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

网络安全建设与运营

蔡　阳　郭启全　付　静　张　潮　詹全忠
邹　希　吕　鑫　卢　青　孔　勇　编著

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

内 容 简 介

本书共 5 章，围绕“网络安全建设与运营”这一主题，系统介绍网络安全建设与运营的法律要求、体系架构和重点内容。其中，第 1 章概括性介绍网络安全建设与运营基础知识，包括网络安全形势、网络安全建设与运营相关法律法规、网络安全建设与运营相关标准规范、网络安全架构等。第 2 章介绍网络安全管理体系，包括安全管理体系设计与组成、安全管理组织、安全管理制度、安全管理人员、安全建设管理、安全运营管理、安全监督管理等。第 3 章介绍网络安全技术体系，包括网络安全技术架构、基础安全防护措施、数据安全、扩展安全、统一安全支撑平台等。第 4 章介绍网络安全运营体系，包括网络安全运营组织、网络安全运营的关键环节和关键指标等。第 5 章介绍网络安全保障体系，包括网络安全人才队伍建设、经费保障、宣传教育和先进技术应用研究等。

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

网络安全建设与运营 / 蔡阳等编著. -- 北京 : 电子工业出版社, 2025. 7. -- ISBN 978-7-121-50115-9

Ⅰ. TP393.08

中国国家版本馆 CIP 数据核字第 2025ET4963 号

责任编辑：刘御廷　　文字编辑：郭瑞琦
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：13　　字数：288.4 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，luy@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

为实施国家安全战略，加快网络空间安全高层次人才培养，继 2001 年教育部批准设立信息安全专业后，2015 年 6 月，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，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”一级学科的设立，充分体现了国家对网络安全人才培养的关注，同时对网络安全人才培养模式提出了更高的要求。

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，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”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，建立实战化人才教育训练体系，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，培养网络安全实战化人才。

为了满足培养网络安全实战化人才的需要，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》。郭启全统筹规划和整体设计全套教材，组织具有丰富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、人工智能安全等方面的重要知识。

在网络安全防护能力建设中，网络安全的建设和运营工作至关重要。如何落实网络安全相关法律法规和标准规范要求，构建符合机构自身实际发展需要的网络安全管理体系、网络安全技术体系、网络安全运营体系、网络安全保障体系，切实保障网络运行安全、信息安全和数据安全，支撑业务的健康发展成为核心。网络安全建设和运营工作的成功实施需要一支理论知识和实践经验兼具的网络安全人才队伍。为了满足实战化网络空间安全人才培养的需求，由水利部信息中心牵头成立的国家关键信息基础设施（水利）网络安全技

术创新团队，其成员结合多年工作实践编写了《网络安全建设与运营》。

本书主要着眼于政府、企事业单位等机构自身网络安全建设和运营工作的重点难点，力求给读者提供理论和实践相结合的技能知识，并提供了丰富的实践参考案例。全书共分为概述、网络安全管理体系、网络安全技术体系、网络安全运营体系、网络安全保障体系5章。本书由蔡阳、郭启全、付静、张潮主编，詹全忠、吕鑫、孔勇、卢青、邹希、黄屿璁等分别编写相关章节。在本书的编写过程中，得到了水利部信息中心、河海大学、深信服科技股份有限公司、奇安信科技集团股份有限公司等单位的大力支持。

书中不足之处，敬请读者指正。

作者

目录 CONTENTS

第 1 章 概　述

本章阐述网络安全的形势、威胁与它在国家安全中的重要地位，网络安全建设与运营相关法律法规、标准规范和网络安全架构，简要介绍网络安全建设与运营架构所包含的网络安全管理、网络安全技术、网络安全运营和网络安全保障四个体系的内容以及各体系间的关系，旨在使读者对网络安全建设与运营的基础知识与架构内容有一个基本了解。

1.1 网络安全形势

网络安全直接关系到国家安全、经济发展和社会稳定。在全球化的背景下，世界各大经济体日益重视网络安全，并制定了一系列政策来加强网络空间的安全防护。我国同样高度重视网络安全问题，在战略、立法和体系架构等层面实施了多项举措，以确保国家网络空间的安全与稳定。

1.1.1 数字化浪潮中的网络安全

随着信息技术的飞速发展，人类社会前后经历了三次数字化浪潮。第一次数字化浪潮以计算机技术为主要驱动力，计算机技术取代了纯手工处理，人们第一次体会到数字技术带来的工作效率的提升，极大地提高了信息处理能力。第二次数字化浪潮以“互联网 +”为主要驱动力，互联网技术使网络带宽快速上升，通信和计算的界限逐渐消弭，带来计算模式的革命，以敏捷化、虚拟化、扁平化、定制化和网络化为特征的经营管理模式成为主流模式，出现了以信息技术外包、电子商务等为代表的新一代数字化产业形态。第三次数字化浪潮以人工智能为核心，万物智能，万物互联，提供一种消弭不同行为空间区域和活动领域的间隙、满足人类时空一体化信息需求的运算能力，人类由此进入了全球性的动态联盟、泛在交流和分布智能时代。

当今时代，数字技术作为世界科技革命和产业变革的先导力量，日益融入经济社会发展各领域全过程，深刻改变着生产方式、生活方式和社会治理方式。近年来，互联网、云计算、人工智能、区块链等技术加速创新，各国竞相制定数字经济发展战略、出台鼓励政

策，数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。据相关机构统计，2022 年，全球 51 个国家数字经济增加值总规模为 41.4 万亿美元，同比增长 7.4%，占 GDP 比重的 46.1%。产业数字化持续成为数字经济发展的主引擎，占数字经济比重的 85.3%。从规模上看，美国数字经济规模蝉联世界第一，达 17.2 万亿美元，中国位居第二，规模为 7.5 万亿美元；从占比看，英国、德国、美国数字经济占 GDP 比重均超过 65%。

随着数字经济的发展，全社会都在快速地进入数字化、网络化和智能化时代。网络空间在数字化发展的过程中形成，成为陆、海、空、天之后的第五空间。在网络空间里不仅包括通过网络互联而成的各种计算系统（包括各种智能终端）、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。网络空间是信息传播的重要渠道，也是国家竞争和利益博弈的新战场。当前，网络安全威胁与风险日益突出，并逐渐向政治、经济、文化、社会、生态、国防等领域传导渗透。具体包括：利用网络干涉他国内政以及大规模网络监控、窃密等活动严重危害国家政治安全和用户信息安全，关键信息基础设施遭受攻击破坏、发生重大安全事件严重危害国家经济安全和公共利益，网络谣言、颓废文化和淫秽、暴力、迷信等有害信息侵蚀文化安全和青少年身心健康，网络恐怖和违法犯罪大量存在直接威胁人民生命财产安全、社会秩序。围绕网络空间资源控制权、规则制定权、战略主动权的国际竞争日趋激烈。

