. 逆向分析是网络空间安全方法论之一

在网络空间安全领域攻防双方的对抗，本质上是攻防双方之间的斗争，许多核心关键问题都具有攻和防两个方面。例如，密码学由密码编码学和密码分析学组成，网络安全由网络安全防护和网络攻击组成等。因此需要引入逆向分析的方法从攻的角度研究防。例如，在密码学的研究中，既要研究密码设计，又要研究密码分析；在网络安全保护体系建设中，既要研究网络安全防护，又要研究网络攻击。

3. 以人为核心是网络空间安全方法论之一

在网络安全保障领域，人们常说“三分技术、七分管理”，说明网络安全问题不仅是技防问题，更重要的是组织管理、人员意识和法律保障的问题，许多网络安全事件的发生表明，组织管理不到位、人员意识薄弱等是事件发生的直接原因。所以，网络空间安全技术研究和各项活动的开展应该以人为核心，同时遵守法律法规，并要推动新兴技术领域立法工作开展。

1.2.3 密码技术

密码学是一门结合了数学、计算机科学、电子与通信等诸多学科的交叉学科，主要研究信息安全保密。密码学（Cryptology）分为密码编码学（Cryptography）和密码分析学（Cryptanalysis），前者寻求提供机密性、完整性、真实性和不可否认性等的方法，后者研究针对加密消息的破译和伪造等破坏密码技术所能提供安全性的方法，两者之间彼此关联又相互促进。密码学之前是信息安全的基础，现在是网络空间安全的基础，在政治、经济、军事、外交等领域的信息、数据、通信安全方面发挥着不可替代的作用，是实现认证、加密、访问控制的基础技术。

一个典型的密码系统通常由明文、密文、密钥及密码算法组成，如图 1-1 所示。明文通常指人们能够看到的文字、内容或信息，通常用 m 标识；明文经过加密后称为密文，通常用 c 表示。把明文加密称密文的算法称为加密算法，把密文解密成明文的算法称为解密算法。密钥加密和解密过程所使用的关键值，可以分为加密密钥和解密密钥，通常用 k 表示，由通信双方掌握，可以相同也可以不同。

在网络安全领域通常使用一个五元组 (M,C,K,E,D) 来表示密码系统。其中 M 为明文空间，C 为密文空间，K 为密钥空间，E 和 D 分别表示加密算法和解密算法。

密钥是密码系统中的可变部分，也是最核心的部分。一方面，现代密码体制的密码算法是公开的，甚至有的加密算法已经成为国际标准；另一方面，在计算机网络环境中，存

在者许多用户和节点，需要大量密钥，密钥一旦丢失，就会对系统的安全造成威胁。因此，在设计密码系统时，需要解决密钥管理问题。密钥管理技术主要包括密钥的产生、存储、分配、保护、销毁等，需要确保在公共互联网络传递过程中的安全性。

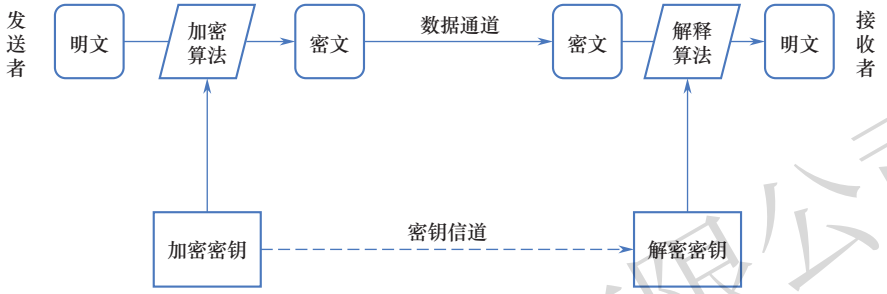

图 1-1　密码系统组成

密钥管理需要实现如下目标：

（1）密钥难以被非法窃取；

（2）密钥分配和交换对用户是透明的；

（3）脱离密码设备的密钥是绝对保密的；

（4）密钥不再使用后需要彻底销毁或更换。

有关密码技术的详细介绍见第 4 章商用密码应用技术。

1.3　网络空间安全的演进过程

从信息安全的角度来看，我们可以把网络空间安全理解为网络空间环境下信息安全发展的新阶段。从这种意义上来讲，网络空间安全发展历程就是信息安全发展历程。纵观它的发展历史，可以将其大致归纳为以下 5 个阶段。

1.3.1　通信安全发展阶段

通信安全发展阶段大致从古代至 20 世纪 60 年代中期，这一时期人们最关心的是信息在传输中的机密性。

自 19 世纪 40 年代电报发明后，安全通信主要面向保护电文的机密性，密码技术成为支撑机密性的核心技术。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，如德国的 ENIGMA 密码机、日本的 PURPLE 密码机、美国的 ECM 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，并且由于在技术上没有安全的密钥或密码本分发方法，因此在战争中有大量的密码通信被破解。以上密码被普遍称为古典密码。

1949 年，Shannon 发表了论文《保密系统的通信理论》，提出了著名的 Shannon 保密通信系统模型，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，这为对称密码学建立了理论基础，从此密码学发展成为一门科学。

1.3.2 计算机安全发展阶段

计算机安全发展阶段大致为 20 世纪 60 年代中期至 80 年代中期。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。这一时期人们不仅要关注通信安全，还要关注计算机和操作系统、数据库等的安全。

20 世纪 60 年代出现了多用户操作系统，由于需要解决安全共享问题，人们对信息安全的关注从机密性扩大到“机密性、访问控制与认证”，并逐渐意识到还需要保障可用。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。

进入 20 世纪 80 年代后，人们在计算机安全方面开始了标准化和商业应用的进程。1980 年，Anderson 做的题为《计算机安全威胁监控与监视》的技术报告首次详细地阐述了主机入侵检测的概念，并首次为入侵和入侵检测提出一个统一的架构，这标志着人们已经关注利用技术手段获得可用性。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等级测评。之后，美国国防部又陆续发表了 TNI、TDI 等 TCSEC 解释性评估标准。标准化工作带动了安全产品的大量出现。访问控制研究也不可避免地涉及商业安全策略，其典型代表是 Clark-wilson 和 Chinesewall 策略模型。

1.3.3 信息安全发展阶段

随着信息技术应用越来越广泛和网络的普及，20 世纪 80 年代中期至 90 年代中期，学术界、产业界和政府、军事等部门对信息和信息系统安全越来越重视，人们对信息安全的关注已扩大到可用性、机密性、完整性、非否认性、真实性和可控性等基本属性。在这一时期，密码学、安全协议、通信安全、计算机安全、安全评估和网络安全等得到了较大发展，尤其是互联网的应用和发展大大促进了信息安全技术的发展与应用，因此，这个时期也可以称之为网络安全发展阶段。

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 4 国于 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），加拿大、法国、德国、荷兰、英国、美国的 NIST 与国家安全局（National Security Agency，NSA）于 20 世纪 90 年代中期提出了信息技术安全通用评估准则（Common Criteria，CC）。

随着计算机网络的发展，这一阶段的网络攻击事件逐渐增多，传统的安全保密措施难以抵御计算机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、分布式 IDS、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 1 个计算机应急响应小组及协调中心（Computer Emergency Response Team Coordination Center，CERT/CC），标志着信息安全从静态防护阶段过渡到主动防护阶段。

1.3.4　信息安全保障阶段

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以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以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过程基础上的，这包括“预警、保护、检测、响应、恢复、反击”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。

在这一阶段，新型网络、计算和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、传感器或 Ad-Hoc 网络下的算法和安全协议、量子密码及其协议、现代信息隐藏、数字版权保护和电子选举等。

为了保护日益庞大、重要的网络和信息系统，信息安全保障（也称为信息保障）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——PDR 模型，后来增加了恢复，成为 PDRR（Protection,Detection,Reaction,Restore）模型；1998 年 10 月，美国 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 年下半年发生“9·11”事件以来，美国政府以国土安全战略为指导，出台了一系列信息安全保障策略，将信息安全保障体系纳入国家战略；一些西方发达国家也高度重视信息安全战略，试图全面建立信息安全保障机制。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），这是我国信息安全领域的指导性和纲领性文件。

1.3.5　网络空间安全发展阶段

进入 21 世纪以来，尤其是自 2010 年以来，世界各国纷纷出台国家层面的网络空间安全战略，网络空间安全上升至国家战略层面，网络空间安全概念正式被提出，牵引信息安全的发展，并替代信息安全成为富有时代意义的热点领域。我国于 2015 年在“工科”门类下增设了“网络空间安全”一级学科，随后多所高校增设了相关院系或专业。我国于 2016 年 11 月颁布了《中华人民共和国网络安全法》、2019 年 10 月颁布了《中华人民共和国密码法》、2021 年 6 月颁布了《中华人民共和国数据安全法》、2021 年 8 月颁布了《中华人民共和国个人信息保护法》，为保障我国网络安全，维护网络空间主权和国家安全、

社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展提供了直接的法律支撑。

在这种大背景下，信息安全技术在攻防两方面都取得了大量的技术突破。攻击者不断利用技术、管理和人性的弱点实施渗透，而网络安全防御体系也在逐步完善；大数据、量子通信等新技术的发展，也带来了信息安全技术的新思路，正推动着信息安全技术的变革。网络攻击与对抗、大数据安全与隐私保护、量子通信与抗量子密码、工业控制系统安全和网络空间身份管理等成为信息安全领域关注的重点和焦点。虽然在这些领域取得了一些重要进展，但仍有众多问题需要研究和解决。以 APT 攻击为代表的有组织攻击越来越普遍，攻击技术在不断发展，如何在不掌握攻击特征的情况下，检测、防御这些高水平攻击是当前防御的难点。量子通信为信息安全传输提供了新的手段，但量子计算却对现用的密码体系提出了新的挑战，在后量子时代，如何实现抗量子的密码保护是目前该领域的重要前沿问题之一。

近年来，大规模信息泄露事件频发，在大数据时代，保护数据安全、保护个人隐私是大数据应用繁荣的重要保障之一。工业控制系统的“以太”化带来了工业信息化的繁荣，但同时也为网络攻击提供了便利，如何保障工业控制系统的安全是关系国计民生的大问题。各类网络犯罪猖獗的重要原因之一就是打击网络犯罪难度大，建立网络空间可信身份管理体系是提高网络空间治理能力的关键，但构建一个良性的可信身份生态系统任重而道远。

1.4 国际网络空间安全战略

1.4.1 美国网络空间安全战略

美国在 2003 年发布了《确保网络空间安全战略》，把网络空间安全提升到国家安全的高度。2011 年，美国发布了《网络空间行动战略》，从作战概念、防御策略、国内协作、国际联盟以及人才培养和技术创新 5 个方面明确了美国网络空间行动的方向和准则。同年，美国发布了《网络空间可信身份国家战略》，并发布了美国首份《网络空间国际战略》文件，阐述美国“在日益以网络相连的世界如何建立繁荣、增进安全和保护开放”，这份战略文件被视为美国 21 世纪的“历史性政策文件”。2015 年，美国颁布《网络安全法》，并于 2016 年发布了《国家网络安全行动计划》，成立了“国家网络安全促进委员会”，为国家网络空间安全领域的政策与规划提供咨询与指导，使美国有能力更好地控制网络空间安全。

2023 年 3 月，美国发布了《国家网络安全战略》（National Cybersecurity Strategy），其中详细阐述了美国政府改善数字安全的系统性方法，旨在帮助美国准备和应对新出现的网络威胁。报告围绕建立“可防御、有韧性的数字生态系统”，给出了保护关键信息基础设

施、破坏和摧毁威胁行为者、塑造市场力量、投资于有人性的未来、建立国际合作伙伴关系等五大支柱 27 项举措，它不仅体现了拜登政府在网络安全领域的优先事项，也为本届政府后半段任期中解决网络威胁具体方式提供清晰的路线图。美国政府拟从根本上调整其对网络空间角色、责任和资源的分配方式，并做出两大转变：一是重新平衡网络空间安全责任，今后将更多地将责任转移到专业机构；二是重新调整激励措施，强调在解决当前紧迫威胁的同时面向未来进行战略规划和投入。该战略充斥着对华意识形态的偏见，毫不掩饰其反华制华立场，充分说明了国际网络空间博弈斗争的复杂性。

2023 年 7 月 13 日，美国发布《国家网络安全战略实施计划》（NCSIP），详细述了相关职能部门在保障美国网络安全方面的举措和要求，并设定具体时间节点，体现了美国抢占“第五空间”制高点的战略图谋。该计划的实施要点与美国《国家网络安全战略》相配套，聚焦于强化 5 个方面的工作：一是基础设施防护；二是威胁实体应对；三是市场力量培塑；四是网络标准把控；五是国际网络合作。

2023 年 8 月，美国网络安全与基础设施安全局（CISA）发布《2024—2026 年网络安全战略计划》，其中阐述了三年网络安全的目标：一是解决现有威胁，为此 CISA 将了解美国及其合作伙伴的网络威胁，挫败地方活动，并更快消除可被对手反复利用的漏洞。二是加固网络态势，包括促进、支持和评估具有安全性和弹性的做法。三是大规模提升安全性，包括理解和减少人工智能等新兴技术带来的风险，要求技术提供商考虑产品全周期的安全问题，以及加强国家网络安全队伍。

1.4.2　欧盟网络空间安全战略

2023 年 1 月，《关于在欧盟全境实施高度统一网络安全措施的指令》正式生效，主要内容包括：建设协调的网络安全框架；加强欧盟和国际层面的合作；明确网络安全风险管理措施和报告义务；规定对各类网络运营主体的登记和管理要求；建立成员国的信息共享机制；完善对各类网络运行实体的监督和执法措施。为保障该指令得到落地实施，欧盟还制定了严格的时间表和路线图。

2023 年 2 月，欧盟发布的《为实施国家网络安全战略而建立有效的治理框架》提出，各成员国应努力建设一套治理框架，以实现更好的网络安全战略实施效果。为保障战略目标的实现，欧盟将治理框架划分为政治治理、战略治理、运营治理、技术治理四大维度，其中，政治治理维度上提出鼓励网络空间建设使用公私合作关系（PPP）模式；战略治理维度上提出重视预算规划和资源分配以及设置风险识别和缓解机构；运营治理维度上提出完善突发事件应急响应机制，并重视网络安全宣传教育；技术治理维度上加强认证与标准化建设。另外，该框架还提出要实行配套的监测评估机制，用以评价成员国网络安全战略实施效果。

2023 年 4 月 18 日，欧盟委员会通过了关于《网络团结法案》的提案。法案通过时间正值俄乌战争之际，体现了欧盟促进成员国之间合作并为重大网络危机做好准备的意愿，

以更好应对因地缘政治局势紧张而产生的网络安全威胁。其目标的实现主要依托以下行动内容：一是部署泛欧安全运营中心基础设施（欧洲网络盾牌），以建立和加强共同检测与态势感知能力；二是建立网络应急机制，形成欧盟网络安全储备，以支持成员国准备、应对重大和大规模网络安全事件；三是建立欧洲网络安全事件审查机制，审查和评估重大或大规模事件。

1.5 我国网络空间安全战略

近年来，我国也越来越重视网络空间安全。2013 年 11 月 12 日，中央国家安全委员会正式成立；2014 年 2 月 27 日，中央网络安全和信息化领导小组成立。习近平总书记在主持召开中央网络安全和信息化领导小组第 1 次会议时指出：没有网络安全就没有国家安全，没有信息化就没有现代化。2014 年 4 月 15 日，习近平总书记在中央国家安全委员会第 1 次会议上的讲话中将信息安全列为我国国家安全体系的重要组成部分，标志着我国持续对探索建立明晰的网络空间国家安全战略高度重视。在 2015 年 7 月发布施行的新国家安全法中，首次明确了“网络空间主权”概念，提出要“维护国家网络空间主权”。

2016 年 12 月 27 日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布我国首部《国家网络空间安全战略》（以下简称《网络空间战略》），《网络空间战略》作为我国网络空间安全的纲领性文件，重点分析了目前我国网络安全面临的“七种机遇和六大挑战”，提出了国家总体安全观指导下的“五大目标”，建立了共同维护网络空间和平安全的“四项原则”，制定了推动网络空间和平利用与共同治理的“九大任务”。“五大目标”指在总体国家安全观指导下，通过统筹国内、国际两个大局和统筹发展、安全两件大事的基础上，推进网络空间“和平、安全、开放、合作、有序”的发展战略目标。“四项原则”即尊重维护网络空间主权、和平利用网络空间、依法治理网络空间、统筹网络安全与发展。“九大任务”指坚定捍卫网络空间主权、坚决维护国家安全、保护关键信息基础设施、加强网络文化建设、打击网络恐怖和违法犯罪、完善网络治理体系、夯实网络安全基础、提升网络空间防护能力、强化网络空间国际合作。

1.6 网络安全技术体系与常见技术和产品

1.6.1 网络安全技术体系框架

网络空间安全发展的不同阶段，因信息安全、系统安全、网络安全保护、保卫和保障工作的不同需要，演化发展形成不同类型的网络安全技术，有的针对共性的安全保护需要，例如访问控制；有的针对特定的保护目标，例如操作系统安全；有的针对特定的威