在此过程中，网络安全始终扮演着重要的角色，与信息化是一体之两翼、驱动之双轮。《中华人民共和国网络安全法》中网络安全的定义是：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，以及保障网络数据的完整性、保密性、可用性的能力。随着数字化浪潮的不断推进，网络安全将安全的范围拓展至网络空间中的一切安全问题，涉及网络政治、网络经济、网络文化、网络社会、网络外交、网络军事等诸多领域，所反映的信息要更立体、更宽领域、更多层次、更多样，更能体现网络和空间的特征，并与其他安全领域有更多的渗透与融合。

网络安全研究的是网络空间中的安全威胁和防护问题，即在对抗环境下，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。网络安全的主要内容仍然是信息安全，但不仅仅包括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。在数字化浪潮中，网络安全既是数字经济健康发展的基础保障，更是促进技术创新、维护社会稳定、建设网络强国的重要基石。

1.1.2 网络安全事件

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，对网络信息系统或者其中的数据和业务应用造成危害，对国

家、社会、经济造成负面影响的事件。随着信息技术的发展，网络安全威胁逐渐从简单的信息安全向网络空间安全渗透，各种新技术被用在网络攻击之中，造成的危害日益严重。2023 年我国颁布《信息安全技术 网络安全事件分类分级指南》（GB/T 20986—2023）国家标准，综合考虑网络安全事件的起因、威胁程度、攻击方式与损害后果等因素，将网络安全事件具体分为恶意程序事件、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、违规操作事件、安全隐患事件、异常行为事件、不可抗力事件、其他事件等十大类事件。

1. 恶意程序事件

恶意程序事件是指将带有恶意意图所编写的一段程序插入网络，损害网络中的数据、应用程序或操作系统，影响网络的正常运行的网络安全事件，恶意程序在网络中的蓄意制造与传播将导致业务损失，甚至造成社会危害。恶意程序事件包括计算机病毒事件、网络蠕虫事件、特洛伊木马事件、僵尸网络事件、勒索软件事件等子类，具体如下：

（1）计算机病毒事件：制造、传播或利用恶意程序，影响计算机使用，破坏计算机功能，毁坏或窃取数据。

（2）网络蠕虫事件：利用网络缺陷，蓄意制造或通过网络自动复制并传播网络蠕虫。

（3）特洛伊木马事件：制造、传播或利用具有远程控制功能的恶意程序，实现非法窃取或截获数据。

（4）僵尸网络事件：利用僵尸工具程序形成僵尸网络。

（5）勒索软件事件：采取加密或屏蔽用户操作等方式劫持用户对系统或数据的访问权，并借此向用户索取赎金。

勒索软件是一类典型的恶意程序。2017 年 5 月，一款名为 WannaCry 的勒索软件在全球范围内迅速传播，感染了大量的计算机和网络系统，波及全球至少 150 个国家、30 万名用户，影响到金融、医疗、交通等多个行业，仅 3 天时间就造成高达 80 亿美元的损失。近几年，勒索软件事件愈演愈烈，各大勒索攻击团伙不断改进攻击手法和模式，对各大机构、团体及用户发起有组织、有针对性、常态化的勒索软件攻击，使得相应的防范及反制愈发困难。特别地，随着人工智能、大数据等新兴技术的成熟应用，勒索软件攻击变得更加复杂、更具针对性，网络安全态势进一步恶化。据 2023 年数据统计显示，当年全球共发生了 4832 起勒索软件攻击事件，较 2022 年剧增了 83%，且全球化扩散趋势显著，造成的直接与间接经济损失难以估量。

2. 网络攻击事件

网络攻击事件是攻击者对网络系统的机密性、完整性、可用性等产生危害的行为，通过技术手段对网络实施攻击而导致大规模的经济损失或造成严重的社会危害的网络安全事件。攻击者利用被攻击方网络系统自身存在的漏洞，通过使用网络命令和专用软件，侵入其网络系统并实施攻击。网络攻击事件包括网络钓鱼事件、网络扫描探测事件、后门植入事件、拒绝服务事件、网页篡改事件等子类，具体如下：

（1）网络钓鱼事件：利用欺诈性网络技术诱使用户泄露重要数据或个人信息。

（2）网络扫描探测事件：利用网络扫描软件获取有关网络配置、端口、服务和现有脆弱性等信息。

（3）后门植入事件：非法在网络中创建能够持续获取其管理权限的后门。

（4）拒绝服务事件：通过非正常使用网络资源影响或破坏网络可用性。

（5）网页篡改事件：通过恶意破坏或更改网页内容影响网站声誉或破坏网页及网站可用性。

分布式拒绝服务（Distributed Denial of Service, DDoS）攻击是拒绝服务事件的一种常见形式，原理是利用多台受控的计算机系统或其他互联网设备作为攻击流量的来源，向目标主机发送大规模互联网流量，使目标主机的网络或系统资源耗尽，导致其无法正常向用户提供服务。DDoS 攻击者一般针对重要服务和知名网站进行攻击，严重威胁互联网的安全。2016 年 10 月，美国主要域名服务商 Dyn 公司遭受大规模 DDoS 攻击。攻击者利用名为“Mirai”的病毒感染大量物联网设备，形成僵尸网络，再向 Dyn 公司的域名解析服务器发起网络攻击，造成域名解析服务中断。超过 1000 台域名服务器受到影响，导致美国东海岸地区大量域名解析服务中断或延迟，其中包括推特、网飞、亚马逊、爱彼迎、华尔街日报等知名网站。近年来，随着物联网技术的不断成熟，攻击者开始将冰箱、洗衣机、摄像头等新型互联网设备作为攻击与利用的对象，使得 DDoS 攻击变得更加频繁与广泛。据统计，2023 年上半年全球共发生 DDoS 攻击约 790 万次，相比于 2022 年上半年增长了 30.5%，范围覆盖到制造、娱乐、医疗、金融等多个行业。

3. 数据安全事件

数据安全事件指通过技术或其他手段对数据实施篡改、假冒、泄露、窃取等威胁行为的网络安全事件，该类事件对政治安全、国家安全及公民隐私都可能造成严重威胁。数据安全事件包括数据篡改事件、数据假冒事件、数据泄露事件、数据窃取事件、数据拦截事件等子类，具体如下：

（1）数据篡改事件：未经授权接触或修改数据。

（2）数据假冒事件：非法或未经许可使用、伪造数据。

（3）数据泄露事件：无意或恶意通过技术手段使数据或敏感个人信息对外公开泄露。

（4）数据窃取事件：未经授权利用技术手段偷窃数据。

（5）数据拦截事件：在数据到达目标接收者之前非法捕获数据。

数据泄露事件是一类典型的数据安全事件，黑客攻击、恶意软件、内部员工操作等都可能导致数据被泄露。2018 年 3 月，美国社交网络服务网站 Facebook 上超过 5000 万用户信息数据被一家名为“剑桥分析（Cambridge Analytica）”的公司泄露。事件发生后，Facebook 股价大跌，市值蒸发超 700 亿美元。无独有偶，一年后 Facebook 再次被曝出泄露丑闻，来自 Facebook 应用程序的两个数据集被暴露在互联网上，这些数据涉及 5.3 亿多 Facebook 用户的隐私信息，包含电话号码、账户名和 Facebook ID 等，造成了极为恶

劣的社会影响。数据泄露不仅仅会威胁到个人隐私与机构利益，甚至已成为影响国家安全的重要因素。据最新统计报告显示，2024 年 1 月在深网与暗网监控到的有效情报共 944,007 份，其中属于泄露数据的高价值买卖情报共 1447 份，包括利比亚选举数据、法国国防部服务器数据等国家级重要数据。

4. 信息内容安全事件

信息内容安全事件指通过网络传播危害国家安全、社会稳定、公共安全和利益的有害信息从而对个人财产、公共安全与社会稳定等构成威胁的网络安全事件，包括反动宣传事件、暴恐宣扬事件、色情传播事件、虚假信息传播事件、网络欺诈事件等子类，具体如下：

（1）反动宣传事件：利用网络传播煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一等危害国家安全、荣誉和利益的非法信息。

（2）暴恐宣扬事件：利用网络宣传恐怖主义、极端主义，煽动民族仇恨、民族歧视的信息，引起社会恐慌和动乱。

（3）色情传播事件：利用网络传播违背社会伦理道德的淫秽色情信息。

（4）虚假信息传播事件：利用网络编造并传播虚假信息来扰乱经济秩序和社会秩序，造成负面影响。

（5）网络欺诈事件：恶意利用技术或非技术手段对特定或不特定目标通过网络进行欺诈以非法获取信息或钱财。

网络诈骗是一类典型的信息内容安全事件，其中电信网络诈骗已成为发案最多、上升最快、涉及面最广的犯罪类型，对公民财产与社会的稳定都造成了极大威胁。根据国家反诈中心的公开资料显示，截至 2022 年年底，公安部门共破获电信网络诈骗案件 115.6 万起，抓获犯罪嫌疑人 155.3 万名，止付冻结涉案资金 9165 亿余元。随着科技的进步，在互联网为人们的工作生活带来便利的同时，网络诈骗方式也在不断更新，封装手机应用、群发邮件“引流”、AI（Artificial Intelligence）语音视频造假诈骗等新型诈骗手法层出不穷。2023 年 4 月，福州市发生了一起利用人工智能技术实施电信诈骗的案件，骗子使用 AI 换脸和语音模拟技术冒充受害者好友，通过微信视频通话的方式向受害者借款，仅花费 10 分钟时间就骗取金额 430 万元。

5. 设备设施故障事件

设备设施故障指由于网络自身出现故障或设备设施受到破坏或干扰而导致网络中断、数据丢失、系统损坏等问题的网络安全事件，包括技术故障事件、配套设施故障事件、物理损害事件与辐射干扰事件等子类，具体如下：

（1）技术故障事件：网络中软硬件的自然缺陷、设计缺陷或运行环境发生变化而引起系统故障，例如：硬件故障、软件故障、过载等。

（2）配套设施故障事件：支撑网络运行的配套设施发生故障，例如：电力供应故障、照明系统故障、温湿度控制系统故障等。

（3）物理损害事件：故意或意外的物理行动造成网络环境或网络设备损坏，例如：失火、漏水、静电设备毁坏或丢失等。

（4）辐射干扰事件：因辐射产生干扰影响网络正常运行，例如：电磁辐射、电磁脉冲、电子干扰、电压波动、热辐射等。

配套设施故障事件是一类常见的设备设施故障事件，配套设施一旦发生故障将直接阻碍网络的正常运行，导致机构业务中断，无法正常为用户提供服务，进而对机构与用户造成巨大影响。2020 年 11 月，欧洲电信运营商沃达丰集团在德国的移动通信网络出现大规模故障，导致用户无法建立语音连接和数据连接，故障持续时间超过 4 个小时，受影响用户达 100 万人。事后沃达丰集团明确表示，该事件发生的原因是部署在慕尼黑、法兰克福与柏林三地的核心网控制设备出现故障，该设备是支撑大规模网络运行的配套设施之一。

6. 违规操作事件

违规操作事件指人为故意或意外地损害网络功能而导致系统功能受损或数据泄露的网络安全事件，包括权限滥用事件、权限伪造事件、行为抵赖事件、故意违规操作事件、误操作事件等子类，具体如下：

（1）权限滥用事件：由于网络服务端功能开放过多或权限限制不严格，导致攻击者通过直接或间接调用权限的方式进行攻击。

（2）权限伪造事件：为了欺骗制造虚假权限。

（3）行为抵赖事件：用户否认其有害行为。

（4）故意违规操作事件：故意执行非法操作。

（5）误操作事件：无意地执行错误操作。

权限滥用事件是机构内常见的违规操作事件，通常由内部员工滥用权限执行非法操作所导致，造成机构核心系统损坏或机密数据泄露。2021 年 1 月，美国路由器厂商 Ubiquiti 遭遇勒索攻击，攻击者窃取了数千兆字节的文件并要求 Ubiquiti 支付 50 枚比特币（按当时汇率约为 190 万美元）作为赎金，勒索未果后在互联网上将部分数据与系统漏洞公开。事后经调查发现，攻击者是一名 Ubiquiti 的前员工，该员工利用内部访问权限从 Ubiquiti 的云服务器下载了一个管理密钥，通过此密钥访问公司基础设施与存储库，从中窃取机密文件，并冒充匿名黑客对公司进行敲诈勒索。此外，该员工还向媒体透露虚假信息，谎称公司将淡化处理此次事件。据统计，该事件直接导致 Ubiquiti 股价下跌约 20%，市值损失超过 40 亿美元。