胁，例如入侵检测；有的则针对特定的领域。可以说从不同的视角出发，网络安全技术会有不同的分类方式。

从网络空间学科的构建开始，网络安全研究领域先后提出了多个网络安全技术体系框架，尝试从不同的视角构建相对完整的技术体系架构。本书综合了相关技术体系架构的优点，从网络安全保护、监测 / 检测、响应、恢复、反击和管理环节进行技术分类梳理，同时考虑网络安全技术对重点保护领域和新技术新应用领域的支撑，采用如图 1-2 所示的网络空间安全体系架构，包括密码学与安全基础、网络安全保护（分为网络与通信安全、系统安全与可信计算、数据与信息安全、应用安全）、监测感知、响应对抗、安全测评、重点保护领域与新应用安全技术，其中密码学与安全基础技术为其他技术提供支撑，网络保护对应网络安全保护环节，监测感知对应监测 / 检测环节，响应对抗对应响应、恢复、反击环节，安全测评对检测、管理环节，重点保护领域与新应用安全则对应全链条。

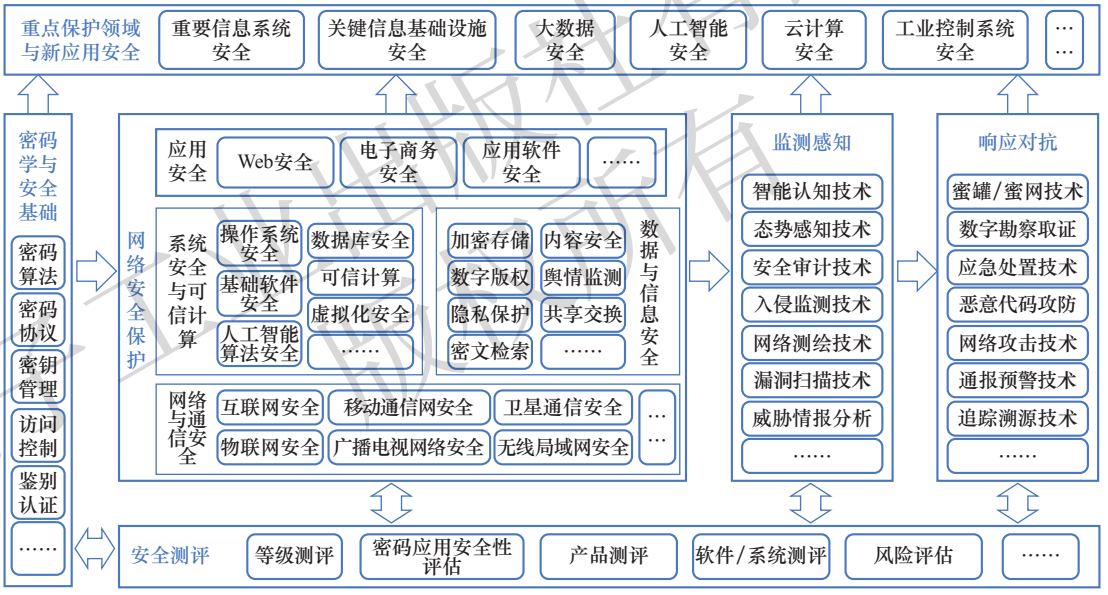

图 1-2　网络空间安全技术体系架构

（1）密码学与安全基础，由密码学理论以及访问控制等共性安全技术构成，具体内容包括密码算法、密码协议、密钥管理、访问控制、鉴别认证等。本书第 4 章将重点介绍商用密码应用技术。有关密码应用技术内容的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《商用密码应用技术》。

（2）网络安全保护，侧重于网络空间威胁攻击防护，以保护网络、系统、数据以及应用等安全为目的，具体内容包括网络与通信安全，如互联网安全、移动通信安全、卫星通信网络安全、广播电视网络安全、物联网安全、无线局域网安全等；系统安全与可信计算，如操作系统安全、基础软件安全、数据库安全、虚拟化安全、人工智能算法安全、可信计算等；数据与信息安全，如加密存储、数字版权、隐私保护、密文检索、内容安全、

舆情监测、共享交换等；应用安全，如 Web 安全、电子商务安全、应用软件安全等。

（3）监测感知，侧重于探测发现网络威胁行为，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。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、态势感知技术等。本书第 10 章将重点介绍网络威胁情报分析与挖掘技术，第 11 章将重点介绍恶意代码分析与检测技术。

（4）响应对抗，侧重于针对网络空间威胁的应急响应与实战对抗，主要目的是针对网络空间主要的攻击手段，例如口令破解、后门攻击、拒绝服务、缓冲区溢出、APT 攻击、勒索病毒等，开展应急演练、攻防对抗等关键技术研究，以便更好地开展响应处置、应急恢复、溯源反制工作。具体包括网络攻击技术、恶意代码攻防、应急处置技术、数字勘查取证、蜜罐 / 蜜网技术等内容。本书第 7 章将重点介绍网络安全事件处置与追踪溯源技术，第 9 章将重点介绍数据勘查与取证技术，第 12 章将详细介绍漏洞挖掘与渗透测试技术。

（5）安全测评，侧重于针对网络、系统、数据开展测试、监测或评估，以验证其安全合规情况和实际的安全保护能力，属于安全保障的范畴。具体内容包括等级测评、密码应用安全性评估、产品测试、软件 / 系统测试、风险评估等。本书第 8 章将重点介绍网络安全检测评估技术。

（6）重点保护领域与应用安全，侧重于重点保护目标、新技术新应用的系统化、体系化的安全保护、保障技术，主要目的是保护、保障重要行业、重点领域、新型应用的安全，确保其安全属性不被破坏。具体内容包括重要信息系统安全、关键信息基础设施安全、大数据安全、人工智能安全、云计算安全、工业控制系统安全等。本书第 3 章将从网络安全建设与运营视角介绍重要信息系统和重要行业部门安全；第 5 章和第 6 章分别就数据安全和人工智能安全展开详细介绍。

有关网络安全技术的全面和详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络空间安全技术》。

1.6.2 网络安全常见技术

1. 互联网安全技术

随着信息技术的飞速发展，互联网已成为承载全球信息系统的网络基础设施之一，其安全问题直接关系到国计民生、社会稳定和国家安全。从承载内容来看，互联网安全涵盖面非常广，涉及多类网络安全技术；从其他类型安全技术不同来看，互联网安全侧重于开放系统互联安全体系结构（Open Systems Interconnection，OSI）中各层次安全，其中物理层（第 1 层）、数据链路层（第 2 层）、网络层（第 3 层）、传输层（第 4 层）常以底层网络安全协议来实现，进一步又可分为链路级安全、网络级安全，后者是互联网安全协议技术关注的重点。会话层（第 5 层）、表示层（第 6 层）、应用层（第 7 层）通常以安全按组

件的方式，包括系统安全组件、安全通信组件实现，通常可分为端系统级安全、应用级安全，应用层安全是互联网安全关注的又一重点。

网络级安全主要在网络层和传输层实现。确保网络层安全的代表性协议 IPSec（Internet Protocol Security）已经成为行业标准，通过在 IP 层引入数据认证机制、加密机制和相关密钥管理，实现比较全面的网络层安全；此外网络层具有代表性的安全协议还包括 AH 协议、ESP 协议、IKE 协议等，有兴趣的读者可参考其他文献进一步了解。安全套接字层协议（Secure Socket Layer，SSL）是建立在 TCP 协议传输层的、有代表性的安全协议，用于保护面向连接的 TCP 通信，应用层协议可以在其上透明地使用 SSL 协议，目前该协议历经多版本的升级，在互联网应用中广泛存在，主流的浏览器和 Web 服务器都支持该协议。

2. 移动通信网络安全

随着无线网络技术的快速发展，移动通信网络成为承载人们工作和生活，促进社会交流的重要网络基础设施之一，其安全问题也成为促进、保障或制约其发展的重要因素，受到学术界、产业界的广泛关注。移动通信网络与传统互联网相比具有开放性、移动性、拓扑结构动态性特点，且计算、存储能力在节点端都比较有限，因此这也成为移动通信网络安全关注的重点。同互联网相似，密码算法、鉴别认证、访问控制以及威胁攻击的防范在移动通信网络安全中起到了重要作用。从自身特性出发，移动通信网络从 2G 时代设计 GSM 安全机制来保障移动通信安全，主要包括基于 IMSI 的用户身份保护、用户接入认证以及传输加密机制，以此来确保移动通信安全。3G 时代因传输内容富化，传输速率提升以及国际漫游需要，传输认证由之前的单行认证扩展至双向认证，接入链路数据完整性保护机制进一步强化，增加了移动台和服务网络之间的安全协商机制实现跨网通信，增强用户身份保密机制（Enhanced User Identify Confidentiality，EUIC）被定义用于确保 IMSI 信息加密传输。4G 时代移动通信网络安全在 3G 体系结构基础上进一步增强，主要体现在防窃听、防伪基站攻击等方面。