7. 安全隐患事件

安全隐患事件指网络中出现漏洞或隐患，一旦被攻击者利用可能对网络造成破坏的网络安全事件，包括网络漏洞事件与网络配置合规缺陷事件两类。

（1）网络漏洞事件：因操作系统、应用程序或安全协议开发及设计过程中，对安全性考虑不充分而出现安全隐患。

（2）网络配置合规缺陷事件：由于软硬件安全配置不合理或缺省配置，不符合网络安全要求而产生安全缺陷或隐患。

网络漏洞事件是常见的安全隐患事件，大部分恶意程序与网络攻击事件的攻击者都是利用网络漏洞来实施危害行为。从传统的计算机系统和应用，到人工智能、大数据等新兴技术领域，各种类型的安全漏洞层出不穷。这些漏洞不仅威胁着网络系统的正常运行和数据安全，还可能对国家安全、社会稳定和经济发展产生深远影响。2014 年 4 月 23 日，安全研究人员发现 Apache Struts2 CVE-2014-0094 的漏洞补丁中存在严重缺陷，能够被轻易绕过，可导致应用 Struts 架构的大量互联网服务器遭受 DDoS 攻击、远程服务器控制等致命威胁。在当时该漏洞尚无彻底修复的方法，且由于新闻炒作和漏洞利用代码的大量扩散，我国国内众多政府、门户、电商、金融机构、运营商等机构的大型网站都面临恶意攻击。随着网络安全形势日益复杂与严峻，网络漏洞数量也在逐年增加。根据相关机构统计，2018 年至 2022 年间全球漏洞新增数量逐年上升，仅 2022 年内新增漏洞就高达 24801 个，较 2021 年增加了 19.28%，其中高危级漏洞占比超过 50%，给网络安全防护工作带来了巨大的挑战。

8. 异常行为事件

异常行为事件指网络本身稳定性不足或违规访问网络造成访问、流量等异常行为，进而影响到网络的正常运行或造成社会危害的网络安全事件，主要包括访问异常事件与流量异常事件两类。

（1）访问异常事件：因网络软硬件运行环境发生变化导致不能提供服务。

（2）流量异常事件：网络流量行为模式偏离正常基线。

访问异常事件是机构内常见的异常行为事件。近年来，随着网络环境日益复杂，访问异常事件出现得更加频繁，并且很难通过传统的基于规则的异常检测方法进行预防与检测，对机构的网络系统与关键数据构成极大威胁。AT&T 网络中断事故是一起因内部程序错误而产生的访问异常事件。2024 年 2 月，美国最大的电信运营商 AT&T 出现网络故障，通话、网络和短信服务均无法正常访问与使用。调查显示，造成相关服务中断的原因主要是技术人员在扩展网络时，某个内部应用程序产生错误，破坏了网络的稳定性。据统计，服务中断时间长达 10 个小时，有超过 7 万名用户受到影响，造成损失达 15 亿美元。

9. 不可抗力事件

不可抗力事件指因突发事件损害网络的可用性的网络安全事件，包括自然灾害事件、事故灾难事件、公共卫生事件、社会安全事件等四类，具体如下：

（1）自然灾害事件：大自然的极端现象导致信息和信息系统受损，例如：地震、火山、洪水、暴风、闪电、海啸、崩塌等。

（2）事故灾难事件：具有灾难性后果的事故导致信息和信息系统受损，例如：公共设施和设备事故、环境污染事故等。

（3）公共卫生事件：传染病疫情等导致信息和信息系统受损。

（4）社会安全事件：危害国家和社会的突发性群体性事件导致信息和信息系统受损，例如：恐怖袭击事件等。

自然灾害事件是一类常见的不可抗力事件，通常具有影响面积广、影响程度深、恢复难度高等特点，极易引起大范围的断网停服问题。2021 年 7 月，河南省郑州市遭遇罕见特大暴雨，全市共 3.52 万个基站、556 条光缆受损，使得部分地区信息基础设施停服，互联网长时间中断。在此次事件中，网络的中断导致了郑州市部分公共服务的瘫痪，对群众日常生活造成了极大的不便，也间接增加了灾后救援指挥的难度。随着全球气候日益恶化，自然灾害事件有增多变强的趋势，为关键信息基础设施的防护带来了新的挑战。

10. 其他事件

其他事件指未归为上述分类的网络安全事件。

1.1.3 网络安全是国家安全的重要基石

当前，数字化浪潮奔涌向前，国际力量对比深刻变化，国际环境日趋复杂，不稳定性不确定性明显增加。截至 2022 年，全球已有超过 60 个国家和地区发布国家级网络安全战略，围绕数字技术、数据要素、产业生态、安全标准等的国际竞争日趋激烈。美国、欧盟、俄罗斯、日本等世界主要经济体，都从自身战略角度出发，明确了网络安全的目标和任务，并规划了实施路径。我国高度重视网络安全，在 2014 年的中央网络安全和信息化领导小组（2018 年 3 月，根据中共中央《深化党和国家机构改革方案》，中央网络安全和信息化领导小组改为中央网络安全和信息化委员会）第一次会议中首次将网络安全提升到国家安全的战略高度，要求统筹应对网络安全挑战，维护网络空间的和平、安全、开放、合作。

1. 美国

2003 年 2 月，小布什政府首次针对网络空间制定专门的国家安全战略，发布《网络空间安全国家战略》报告，这标志着美国对网络安全政策独立地位的最终确认。2009 年 5 月，奥巴马政府发布《网络空间政策评估——保障可信和强健的信息和通信基础设施》报告，随后于 2011 年 5 月发布《网络空间国际战略——网络化世界的繁荣、安全和开放》报告，以推动美国在网络相关议题上的国际参与。2018 年 9 月，特朗普政府发布《国家网络战略》报告，强调要对恶意网络行为作出快速反应。

2023 年 3 月，美国发布新版《国家网络安全战略》。战略基于网络空间安全形势严峻、地缘政治博弈加剧、国内政治生态极化、新技术新应用发展倒逼的现实环境，以建立“可防御且富有弹性的数字生态体系”为目标，提出重塑网络安全责任分配、推进进攻性网络行动、加强政府长期投资等变革性举措。战略围绕保卫关键基础设施、打击和摧毁威胁行为体、塑造市场力量以推动安全和弹性网络建设、投资打造富有弹性的未来、建立国际伙伴关系以实现共同目标五大支柱展开。

在保卫关键基础设施方面，提出了制定满足国家安全和公共安全需求的网络安全规则、扩大公私合作、整合各联邦网络安全中心、更新联邦事件响应计划及进程、发展现代化的联邦防御能力的战略目标。

在打击和摧毁威胁行为体方面，提出了统一联邦政府的打击行动、通过公共和私营部门间的业务合作来打击威胁、加快信息通报的速度并扩大情报共享的规模、保护美国境内的基础设施、打击网络犯罪和挫败勒索软件的战略目标。

在塑造市场力量以推动安全和弹性网络建设方面，提出了让管理方对个人数据负责、推动安全物联网设备的发展、勒令不安全软件产品和服务的责任方进行调整、通过联邦补助金及其他激励措施来强化网络安全、利用联邦采购机制来加强问责制度、推进以联邦网络保险为后盾的新机制的战略目标。

在投资打造富有弹性的未来方面，提出了保护互联网的技术基础、重振联邦层面的网络安全研发、为后量子时代做好准备、保护美国未来的清洁能源、支持数字身份生态体系的发展、通过国家战略以充实美国的网络劳动力的战略目标。

在建立国际伙伴关系以实现共同目标方面，提出了建立联盟以打击美国数字生态体系面临的威胁、加强国际合作伙伴的能力、提升美国协助盟友和合作伙伴的能力、建立相关全球规范、保护网络安全相关技术类产品与服务的全球供应链的战略目标。

2. 欧盟

2012 年 3 月 28 日，欧盟委员会发布欧洲网络安全策略报告，确立了部分具体目标，如促进公私部门合作和早期预警，刺激网络、服务和产品安全性的改善，促进全球响应、加强国际合作等。2012 年 5 月，欧洲网络与信息安全局发布《国家网络安全策略——为加强网络空间安全的国家努力设定线路》，提出了欧盟成员国国家网络安全战略应该包含的内容和要素。2013 年 2 月 7 日，欧盟委员会和欧盟外交安全事务高级代表宣布欧盟的网络安全战略，对当前面临的网络安全挑战进行评估，确立了网络安全指导原则，明确了各利益相关方的权利和责任，确定了未来优先战略任务和行动方案。2016 年 7 月 6 日，欧洲议会全体会议通过《欧盟网络与信息系统安全指令》，以加强欧盟各成员国之间在网络与信息安全方面的合作，提高欧盟应对处理网络信息技术故障的能力，提升欧盟打击黑客恶意攻击特别是跨国网络犯罪的力度。

2020 年 12 月 16 日，欧盟委员会发布《欧盟数字十年网络安全战略》，回顾了欧盟在网络安全上面临复杂的威胁环境，并指出欧盟缺乏应对网络威胁的集体意识，重点阐述了欧盟将如何应对网络安全威胁，加强国际合作，确保欧盟在全球开放的互联网空间发挥领导作用。网络主权方面，战略重视网络空间主权，致力于实现技术主权，提高欧盟网络复兴能力；法律规范方面，战略强调法律顶层设计，成立网络安全行动中心，打造联合网络单元；人才培养方面，战略支持多方参与，加强对网络安全人才理论与实践培养的制度和资金保障；国际参与方面，战略深化与合作伙伴和利益攸关方的合作，争夺全球领导力，推动构建全球开放、安全的网络空间。

3. 俄罗斯

2013 年 8 月，俄罗斯联邦政府公布《2020 年前俄罗斯联邦国际信息安全领域国家政策框架》。该文件确定了国际信息安全领域的主要威胁、俄罗斯联邦在国际信息安全领域国家政策的目标、任务及优先方向以及其实现机制。2021 年 7 月，俄罗斯总统普京签署法令，颁布实施新版《俄罗斯联邦国家安全战略》，首次将“信息安全”以单独战略方向列出，突出强调维护信息领域主权，加强网络安全防范，提高信息基础设备安全性，用先进技术如人工智能、量子计算等保障信息安全，优先使用本国技术装备；同时，积极发展信息战力量，预防、侦察和制止信息技术犯罪，建立预测和识别威胁系统，及时消除影响；最后，加强国际合作，建立多方合作平台，共同应对网络威胁和挑战。

围绕使用其他国家的信息技术和电信设备带来的隐患、个人数据与关键信息泄露问题、利用信息和通信技术实施的违法犯罪活动等安全威胁，提出了从新技术与传统安全领域的交叉运用、信息安全与信息安全系统三个维度推进的信息治理方案。基于新技术与传统安全领域的交叉运用，通过推动技术发展和进行使用限制加以指导和规范；围绕信息与信息安全本身，对信息生产、传输、使用、存储和跨境问题与保护加以限制和规范；对于信息安全的系统架构，始终围绕保护国家安全利益角度，以防范敌对国家的攻击和利用为预设目标进行开发和合规要求。

围绕其他国家网络部队针对关键信息基础设施与信息空间的网络攻击和情报活动增加、跨国公司出于政治目的实行信息操纵并危害数据主权安全等安全威胁，对国际关系的考量进行了转变。战略指出，俄罗斯的战略意图已从维护周边战略环境稳定转向制定公平的国际规则，发挥俄罗斯的大国影响力以推进全球信息空间治理。俄罗斯始终从地缘政治出发对美俄关系进行战略考量，战略中明确提出将与中国达成战略伙伴关系，通过上海合作组织等国际组织加强与中国的信息对话与信任。俄罗斯始终强调以联合国安理会为核心，遵守国际法，深化信息领域多边互动与安全合作，共同解决全球和地区问题。

4. 日本

2013 年 6 月 10 日，日本正式发布《网络安全战略》，提出了创建“领先世界的强大而有活力的网络空间”。2014 年 11 月 6 日，日本国会表决通过《网络安全基本法》，规定电力、金融等重要社会基础设施运营商、网络相关企业、地方自治体等有义务配合网络安全相关举措或提供相关情报，此举旨在加强日本政府与民间在网络安全领域的协调和运用，更好应对网络攻击。该法还规定，日本政府将新设以内阁官房长官为首的“网络安全战略本部”，协调各政府部门的网络安全对策，并与日本国家安全保障会议、IT 综合战略本部等其他相关机构加强合作。

2021 年，日本政府发布新版《网络安全战略》，提出了“加强防御、威慑和评估能力，加强相关机构间合作”等要求。战略围绕“复杂的、有组织的网络攻击威胁日益增加，企图破坏关键基础设施的服务、窃取个人信息和知识产权，干扰民主进程”的威胁挑战，遵循“确保信息的自由流通、依法治网、开放性、自律性和多方主体合作”五项原

则，以确保“自由、公平和安全的网络空间”为目标，力图实现“参与整个网络空间，人人享有网络安全”的愿景。战略提出了三项战略目标，包括提高经济和社会活力及可持续发展能力，用网络安全促进数字化转型；实现国家安全、民众安心舒适生活的数字社会；维护国际社会和平稳定，保障日本的国家安全。为实现战略目标，战略制定了相应的行动举措，包括构建企业、政府与学术界联合的产、学、研生态环境，培育和发展国内产业，做好应对供应链风险的准备；推进人才培养和全员知识普及工作；全民参与普及网络意识工作，培养网络安全人才，推动公众网络安全意识提升等。