5G 时代是一个万物互联的时代，移动通信网络承载的系统和设备扩充迅猛，宽带速率大幅提升，个性化场景和特殊需求层出不穷，其中网络功能虚拟化、软件定义网络成为 5G 组网的关键技术，用户角色进一步扩充，传统基于物理设备隔离的安全保障不再适用，虚拟化安全、转发节点安全成为关注焦点；加之移动 App 的服务，使得个人隐私和关键数据安全问题加剧，需要 5G 安全机制严格控制数据生命周期的各个环节。因此，5G 时代安全机制扩充为覆盖接入安全域、网络安全域、用户安全域、应用安全域、可信安全域的更为复杂的安全框架。5G 安全关键技术包括接入安全——统一的认证框架（Extensible Authentication Protocol，EAP），解决海量异构终端设备认证身份绑定问题，解决海量异构终端接入；接入安全——基于群组的海量 IoT 设备认证，实现一次性认证一组设备，解决海量设备接入和频繁接入问题；网络切片安全——基于标识的切片安全隔离，旨在实现网络灵活组合配置的网络切片安全需要有效的隔离机制，以此实现网络功能在不同切片之

间、基础网络功能域第三方提供的网络功能之间安全共存、安全共享。

3. 无线局域网安全

无线局域网是指应用无线通信技术将计算机、终端、工作站等信息设备互联起来，构成可以互相通信和实现资源共享的网络体系。与传统的有线网络相比，无线局域网配置便捷，扩展性和移动性较好，适用于布线困难、人员流动频繁的环境。随着无线局域网的广泛应用，其安全保护需求日渐突出，需要专门的网络传输保护机制保护数据的传输安全，需要边界接入控制相关技术，如身份认证、访问控制等，保护无线局域网的边界安全。因此，无线局域网安全研究的目标是构建无线局域网安全保护机制，实现安全的无线局域网传输和边界保护。

针对无线局域网自身特点，无线局域网络标准 IEEE802.11 中定义了开放系统认证（Open System Authentication）和共享密钥认证（Shared Key Authentication）两种认证方式，定义有线等价保密（Wired Equivalent Privacy，WEP）采用序列密码算法 RC4 保障数据传输安全。针对上述机制中 WEP 存在弱密钥、密钥管理、初始向量重用等问题，难以有效保护传输数据安全性问题，IEEE802.11i 中重新定义了新的安全体系——坚固安全网络，其中定义了 TKIP（Temporal Key Integrity Protocol）或 CCMP（Counter-Mode/CBC-MAC Protocol）两种加密机制，前者对 RC4 进行升级，可通过升级固件和驱动程序来提高适用 WEP 加密机制的设备安全性，并增加 RSN 作为可选算法；后者基于高级加密标准 AES 加密算法和 CCM*（Counter-Mode/CBC-MAC）认证方式，是 IEEE802.11i 最强的安全算法。

针对 OSA 认证为单向认证，无法提供站点单向认证，容易受到会话劫持和中间人攻击的问题，IEEE802.11 工作组公布了 IEEE802.1x 协议，该协议提供了可靠的用户认证和密钥分发框架，其核心是 EAP。EAP 是一种封装协议，在具体应用中根据不同的认证方式进行扩展，可选 EAP-TLS、PEAP、EAP-SIM 等任意一种，其中 EAP-TLS 最为主流，可以有效地抵抗窃听攻击、身份欺骗、中间人攻击、会话劫持、重放攻击、报文篡改等。感兴趣的读者可借鉴参考文献进一步了解。

4. 操作系统安全

操作系统安全是保障计算机系统、网络、数据安全的基础，一个安全的操作系统能够有效防御各类安全威胁，保护敏感数据，维护系统的稳定性。操作系统安全分狭义和广义两个方面，前者主要是指对外部攻击的防范，而后者是指保障系统的机密性、完整性和可用性。作为网络空间安全一项常见技术，这里我们重点介绍安全操作系统。

安全操作系统是指计算机信息系统在自主访问控制、强制访问控制、标记、身份鉴别、客体重用、安全审计、数据完整性、隐蔽信道分析、可信路径、可信恢复等十个方面满足响应的安全技术要求。主流操作系统 Linux 和 Windows 均通过自身安全机制设计实现操作系统的安全。SELinux 通过定义 LSM（Linux Security Module）框架、SELinux 引用监视器（含授权模块和策略库）、强制访问控制策略来实现一个安全的操作系统，其中

LSM 旨在通过在 Linux 中加载该安全内核模块实现操作系统底层用户进程的监测、可信和保护；引用监视器则通过授权模块为强制保护系统在策略库中建立抽全查询；强制访问控制策略确保只有系统管理员可以修改保护系统的状态。

Windows 操作系统的安全性一直为人诟病，其安全机制设计主要体现在 Windows Vista，Windows 7 之后沿用 Windows Vista 的安全机制，具体包括用户账号控制、强制完整性控制、用户界面特权隔离、网络访问保护等。用户访问控制旨在使用户能够适用标准用户权限而不是管理员权限运行系统；强制完整性控制基于 Biba 完整型模型建立，由系统保护对象（文件、进程、注册表）的系统防控控制列表的访问控制项控制，实现对资源分等级保护；用户界面特权不允许低特权等级进程向高特权等级进程发送窗口消息；网络访问保护则确保每台计算机在连接本地网络时必须通过网络访问保护策略的允许，确保隔离出现问题的计算机。

5. 数据库安全

数据库系统是当今大多数信息系统中数据存储和处理的核心。数据库安全研究的基本目标是研究如何实现数据库内容的机密性、完整性与可用性保护，防止非授权的信息泄露、内容篡改及拒绝服务等。数据库安全相关技术包括高安全等级数据库管理技术、数据库访问控制技术、数据库加密技术等。安全数据库管理通常通过数据库形式化安全模型确保数据库多级关系、多级关系完整性约束、多级关系操作能够实现；数据库访问控制技术则通过访问控制机制的设计防止数据库表及内容的非授权访问，确保访问控制过程中不存在隐通道；数据库加密提供密码控制手段来保护数据的存储安全。

随着网络技术的飞速发展，数据集服务、云计算存储成为新的数据库模式，伴随而生新的数据库安全问题。其关注的焦点主要集中在数据库安全检索、数据库密文访问控制、数据库水印、数据完整性保护、海量数据隐私保护等方面。

6. 可信计算

可信计算（Trusted Computing）通过建立一种特定的完整性度量机制，使计算平台运行时具有分辨可信程序代码和不可信程序代码的能力，从而对不可信程序代码建立有效的防止方法和措施。可信计算利用硬件属性作为信任根，系统启动时层层度量，建立一种隔离执行的运行环境，保障计算平台敏感操作的安全性，从而实现对可信代码的保护。

可信计算平台模块（Trusted Computing Module，TPM）通常的构建方式是结合计算机系统平台体系结构，在硬件系统中嵌入一个可信硬件模块（Trusted Cryptography/Control Module，TCM），在软件系统中构建一个可信平台服务模块，然后以可信硬件模块为可信根，通过可信平台服务模块，建立系统平台完整性、身份可信性和数据安全性 3 个维度的安全功能。信任根、隔离执行和远程执行是可信计算的信任核心。信任根通常在物理层，将用户信任锚点固定在系统中最基础、变化最小的部分，以便确保信任证据的绝对可信；隔离执行基于 CPU 的隔离首保来保护环境运行的代码、数据的安全性，可信执行环境（TEE）是隔离执行的重要技术手段，独立于主机系统之外的安全隔离子系统，可以对

主系统的敏感操作进行安全检查，依据安全策略检查内核和应用程序的状态，对外证明当前系统的可信性；远程证明将可信计算平台的内部信任通过网络拓展至外部。安全启动、可信执行环境、度量与执行、可信存储是可信计算的四大关键技术，安全启动确保系统的初始可信；可信执行环境建立隔离受保护的安全计算环境，确保系统运行时信任；度量与证明基于信任根或可信执行环境度量系统当前运行状态，并对外证明当前系统可信；可信存储则用于保障系统运行时敏感数据安全和数据存储安全。

有关可信计算内容的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络空间安全技术》。

7. 数据与信息安全

数据安全是研究网络与系统中数据保护方法的一门科学，它既包括访问控制、信息流控制、隐私保护等各种控制手段，也包括容灾备份与数据恢复等各种方法。数据安全涉及数据产生、采集、传输、共享、交换、处理、存储、使用、销毁的全生命周期，周期中的每个环节都面临不同的网络安全威胁，需要面向数据的全生命周期进行安全保护。数据安全相关关键技术包括隐私计算、密文检索、密文计算、信息流控制、容灾备份、数据恢复等。

有关数据安全的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络安全保护制度与实施》和《数据安全管理与技术》。