5. 中国

2014 年 4 月 15 日，总体国家安全观在中央国家安全委员会第一次会议上首次被提出，网络安全被提升到国家安全的战略高度。2016 年 4 月 19 日，网络安全和信息化工作座谈会在北京召开，明确提出“要树立正确的网络安全观”。2016 年 12 月 27 日，国家互联网信息办公室发布《国家网络空间安全战略》。

战略围绕当前网络安全日益严峻的形势，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战，包括危害政治安全的网络渗透、威胁经济安全的网络攻击、侵蚀文化安全的网络有害信息、破坏社会安全的网络恐怖和违法犯罪，以及方兴未艾的网络空间国际竞争等。战略以总体国家安全观为指导，贯彻落实创新、协调、绿色、开放、共享的新发展理念，增强风险意识和危机意识，统筹国内国际两个大局，统筹发展安全两件大事，积极防御、有效应对，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。战略遵循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的原则，明确制定了中国的网络安全战略任务，包括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等九个方面。

（1）在坚定捍卫网络空间主权方面，依据宪法和法律，采取各种措施保护国家网络空间主权，反对任何网络颠覆行为。

（2）在坚决维护国家安全方面，防范和惩治利用网络进行叛国、分裂国家等行为，保护国家秘密，抵御境外网络渗透和破坏活动。

（3）在保护关键信息基础设施方面，建立实施关键信息基础设施保护制度，依法综合施策，加强风险评估，建立政府、企业与行业的信息共享机制，建立实施网络安全审查制度，加强供应链安全管理。

（4）在加强网络文化建设方面，大力培育和践行社会主义核心价值观，推广优秀文化，加强网络伦理和文明建设，打击网络有害信息。

（5）在打击网络恐怖和违法犯罪方面，加强网络反恐、反间谍、反窃密能力建设，严厉打击各类网络犯罪行为。

（6）在完善网络治理体系方面，坚持依法、公开、透明管网治网，健全网络安全法律

法规体系，加快构建法律规范、行政监管、行业自律、技术保障、公众监督、社会教育相结合的网络治理体系，保护网络合法权益。

（7）在夯实网络安全基础方面，坚持创新驱动发展，加快核心技术突破，大力发展网络经济，实施国家大数据战略，建立完善国家网络安全技术支撑体系，加强网络安全教育和人才培养。

（8）在提升网络空间防护能力方面，建设与我国国际地位相称、与网络强国相适应的网络空间防护力量，大力发展网络安全防御手段，及时发现和抵御网络威胁。

（9）在强化网络空间国际合作方面，加强国际网络空间对话合作，支持联合国发挥主导作用，推动全球互联网治理体系变革，助力发展中国家和落后地区互联网技术发展，共同构建和平、安全、开放、合作、有序的网络空间。

1.2 网络安全建设与运营相关法律法规

互联网在促进经济社会发展的同时，也对监管和治理形成巨大挑战。发展好治理好互联网，让互联网更好造福人类，是世界各国共同的追求。实践证明，法治是互联网治理的基本方式。运用法治观念、法治思维和法治手段推动互联网发展治理，已经成为全球普遍共识。据统计已有 90 多个国家制定了网络安全专门的法律法规。美国颁布了《网络安全法》《网络安全信息共享法》《关键基础设施网络事件报告法》等法律，欧盟颁布了《网络与信息系统安全指令》《通用数据保护条例》等法律，俄罗斯颁布了《信息、信息技术和信息保护法》《俄罗斯联邦关键信息基础设施安全法》等法律。

我国高度重视网络安全立法，党的十八大以来，网络安全立法进程明显加快，在网络安全、关键信息基础设施安全、数据安全、个人信息保护等领域出台了一系列法律法规和部门规章。本节主要从机构网络安全建设与运营的角度对我国网络安全主要法律法规和部门规章进行梳理。

1.2.1 国家法律

1.《中华人民共和国网络安全法》

《中华人民共和国网络安全法》（以下简称《网络安全法》）自 2017 年 6 月 1 日起施行。这是我国第一部全面规范网络空间安全的基础性法律。

《网络安全法》在第三章中明确规定了网络运行安全要求，提出国家实行网络安全等级保护制度，并对网络运营者应当履行的网络安全保护义务进行了规定。同时，关键信息基础设施作为网络安全的重中之重，《网络安全法》强调在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护。

机构在进行网络安全建设与运营时，首先需要落实网络安全保护责任，制定内部安

全管理制度和操作规程，确定网络安全负责人；其次，采取防范处置计算机病毒、网络攻击、网络侵入等危害网络安全行为的措施和数据分类、重要数据备份、加密等数据安全防护的措施，并监测、记录网络运行状态、网络安全事件，留存相关的网络日志不少于六个月；最后，还应当制定网络安全事件应急预案，在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

运营关键信息基础设施的机构，还应当在落实上述一般规定的基础上，设置专门安全管理机构和安全管理负责人，落实人员教育培训、容灾备份、应急演练、风险评估等重点保护措施；在采购网络产品和服务时，落实网络安全审查、签订保密协议等要求；在数据出境前，进行安全评估。

2.《中华人民共和国密码法》

《中华人民共和国密码法》（以下简称《密码法》）自 2020 年 1 月 1 日起施行。《密码法》是我国密码领域的综合性、基础性法律，对全面提升密码工作法治化水平起到关键性作用。

《密码法》规定，我国密码分为核心密码、普通密码和商用密码。核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

密码作为保障网络安全的核心技术，机构在规划、采取各项网络安全技术措施时，应考虑采用密码技术，特别是承担关键信息基础设施运营者角色的机构，应当对关键信息基础设施使用商用密码进行保护，并自行或委托开展商用密码应用安全性评估。在此过程中，如果涉及商用密码产品和服务采购的，还应当落实网络安全审查要求。

3.《中华人民共和国数据安全法》

《中华人民共和国数据安全法》（以下简称《数据安全法》）自 2021 年 9 月 1 日起施行。作为数据安全领域的基础性法律和国家安全法律体系的重要组成，《数据安全法》是护航数字经济发展的重要举措。

《数据安全法》明确国家建立数据分类分级保护制度和数据安全审查制度，以及数据安全风险评估、报告、信息共享、监测预警机制和数据安全应急处置机制等。

落实《数据安全法》的规定，机构应当按照地区、行业数据分类分级要求，对本机构数据进行分类分级，建立重要数据目录。开展数据处理活动，应当建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。处理重要数据的机构，还应当明确数据安全负责人和管理机构。

机构在开展数据处理活动时，应当加强数据安全风险监测，及时对安全缺陷、漏洞等采取补救措施；及时处置数据安全事件，并履行相应的报告义务。处理重要数据的机构，还应当对其数据处理活动定期开展风险评估；重要数据出境时，应当进行安全评估。