8. 应用安全

应用安全是为保障各种应用系统在信息的获取、存储、传输和处理各个环节的安全所涉及的相关技术的总称。密码技术是应用安全的核心支撑技术，系统安全技术与网络安会技术则是应用安全技术的基础和关键技术。应用安全涉及如何防止身份或资源的假冒、未经授权的访问、数据的泄露、数据完整性的破坏，系统可用性的破坏等。关键技术包括身份认证与信任管理、应用访问控制、Web 安全、App 安全、电子商务安全等。

有关应用安全内容的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络安全建设与运营》。

9. 网络安全检测与评估

网络安全检测评估（简称安全测评）是指对网络安全模块、产品或信息系统的安全性进行验证、测试、评价和定级，以规范它们的安全特性。安全测评的目的是形成针对模块、产品或信息系统安全性的系统性、权威性的判断，对于模块和产品的设计、研发、集成、使用，以及信息系统的规划、设计、建设、运营、维护等工作提供安全性指导。安全测评技术能够系统、客观、准确、全面地测试并评价模块、产品和信息系统的安全性并给出量化评估结果，包括测试和评估两方面的技术，前者通过分析或技术手段对测试对象（模块、产品、信息系统等）的安全性进行检测和验证，获得测试对象的网络安全度量指标；后者包括一系列标准化的流程和方法，用于在测试的基础上对测试对象的安全性进行客观、公正的评价和估算。典型的网络安全测评技术包括等级测评、密码应用安全性评

估、产品测评与认证、软件 / 系统安全测试、风险评估、渗透测试等。本书第 8 章将重点介绍，这里不再赘述。

有关网络安全检测与评估的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络安全检测评估技术与方法》。

10. 等级保护 / 重要信息系统安全

《中华人民共和国网络安全法》第二十一条规定，国家实行网络安全等级保护制度。该制度的核心是对网络实施分等级保护和分等级监管。2003 年，《国家信息化领导小组关于加强信息安全保障工作的意见》在部署等级保护工作时指出：“信息化发展的不同阶段和不同的信息系统有着不同的安全需求，必须从实际出发，综合平衡安全成本和风险，优化信息安全资源的配置，确保重点。要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南。”

根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，网络分为五个安全保护等级。安全等级越高，其安全保护能力要求也就越高，应保证等级保护对象具有相应等级的安全保护能力。第三级及以上的等级保护对象是国家核心系统。等级保护工作分为定级（确定等级保护对象等级）、备案（向公安机关报备）、建设整改（按等级要求进行规划设计 / 建设 / 整改）、等级测评（对安全状况进行检测评估）、监督检查（对三级以上系统安全保护状况进行监督检查）。

有关网络安全等级保护内容的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络安全保护制度与实施》。

11. 关键信息基础设施保护

《中华人民共和国网络安全法》第三十一条规定，国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或数据泄露就可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上实行重点保护。

关键信息基础设施运营者应按照《关键信息基础设施安全保护要求》，落实关键信息基础设施安全保护措施，包括分析识别、安全防护、检测评估、技术对抗、事件处置六个环节的措施。分析识别是关键信息基础设施安全保护的首要环节，主要是围绕关键信息基础设施所承载的关键业务，开展业务依赖性识别、关键资产识别、风险识别等，当关键信息基础设施发生重大变化时，重新开展分析识别和认定工作。安全防护应在落实等级保护制度的前提下，从安全管理制度、安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运维管理、供应链安全、数据安全防护等方面进行保护措施加强。检测评估要求运营者应建立健全关键信息基础设施安全检测评估制

度，制定检测评估方案，确定检测评估的服务机构选择、流程、过程管理、方式方法、周期、人员组织、资金保障等。监测预警应建立监测预警制度、建设监测预警技术手段，开展网络安全风险威胁的通报预警和应急处置，建立攻防对抗队伍、开展攻防演练，加强供应链和数据安全防护。

有关关键信息基础设施保护内容的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络安全保护制度与实施》。

12. 云计算安全

网络空间应用的不断发展产生了海量数据，这对传统的数据存储、计算提出了巨大挑战，云计算技术应运而生。云计算是一种计算方法，即按需提供的服务汇聚成高效资源池，以服务的形式交付给用户使用，云服务、云主机、云平台相继出现，云计算安全是一个从云计算所需要的伴生安全概念，是指云及其承载的服务可以高效、安全、持续、稳定运行。云安全类似传统领域安全，涵盖云环境所涉及的物理安全、网络安全、主机安全、数据库安全、应用安全等，云安全在传统安全的基础上还增加了虚拟安全等方面的安全保护。同时，在安全设备商也可以实现虚拟化安全设备的部署，如云 WAF 等。

虚拟化技术通过将物理硬件资源虚拟化为多个独立的虚拟机（Virtual Machine，VM），提高了硬件利用效率和灵活性，也因此带来了安全隔离的挑战。虚拟化安全是一种保障虚拟机之间、虚拟机和宿主机之间、以及虚拟机与外部网络之间的隔离与通信安全的技术，通常包括虚拟化软件安全、虚拟网络隔离、虚拟机加密技术。其中虚拟化软件安全研究虚拟化软件自身身份认证、访问控制、虚拟机隔离、安全漏洞修补更新等技术，确保管理虚拟机运行的底层软件安全。虚拟网络隔离技术研究虚拟机之间的网络通信安全，防止因虚拟化带来的网络攻击、数据泄露、配置管理等威胁风险，确保虚拟机网络通信隔离和安全。虚拟机加密技术研究虚拟机承载数据安全性、隐私保护以及响应密钥管理和分发问题。

有关云计算安全内容的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络安全保护制度与实施》。

13. 内容安全

内容安全主要是指数字内容的制作、复制、传播和流动得到人们预期的控制和监管，内容安全技术就是指实施这类控制和监管的技术，又称网络舆情监管，通常在对网络公开发布信息的深入与全面提取的基础上，通过对海量非结构化信息的挖掘与分析，实现对网络舆情的热点、焦点、演变等信息的掌握，从而为网络舆情监测与引导部门的决策提供科学的依据。随着网络空间应用的富化，舆情监管对象从文本内容向图片、音频、视频等多媒体内容监管过渡。

内容安全关键技术主要包括文本内容过滤、话题识别与跟踪、内容分级监管以及多媒体内容安全。内容过滤通过分析获得内容本身的性质，之后根据相关监管要求实施响应的控制策略；话题识别与跟踪技术以网络新闻、广播和电视信息流为处理对象，将内容按照话题区分，监控对新话题的报道，并将涉及某个话题的报道组织起来，以某种需要的方式

呈现给用户；内容分级监管是一种主动内容安全技术，它是指在内容发布之前，在内容中嵌入分级标识，随后各种监管措施基于分级标识进行。多媒体内容安全主要通过监管多媒体内容的制作和散布情况，制约不良和盗版内容的制作和传播，包括了大量的多媒体编解码、信号处理和模式识别等技术。

14. 人工智能安全

在 5G、大数据、云计算、深度学习等新技术的共同驱动下，人工智能作为新型基础设施的重要战略性技术加速发展，并与社会各行各业创新融合。人工智能技术的快速发展和广泛应用为社会带来了巨大的变革，同时也带来了一系列的安全挑战。这些挑战不仅涉及个人隐私和数据安全，也关乎国家安全和社会稳定。人工智能的发展表现出以下特征：一是人工智能执行的关键业务对安全防护的实时性提出了更高要求；二是人工智能的个性化服务需求对敏感信息保护提出了更高要求；三是人工智能跨组织融合对数据安全共享提出了更高要求；四是基于机器学习的安全算法与软件漏洞问题日益突出。

有关人工智能安全的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《人工智能安全治理与技术》。

15. 入侵检测技术

入侵检测（Intrusion Detection）是用于检测损害或者企图损害系统的机密性、完整性或可用性等行为的一类安全技术。这类技术通过在受保护网络或系统中部署检测设备，监视受保护网络或系统的状态与活动，根据采集的数据，采用相应的检测方法发现非授权或者恶意的系统及网络行为，并为防范入侵行为提供支持手段。

入侵检测的核心技术是其采用的分析检测方法，即根据已有的知识，判断网络和系统是否遭受攻击以及遭受何种攻击。主流的分析检测方法包括异常入侵检测和误用入侵检测两类，也出现了一些新的方法，例如引入人工免疫、基因算法、代理方法、数据挖掘思想的检测方法，以及利用当前快速发展的人工智能技术进行的智能化检测。

误用检测（Misuse Detection）也称为特征检测、指纹检测或基于签名的检测（Signature-based Detection）等。误用检测基于以下事实：程序或者用户的攻击行为存在特定的模式，这类攻击行为被称为系统的误用行为。误用检测技术首先建立各类入侵的行为模式，对它们进行标识或编码，形成误用模式库；在运行中，入侵检测系统对数据进行分析检测，检查是否存在已知的误用模式（攻击行为）。异常检测的关键在于建立“正常使用描述”（Normal Usage Profile，NUP）以及利用 NUP 对当前系统或者用户行为进行比较，判断出与正常模式的偏离程度。“描述”（Profile）通常由一组系统或用户行为特性的度量（Metrics）组成，一般为每个度量设置一个门限值（Threshold）或者一个变化范围，当超出它们时认为出现异常。

有关入侵检测技术的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络安全事件处置与追踪溯源技术》《网络安全威胁情报分析与挖掘技术》《恶意代码分析与检测技术》。

16. 网络威胁情报分析与挖掘

根据 Gartner 的定义，安全威胁情报是针对已经存在或正在显露的威胁或危害资产行为，基于证据知识，包含情境、机制、影响和应对建议，用于帮助解决威胁或危害进行决策的知识。威胁的三要素包括意图、能力和机会，如果攻击者有意图有能力，但是攻击对象没有脆弱性或者说没有机会，那么攻击者并不构成威胁。威胁情报分析与挖掘技术是一种基于威胁模型和安全数据分析威胁行为的技术，通过挖掘行为模式和推理攻击意图来了解这些数据之间的关系。在大数据和人工智能技术中进行智能威胁情报分析，可以智能地支持防御策略的制定，实现更精准的动态防御。威胁分析的价值在于通过获取和关联攻击数据来提高威胁参与者的攻击检测和归因准确性。

在当前复杂的网络攻防博弈过程中，攻击方通常根据攻击意图和能力，通过杀伤链 7 个步骤（侦察、武器化、装载、利用、安装、控制、达成目标）向攻击目标发起攻击，而防御方则依赖主动防御的思想采取 WPDRRC（预警、防御、检测、响应、恢复、反制）模型的纵深动态防御机制。由于攻防双方信息的非对称性，使得传统的防御方大多处于被动局面，即攻击方暗处而防御方的信息已先期被侦察、掌握。从杀伤链来看，越早发现攻击者的踪迹，就能使防御方越早控制攻击进程，使攻击陷入被动。这也正是安全威胁情报分析在化解攻击杀伤链过程中的价值所在，即安全专家以基于大数据的威胁情报分析为有力武器，通过跨部门、跨组织边界的威胁情报共享，使关于攻击者和攻击手段的各种信息逐步明朗起来，使防御方对正在和即将面临风险的不确定性逐渐消失，并针对安全威胁加固资产，进而成功阻断瓦解攻击方的进攻。

有关网络威胁情报分析与挖掘的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《网络安全威胁情报分析与挖掘技术》。

17. 恶意代码分析与检测

以计算机病毒、蠕虫和特洛伊木马为代表的恶意代码对网络、系统的正常使用以及信息安全造成了危害。恶意代码分析技术对恶意代码传播、感知和出发机制进行分析挖掘，包括恶意代码散布和侵入受害系统的方法分析、恶意代码依附于宿主机或隐藏于系统中的方法分析、恶意代码执行的方法 / 条件 / 路径出发机制分析等，以此为恶意代码监测、清除与预防提供基础。

恶意代码分析从技术层面可以分为静态分析和动态分析，静态分析可通过反汇编而进行文件寻找关键的代码流程来帮助分析理解恶意代码的内部细节；动态分析则通过调试或虚拟运行等手段运行恶意代码，通过查看指令执行信息来跟踪发现恶意代码的行为。恶意代码监测通常包括特征代码法、校验和法、行为监测法、软件模拟法、比较法和感染实验法。恶意代码清除是指尽量在保全被感染程序功能的情况下移除恶意代码或使其失效。恶意代码预防则通过切断传播和感染的途径或破坏它们实施的条件来抵御恶意代码的传播和感染。

有关恶意代码分析与检测内容的详细介绍，见高等院校网络空间安全专业实战化人才

培养系列教材中的《恶意代码分析与检测技术》。

18. 漏洞挖掘与渗透测试

漏洞挖掘是一种查找目标软件、系统中可能存在脆弱性的技术。根据挖掘对象的不同，漏洞挖掘技术通常分为基于源代码的漏洞挖掘和基于目标代码的挖掘。漏洞挖掘的主要方法包括：手工测试技术，通过人的手工方式向测试的目标系统或软件发送特殊的数据，这些数据包括正确的或错误的输入，在发送数据后，通过观察测试目标对输入数据的反应来查找系统中可能存在的漏洞；Fuzzing 技术的实现原理是软件工程中的黑盒测试思想，其主要方法是使用大量的数据作为应用系统或软件的输入，以目标对象接受输入后是否出现异常为标志，来查找目标系统中可能存在的安全漏洞；动态分析技术是指在目标系统或软件的动态运行中查找漏洞的技术。其主要思想是在特定的容器中运行目标程序，通过目标程序在执行过程中的状态信息来发现潜在问题，这些状态信息包括当前内存使用状况、CPU 寄存器的状态等方面；静态分析技术是通过程序的语法、语义来检测目标中可能潜在的安全问题。其基本思想是对测试的目标系统或软件的源代码进行静态分析、扫描，重点是检查函数的调用、边界检测和缓冲区检测，也就是对容易在安全方面出现漏洞的代码进行重点的查找、分析，以期能够发现问题；补丁比较技术也称为二进制文件比较技术，在漏洞挖掘中往往是指对“已知”漏洞的探查，通过对比打上补丁前后的二进制文件来发现目标是否存在漏洞。

渗透测试（Penetration Testing）是指由安全人员利用安全工具并结合个人实战经验，通过模拟攻击的技术与方法，对指定的目标进行非破坏性质的模拟黑客攻击和深入的安全测试，发现信息系统隐藏的安全脆弱性，并根据系统的实际情况，测试系统脆弱性被一般攻击者利用的可能性和被利用后的影响，了解攻击者可能利用的攻击方法和进入信息系统的途径，帮助用户进一步了解目标系统的安全状况，采取强有力的安全方式提前防御。

有关漏洞挖掘与渗透测试内容的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《漏洞挖掘与渗透测试技术》。

19. 数据勘查与取证

数据勘查与取证是基于侦查思维，采用取证技术，获取、分析、固定电子数据作为认定事实的科学过程，是能够为法庭接受的、足够可靠和有说服力的、存在于网络设备中的电子数据的确认、保护、提取和归档的过程。数据勘查与取证通常由勘验准备、保护现场、外围勘验、搜集证物、提取和固定证据、固定证物、证物的传递和移交等步骤组成。数据勘查与取证技术按照勘查取证的目标对象不同，通常可分为单机电子数据取证技术（包括计算机、移动智能终端、移动存储介质等）、服务器电子数据取证技术、网络电子数据取证技术，这些技术在满足电子取证基本原则的前提下，辅助公安机关完成网络违法犯罪现场的勘验。

有关数据勘查与取证内容的详细介绍，见高等院校网络空间安全专业实战化人才培养系列教材中的《数字勘查与取证技术》。

1.6.3 网络安全常见产品

网络安全技术的发展促成了大量网络安全产品的成熟、落地与应用，当前市场主流的网络安全产品包括身份认证与访问控制产品，如智能 IC 卡、统一认证与单点登录系统、智能密码钥匙等；数据与信息安全产品，如数据加密机、加密存储系统、数据防泄露产品、加密硬盘等；计算环境安全产品，如安全操作系统、安全数据库系统、可信计算平台、终端安全管理系统、主机防病毒产品等；通信安全产品，如 VPN、安全网关等；边界安全防护产品，如防火墙、安全隔离设备、网络接入控制系统、信息安全交换产品等；安全检测与监测审计产品，如入侵检测系统、入侵防御系统、态势感知系统、主机 / 网络脆弱性扫描器、安全审计系统等；应用安全产品，如反垃圾邮件系统、网页防篡改、敏感内容过滤系统；安全服务产品，如安全运营管理系统、安全检测工具等。本节对防火墙、入侵监测系统、VPN、安全运营 4 类典型网络安全产品进行介绍。

1. 防火墙

防火墙是最为常见的网络防护技术产品，几乎所有组织机构的网络出口处都会选择部署防火墙，部分机构在内部不同网络之间也部署了防火墙设备。防火墙是一个网络安全设备或者由多个硬件设备和相应软件组成的系统，位于不可信的外部网络和被保护的内部网络之间，目的是保护内部网络不遭受来自外部网络的攻击和执行规定的访问控制策略。如果防火墙部署在内外网之间，所有内网到外网的通信以及外网到内网的通信都必须经过防火墙，只有满足访问控制策略的通信才允许通过。防火墙本质上是一种实现网络层访问控制策略的设备，由于防火墙通常串接在网络中，因此设备本身具有较高的计算能力和通信处理能力。