4.《中华人民共和国个人信息保护法》

《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）自 2021 年 11 月

1 日起施行。《个人信息保护法》在有关法律的基础上，进一步细化完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作体制机制。

《个人信息保护法》强调处理个人信息应当遵循合法、正当、必要和诚信原则；应当具有明确、合理的目的；应当遵循公开、透明的原则；应当保证个人信息的质量；应当采取必要措施保障所处理的个人信息的安全。

机构在处理个人信息前，应当在事先充分告知的前提下取得个人同意，处理敏感个人信息，应当取得个人的单独同意或者书面同意。在处理个人信息时，应当履行下列义务：

（1）制定内部管理制度和操作规程，对个人信息实行分类管理，采取相应的安全技术措施。

（2）合理确定个人信息处理的操作权限，定期对从业人员进行安全教育和培训，定期对个人信息处理活动进行合规审计。

（3）对处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息及其他对个人权益有重大影响的个人信息处理活动事前进行个人信息保护影响评估。

（4）制定并组织实施个人信息安全事件应急预案，履行个人信息泄露通知和补救义务等。

1.2.2 行政法规

1.《中华人民共和国计算机信息系统安全保护条例》

《中华人民共和国计算机信息系统安全保护条例》（以下简称《信息系统保护条例》）于 1994 年发布，并于 2011 年修订。《信息系统保护条例》是我国首部关于网络安全的行政法规，是网络安全保护的法律基础。

《信息系统保护条例》规定计算机信息系统实行安全等级保护。机构在建设和应用计算机信息系统时，应当确保机房符合国家标准和国家有关规定；对国际联网的计算机信息系统进行备案，运输、携带、邮寄计算机信息媒体出入境时，如实向海关申报。应当建立健全安全管理制度，负责本机构计算机信息系统的安全保护工作，计算机信息系统中发生的案件，应在 24 小时内报告公安机关。

2.《关键信息基础设施安全保护条例》

《关键信息基础设施安全保护条例》（以下简称《关保条例》）自 2021 年 9 月 1 日起施行。《关保条例》是我国首部专门针对关键信息基础设施安全保护的行政法规，明确关键信息基础设施安全保护中各个责任主体及其责任义务，为开展关键信息基础设施安全保护工作提供了基本遵循。

《关保条例》对《网络安全法》中关键信息基础设施运营者的责任义务进一步细化。

机构是关键信息基础设施运营者的，应当对关键信息基础设施实行“一把手负责制”，明确机构主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题，保障人力、财力、物力投入，同步规划、同步建设、同步使用关键信息基础设施安全保护措施。

为落实相关责任义务，机构应当设置专门安全管理机构，具体负责本机构的关键信息基础设施安全保护工作，并参与本机构网络安全和信息化有关的决策。机构应当保障专门安全管理机构的运行经费、配备相应的人员，对专门安全管理机构负责人和关键岗位人员进行安全背景审查。

机构应当对关键信息基础设施每年至少进行一次网络安全检测和风险评估；应当优先采购安全可信的网络产品和服务，并与提供者签订安全保密协议，可能影响国家安全的，应当按规定通过网络安全审查；当关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，应当按规定向保护工作部门、公安机关报告。当机构发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置。

3.《商用密码管理条例》

2023 年 7 月 1 日，新修订的《商用密码管理条例》（以下简称《商密条例》）正式施行。《商密条例》全面落实《密码法》要求，规范商用密码应用和管理，为推进新时代商用密码高质量发展、保障网络与信息安全、维护国家安全和社会公共利益、保护公民合法权益提供了有力法治保障。

《商密条例》对关键信息基础设施商用密码应用进行了更为具体的规定。机构是关键信息基础设施运营者的，应当制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运营商用密码保障系统，自行或者委托开展商用密码应用安全性评估，通过商用密码应用安全性评估后，关键信息基础设施方可投入运行，并在运行后每年至少进行一次评估。

关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当依法通过网络安全审查。

1.2.3　部门规章

1.《国家政务信息化项目建设管理办法》

2019 年 12 月 30 日，国务院办公厅印发《国家政务信息化项目建设管理办法》，从规划和审批管理、建设和资金管理、监督管理等方面对国家政务信息化项目网络安全要求进行了规定。

机构在进行项目（本节中项目特指国家政务信息化项目）备案时，备案文件中应当包括等级保护或者分级保护备案情况、密码应用方案和密码应用安全性评估报告等内容。

机构在进行项目建设时，应当建立网络安全管理制度，采取技术措施，加强政务信息系统与信息资源的安全保密设施建设，定期开展网络安全检测与风险评估，保障信息系统安全稳定运行；应当同步规划、同步建设、同步运行密码保障系统并定期进行评估；应当采用安全可靠的软硬件产品。

机构在申请项目验收时，应当提交项目安全风险评估报告（包括涉密信息系统安全保密测评报告或者非涉密信息系统网络安全等级保护测评报告等）、密码应用安全性评估报告等材料。对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，国家将不安排运行维护经费，机构也不得新建、改建、扩建政务信息系统。

机构在系统投入运行后，应当构建全方位、多层次、一致性的防护体系，按要求采用密码技术，并定期开展密码应用安全性评估，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。

2.《网络安全审查办法》

《网络安全法》《数据安全法》《关保条例》等均明确，关键信息基础设施运营者采购网络安全产品和服务，可能影响国家安全的，应当通过网络安全审查。为落实相关法律法规要求，指导机构开展网络安全审查，2022 年 2 月 15 日，由国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部等十三部门联合修订的《网络安全审查办法》正式施行。

除规定关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当进行网络安全审查外，《网络安全审查办法》还规定，掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须申报网络安全审查。

机构在申报网络安全审查前，应当准备以下材料：

（1）申报书。

（2）关于影响或者可能影响国家安全的分析报告。

（3）采购文件、协议、拟签订的合同或者拟提交的首次公开募股（IPO）等上市申请文件。

（4）网络安全审查工作需要的其他材料。

3.《数据出境安全评估办法》

为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，根据《网络安全法》《数据安全法》《个人信息保护法》等法律法规，国家互联网信息办公室制定《数据出境安全评估办法》，自 2022 年 9 月 1 日起施行。

机构向境外提供在我国境内运营中收集和产生的重要数据和个人信息前，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估，具体情形包括：