防火墙的主要功能包括：过滤不安全的网络服务和通信行为，例如阻止外部 ICMP 数据包进入内部网络；禁止未授权用户访问内部网络，例如不允许来自特殊地址的通信，或对外部连接进行用户认证；控制对内网的访问方式，例如只允许外部访问连接内部网络特定区域中的 WWW、FTP 和邮件服务器，而不允许访问其他服务器；记录相关的网络访问事件，提供访问数据统计、预警和访问审计功能。

随着防火墙技术的发展，其功能也逐渐扩展，增加了如防止内部信息泄露、提供应用层安全过滤等功能。同时，防火墙也越来越多地和其他类型网络设备或安全设备结合在一起，例如路由器、网关、虚拟专用网（Virtual Private Network，VPN）设备等。

（1）包过滤防火墙

包过滤防火墙是最经典的防火墙，也是防火墙实现安全防护工作的设计初衷。包过滤防火墙工作在网络协议栈的网络层，逐一检查每个流经的网络层数据包（通常是 IP 数据包），判断数据包是否满足既定的过滤规则，如果满足则允许通过，否则进行阻断。IP 数据包的包头中包含了承载的协议类型、源地址、目的地址、源端口、目的端口、标志位等信息，包过滤防火墙可以检查协议类型控制各个协议的通信，检查 IP 地址控制来自特

定源地址或者发往特定目的地址的通信，也可以检查端口控制对外部服务的访问和内部服务的开设。包过滤防火墙的管理员负责制定这些过滤规则，将规则配置到防火墙系统中并启用。

包过滤防火墙具有通用性强、效率高、性价比高等优势，但也存在较为明显的缺点，主要包括：仅能够执行较简单的安全策略，例如只能对单个 IP 数据包进行检查，当需要完成复杂的涉及多个数据包的检查任务时，就显得力不从心；另一方面，包过滤防火墙通常只针对包头部分进行检查，对于利用特定应用层协议的攻击行为，则无法检查；另外，仅通过端口来管理服务和应用通信不够合理，因为一些特定服务或应用的端口号并不固定。因此，在网络安全实际应用的不断推动下，防火墙逐渐发展出了更多的功能。

（2）连接状态防火墙

连接状态防火墙增加了对连接状态的控制。连接状态是指一个连接的上下文情况，连接状态防火墙可以更准确地判断一个从外向内或从内向外的连接的合法性，在一定程度上防止了一些潜在的网络攻击。由于连接状态是随着通信进行不断变化的，因此基于连接状态的访问控制也被称为“动态过滤”。

很多网络攻击都利用正常的网络应用协议（如 HTTP、SMTP、FTP 等）来实施，需要对网络连接的完整信息进行综合判断后，才能确定是属于攻击还是正常的访问请求，此时如果仅使用前面介绍的包过滤防火墙，则由于缺乏完整的连接信息而无法完成检查工作。利用连接状态防火墙，结合应用载荷检查，可以较为精准地发现此类攻击。

（3）代理网关

一般认为来自外部网络的连接请求是不可靠的，代理网关是执行连接代理程序的网关设备或系统，按照一定的安全策略，判断是否将外部网络对内部网络的访问请求提交给相应的内部服务器，如果可以提交，代理网关将代替外部用户与内部服务器进行连接，也代替内部服务器与外部用户连接。在此过程中，代理网关相当于外部用户与内部服务器之间的“中间人”，面向外部用户担当服务器的角色，面向内部服务器担当用户的角色，因此，代理网关中既包含服务器的部分，也包含客户端的部分。按照网关所处的网络层次，可以将其分为回路层代理和应用层代理。

回路级代理也称为电路级代理，建立在传输层上。在建立连接之前，先由代理服务器检查连接会话请求，若满足配置的安全策略，再以代理的方式建立连接。在连接中，代理将一直监控连接状态，若符合所配置的安全策略则进行转发，否则禁止相关的 IP 通信。由于这类代理需要将数据传输给上层处理，再接收处理或回应结果，类似于建立了数据回路，所以被称为回路级代理。由于回路级代理工作在传输层，它可以提供较为复杂的访问控制策略，而不仅是通过检查数据包包头实施访问控制策略。回路级代理的特点是：对于全部面向连接的应用和服务，只存在一个代理。回路层代理的代表是 SOCKS 代理系统，它面向控制 TCP 连接，由于需要实现对客户端连接请求的统一认证和代理，普通客户端需要加入额外的模块，多数浏览器都提供了对于这项功能的支持。

应用层代理则针对不同的应用或服务具体设计，因此对不同的应用或服务存在不同的

代理。应用层代理由于需要对应用层协议进行还原和分析，其处理性能明显低于前面介绍的包过滤防火墙。

（4）应用防火墙

典型的应用防火墙如 Web 应用防火墙（WAF），能够为 Web 服务器提供应用层防护功能，对通过 HTTP 协议传输的 Web 访问数据进行分析和过滤，根据预定义的检测规则或自适应检测算法，自动发现并过滤掉那些存在典型 Web 攻击（如 SQL 注入、XSS 等）的访问请求，从而实现功能较强的应用级安全防护策略。

2. 入侵检测系统

入侵检测系统（IDS）通常分为数据源、分析检测和响应三个模块，如图 1-3 所示。数据源模块为分析检测模块提供网络和系统的相关数据和状态，分析检测模块执行入侵检测后，将结果提交给响应模块，后者采用必要的措施，以阻止进一步的入侵或恢复受损害的系统。在以上过程中，用于支持检测工作的数据库起到了重要作用，它负责存储入侵行为的特征模式，通常也称为入侵模式库或入侵特征库。

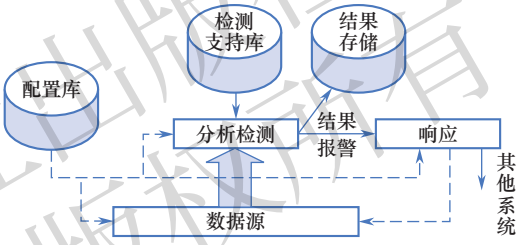

图 1-3　IDS 的系统架构

针对 IDS 的系统架构，比较有影响的成果是美国加州大学戴维斯分校研究人员提出的通用入侵检测框架（Common Intrusion Detection Framework，CIDF）。CIDF 是一套规范，它定义了 IDS 表达检测信息的标准语言以及 IDS 组件之间的通信协议。符合 CIDF 规范的 IDS 可以共享检测信息、相互通信、协同工作，还可以与其他系统配合实施统一的配置响应和恢复策略。CIDF 的主要作用在于集成各种 IDS 使之协同工作，实现各 IDS 之间的组件重用。按照 IDS 数据源的不同，IDS 主要可以分为以下三类。

（1）基于主机的 IDS

基于主机的 IDS 的检测目标主要是主机系统和本地用户，它可以运行在被检测主机或者其他单独的主机上，根据主机的审计数据和系统日志发现攻击迹象。若攻击者已经突破网络防护设施，进入被攻击主机的操作系统中，则基于主机的 IDS 能够发现主机被攻击情况并提供及时的响应。基于主机的 IDS 依赖于主机的审计数据和系统日志，这些数据本身容易被攻击者清除或者修改，攻击者也可能使用某些特权操作或者低级别操作逃避审计。基于主机的 IDS 仅分析主机的审计数据和系统日志，一般不能发现网络层面的攻击和审计范围之外的系统攻击。

基于主机的 IDS 进一步发展出了基于系统内核的 IDS，它可以在操作系统内核中检测

异常行为，从而提高了检测的准确性和时效性。

（2）基于网络的 IDS

基于网络的 IDS 主要根据网络流量检测入侵，可以采用分布式部署模式：一个或多个网络探测器（探针）负责采集网络的数据流，对网络数据进行初步处理后传递给分析检测模块。需要指出，为了避免影响网络性能，基于网络的 IDS 通常采用旁路模式部署（而不是串接模式），例如通过分光设备将流量复制后送到 IDS 进行检测，或是将 IDS 部署在交换机的镜像端口，以获得该交换机中传输的全部网络数据。

IDS 的核心技术是其采用的分析检测方法，即根据已有的知识，判断网络和系统是否遭受攻击以及遭受何种攻击。主流的分析检测方法包括异常入侵检测和误用入侵检测两类，也出现了一些新的方法，例如引入人工免疫、基因算法、代理方法、数据挖掘思想的检测方法，以及利用当前快速发展的人工智能技术进行的智能化检测。

（3）分布式入侵检测

分布式入侵检测系统（Distributed Intrusion Detection System，DIDS）能够同时分析来自主机系统审计日志和网络数据流，一般为分布式结构，由多个部件组成。DIDS 可以从多个主机获取数据，也可以从网络传输取得数据。典型的 DIDS 采用控制台 / 探测器结构。NIDS 和 HIDS 作为探测器放置在网络的关键节点，并向中央控制台汇报情况。攻击日志定时传送到控制台，并保存到中央数据库中，新的攻击特征能及时发送到各个探测器上。每个探测器能够根据所在网络的实际需要配置不同的规则集。

3. VPN

虚拟专用网络（VPN）是一种网络技术，它通过加密和隧道协议在公共互联网或不受信任的网络上创建了安全的连接，以实现远程访问、数据保护和隐私保护，在该项技术的支持下，用户可以在不安全的网络上创建一个安全的、私密的网络连接，使得用户可以在远程地点访问网络资源。

VPN 设备主要实现如下功能：隧道建立，隧道建立是 VPN 技术中最关键的技术，是指在隧道的两端通过封装以及解封装技术在公网上建立一条数据通道，使用这条通道对数据报文进行传输；加解密，该项功能设计确保即使传输信息被窃听或者截取，攻击者也无法知晓信息的真实内容，可以对抗网络攻击中的被动攻击；身份认证技术，通过标识和鉴别用户的身份，防止攻击者假冒合法用户来获取访问权限；密钥管理技术，实现对认证过程中密钥信息的安全管理。

VPN 根据其实现方式和协议的不同可以分为多种类型，其中两种主要分类是 IPsec VPN 和 SSLVPN。

（1）IPsec VPN

IPsec VPN 是一种常见的 VPN 类型，它以 Internet 协议安全（IPsec）协议为基础，提供了强大的数据加密和安全性功能。IPsec VPN 在不同网络之间建立安全通道，以确保数据传输的保密性和完整性。

IPsec VPN 使用多个协议来确保数据的安全传输。其中两个主要的 IPsec 协议是 AH（身份验证报头）协议和 ESP（封装安全有效负载）协议。AH 协议负责数据的身份验证，确保数据在传输过程中不被篡改，而 ESP 协议则用于加密和保护数据的隐私。此外，IKE（Internet 密钥交换）协议用于建立和管理 VPN 连接，协商密钥和安全参数。

IPsec VPN 广泛应用于企业和组织中，用于远程访问、分支机构连接、云连接和合规性要求。它们通常用于连接不同地理位置的局域网络（LANs），建立虚拟专用网络，确保远程用户和分支机构能够安全地访问中央网络和资源。

（2）SSLVPN

SSLVPN 是另一种流行的 VPN 类型，它以安全套接层（SSL）协议为基础，提供了通过 Web 浏览器安全访问内部网络资源的能力。SSLVPN 通常不需要额外的客户端软件，因为它使用常见的 Web 浏览器作为接口。

SSLVPN 使用 SSL/TLS 协议来加密数据传输，确保数据的安全性。用户可以通过 Web 浏览器或特定的 SSLVPN 门户访问内部网络资源，通过 SSL 加密通道进行数据传输。SSLVPN 网关负责验证用户身份，并控制用户对资源的访问。

SSLVPN 通常用于提供远程访问，允许用户通过互联网安全地访问公司网络。它们适用于远程办公、出差、合规性要求和访问内部应用程序。

4. 漏洞扫描器

漏洞扫描器是一种用于对目标网络进行漏洞扫描的专业产品，它能够自动检测远程或本地计算机系统的安全脆弱性，发现可利用的漏洞，并提供相应的修复建议。漏洞扫描器基于漏洞数据库，通过扫描等手段对指定的计算机系统进行安全检测，从而发现系统中的安全漏洞，其主要功能包括对网站、系统、数据库、端口、应用软件等网络设备进行智能识别扫描检测，并对其检测出的漏洞进行报警提示管理人员进行修复。漏洞扫描器在网络安全领域中发挥着重要的作用，它可以及时发现和修复网络中存在的安全漏洞，提高系统的安全性，降低被攻击的风险。

漏洞扫描器的主要功能如下。

（1）漏洞检测，漏洞扫描设备能够对网络中的各种设备和系统进行自动化的漏洞检测，包括操作系统、数据库、网络设备、应用程序等。它通过模拟攻击者的行为来尝试利用各种漏洞，并记录下目标系统的反应，以判断是否存在漏洞。

（2）脆弱性评估，漏洞扫描设备能够对目标系统的脆弱性进行评估，识别出可能被攻击者利用的漏洞和弱点。它还能够提供详细的漏洞描述和影响范围，帮助管理员及时了解系统存在的安全风险。

（3）实时监测，漏洞扫描设备可以实时监测网络中的异常行为和恶意攻击，及时发现并阻止潜在的入侵行为。它还可以与防火墙、入侵检测系统等其他安全设备进行联动，共同构建起强大的安全防护体系。

（4）报告生成，漏洞扫描设备能够生成详细的漏洞报告，列出已检测到的漏洞信息和

修复建议。这些报告可以帮助管理员快速了解系统的安全状况，并制订相应的修复计划。

（5）自动化修复，一些高端的漏洞扫描设备还具备自动化的修复功能，能够自动安装补丁或配置安全设置，以消除检测到的漏洞。这大大提高了漏洞修复的效率和安全性。

漏洞扫描器根据扫描对象不同可大致分为如下几类。

（1）网络扫描器，基于网络的扫描器就是通过网络来扫描远程计算机中的漏洞。价格相对来说比较便宜；在操作过程中，不需要涉及目标系统的管理员，在检测过程中不需要在目标系统上安装任何东西，维护简便。

（2）主机扫描器，基于主机的扫描器则是在目标系统上安装了一个代理或者服务，以便能够访问所有的文件与进程，这也使得基于主机的扫描器能够扫描到更多的漏洞。

（3）数据库扫描器，数据库漏洞扫描系统可以检测出数据库的 DBMS 漏洞、默认配置、权限提升漏洞、缓冲区溢出、补丁未升级等自身漏洞。

（4）Web 应用扫描器，专门用于扫描 Web 应用程序的漏洞，例如 SQL 注入、跨站脚本（XSS）和跨站请求伪造（CSRF）等，可以模拟攻击者的行为，识别应用程序中的漏洞并生成报告。

（5）移动应用扫描器，用于扫描移动应用程序中的漏洞和安全问题，可以检测移动应用中的 API 漏洞、不安全的数据存储和未加密的通信等问题。

5. 安全运营管理

安全运营管理是面向信息系统运行阶段的安全服务产品。由于在信息系统运行过程中，安全事件随时都可能发生，因此及时掌握出现的故障和存在的隐患等问题，并采取必要的应对措施。安全运营管理通过统一的运营管理体系和风险管理平台，提供有效的技术、人员及流程支持，帮助用户及时地检测、响应安全事件，针对安全状况实施动态监控和运营管理支持。

安全运营管理中心（SOC）包含安全运营管理类产品的常见形态。它是一个集人员、流程和技术于一体的中心，负责全天候检测端点、服务器、数据库、网络应用程序、网站和其他系统的所有活动，以实时发现潜在的威胁；对网络安全事件进行预防、分析和响应，以改进企业的网络安全态势。其主要功能如下。

（1）监测中心，通过仪表板或态势大屏，总览特定单位范围内的资产安全状况、最新待处理威胁、风险事件、安全事件趋势等值得关注的安全信息。

（2）资产中心，为用户提供资产可视功能，从资产角度了解安全态势，盘点现有资产，对资产进行编辑管理，同时方便运维人员对企业内网资产进行管理。可对用户环境中的各个资产实现列表管理，包含列表呈现各个资产基本信息，例如资产名称、资产 IP、资产来源、资产分组等。

（3）漏洞管理，实时收集互联网最新安全漏洞情报，扫描内网资产安全状况，发现并生成漏洞事件，方便运维跟踪处理。

（4）告警与事件管理，将接收的日志归一化为事件，经关联引擎匹配告警策略，生成

安全告警，帮助用户调查分析、溯源事件、联动处置问题。

（5）调查中心，供用户对日志进行查询、检索。通过接收并保存企业内部各种设备日志及流量日志，提供给安全运维人员进行关键字段筛选搜索。

（6）响应中心，响应中心支持用户在发现安全事件或漏洞事件后进一步处置操作。

（7）报表中心，可根据用户实际需求制定并输出安全报表，方便安全运维人员总结一段时间内的安全工作成果，提供向上汇报、内部总结分析的材料支撑。

根据 SOC 构建模式的不同，SOC 可分为虚拟型 SOC、混合型 SOC、多功能型 SOC/NOC、专业型 SOC、指挥型 SOC 等，不同类型的 SOC 适用于不同的应用场景，在运维人员参与程度方面存在差异，用户单位应根据自身需要选择配备。

习　题

1. 什么是网络空间？
2. 什么是网络空间安全？
3. 网络空间安全的基本属性有哪些？
4. 安全威胁主要包括哪些？
5. 简述漏洞、恶意软件、僵尸网络的定义。
6. 什么是网络攻击？
7. 什么是网络安全事件？
8. 简述密码系统的基本原理。
9. 简述网络空间安全的发展历程。
10. 简述网络安全技术体系。
11. 网络安全产品主要有哪些？