（1）向境外提供重要数据。

（2）运营关键信息基础设施或处理 100 万人以上个人信息的机构向境外提供个人

信息。

（3）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的机构向境外提供个人信息。

（4）国家网信部门规定的其他需要申报数据出境安全评估的情形。

按照申报数据出境安全评估应当提交的材料要求，机构在数据出境前应当进行数据出境风险自评估，并与境外接收方拟订数据出境相关合同或者其他具有法律效力的文件。

4.《商用密码应用安全性评估管理办法》

根据《密码法》《商密条例》等法律法规，国家密码管理局研究制定了《商用密码应用安全性评估管理办法》（以下简称《密评办法》），自 2023 年 11 月 1 日起施行。《密评办法》进一步细化落实“三同步一评估”要求，对依法应当使用商用密码进行保护的重要网络与信息系统，明确要求同步规划、同步建设、同步运营商用密码保障系统，并定期进行商用密码应用安全性评估。

重要网络与信息系统在规划阶段，机构应当制定商用密码应用方案，规划商用密码保障系统，并对商用密码应用方案进行商用密码应用安全性评估。商用密码应用方案未通过商用密码应用安全性评估的，不得作为商用密码保障系统的建设依据。

重要网络与信息系统建设阶段，机构应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。

重要网络与信息系统运行前，机构应当对网络与信息系统开展商用密码应用安全性评估。网络与信息系统未通过商用密码应用安全性评估的，机构应当进行改造，改造期间不得投入运行。

重要网络与信息系统建成运行后，机构应当每年至少开展一次商用密码应用安全性评估，确保商用密码保障系统正确有效运行。未通过商用密码应用安全性评估的，机构应当进行改造，并在改造期间采取必要措施保证网络与信息系统运行安全。

1.3　网络安全建设与运营相关标准规范

标准是经济活动和社会发展的技术支撑，是国家基础性制度的重要方面。标准化在推进国家治理体系和治理能力现代化中发挥着基础性、引领性作用。网络安全相关标准为网络安全产品和系统在设计、研发、生产、建设、使用、测评等环节提供了统一一致、先进可靠等技术规范，对促进网络安全产业发展和机构网络安全能力提升发挥了基础性、引领性作用。目前，网络安全相关标准化组织主要有国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（ITU）、国际互联网工程任务组（IETF），以及国内的全国网络安全标准化技术委员会、密码行业标准化技术委员会等。

1.3.1 主要网络安全标准化组织

1. 国际化的标准组织

（1）国际标准化组织和国际电工委员会

国际标准化组织（ISO）成立于 1947 年，是标准化领域中的一个国际性非政府组织，其宗旨是在世界上促进标准化及其有关活动的发展，以便于国际物资交流和服务，并扩大在知识、科学、技术和经济领域中的合作，主要任务包括协调世界范围内的标准化工作、制定和发布国际标准并采取措施以便在世界范围内实施、组织各成员国和技术委员会进行信息交流、与其他国际组织共同开展有关标准化课题的研究等。

国际电工委员会（IEC）成立于 1906 年，是世界上成立最早的国际性电工标准化机构，负责制定电工电子及相关领域的国际标准和合格评定程序，在便利国际贸易和推动产业发展中发挥着举足轻重的作用。

ISO 和 IEC 关系密切，根据分工，IEC 负责电工电子领域的国际标准化工作，其他领域则由 ISO 负责。1987 年，ISO 和 IEC 成立第一个联合技术委员会——信息技术委员会，编号为 JTC 1，承担信息技术领域国际标准制定工作。

SC27 是 ISO/IEC JTC 1 下设专门负责网络安全领域标准化工作的分技术委员会，具体负责开展信息安全、网络安全和隐私保护领域的国际标准研制工作。SC27 秘书处设在德国标准化协会（DIN）。全国网络安全标准化技术委员会承担 SC27 国内技术业务工作，负责统筹协调和组织参加网络安全领域国际标准化活动。

目前，SC27 直属管理包括 WG1（信息安全管理体系）、WG2（密码与安全机制）、WG3（安全评估、测试和规范）、WG4（安全控制与服务）、WG5（身份管理和隐私保护技术）等在内的 5 个工作组。同时，SC27 还成立两个联合工作组 JWG4（区块链和 DLT 的安全、隐私和身份）、JWG6（网联汽车设备网络安全要求及评估活动）。

除 ISO/IEC JTC 1 外，IEC 还成立 TC56、TC74 等技术委员会制定网络安全相关标准。

（2）国际电信联盟电信标准化部门

国际电信联盟电信标准化部门（ITU-T）的第 17 研究组（SG17）专注于增强信息通信技术（ICT）的安全，旨在使网络基础设施、业务和应用更加安全。SG17 负责协调 ITU-T 所有研究组涉及安全的工作，并与其他外部标准化组织、ICT 行业联合体合作处理标准化相关问题。

SG17 主要工作领域包括网络安全、安全管理、安全架构与框架、打击垃圾信息、身份管理、个人标识信息保护、数据保护操作、开放身份信任框架、基于量子技术的安全措施以及儿童上网保护等。

SG17 的重要成果包括 ITU-T X.509 建议书，用于公共网络上的电子认证，是设计公钥基础设施（PKI）相关应用的基石。ITU-T X.1500 CYBEX，提供了一套用于交换网络安全信息的最佳标准组合，帮助防范网络攻击。ITU-T X.805 建议书，为电信网络运营商和

企业从安全角度提供端到端的架构描述。

（3）国际互联网工程任务组

国际互联网工程任务组（IETF）成立于 1986 年，是最具权威的互联网技术标准化组织，当前绝大多数国际互联网相关技术标准出自 IETF。IETF 将其技术文档作为请求注解文档（RFC）发布。在互联网安全方面，IETF 发布了传输层安全协议（TLS）、互联网密钥交换协议（IKE）、网络层安全协议簇（IPsec）、PKI 等一系列安全协议相关的 RFC。

2. 我国的标准化组织

（1）全国网络安全标准化技术委员会

为充分发挥企业、科研机构、检测机构、高等院校、政府部门、用户等方面专家的作用，引导产学研用各方面共同推进网络安全标准化工作，经国家标准化管理委员会批准，全国信息安全标准化技术委员会（编号为 TC260，以下简称信安标委）于 2002 年 4 月 15 日在北京正式成立。信安标委是在信息安全技术专业领域内，从事信息安全标准化工作的技术工作组织，负责组织开展国内信息安全有关的标准化技术工作，对信息安全国家标准进行统一技术归口，统一组织申报、送审和报批，具体工作范围包括：安全技术、安全机制、安全服务、安全管理、安全评估等领域的标准化技术工作。信安标委业务上受中央网络安全和信息化委员会办公室指导。

2024 年 2 月，信安标委更名为全国网络安全标准化技术委员会（以下简称网安标委），进一步突出了网络空间安全的概念。根据《关于印发全国网络安全标准化技术委员会工作组设置的通知》，目前，网安标委下设 8 个工作组和 1 个特别工作组，组织结构如图 1-1 所示。

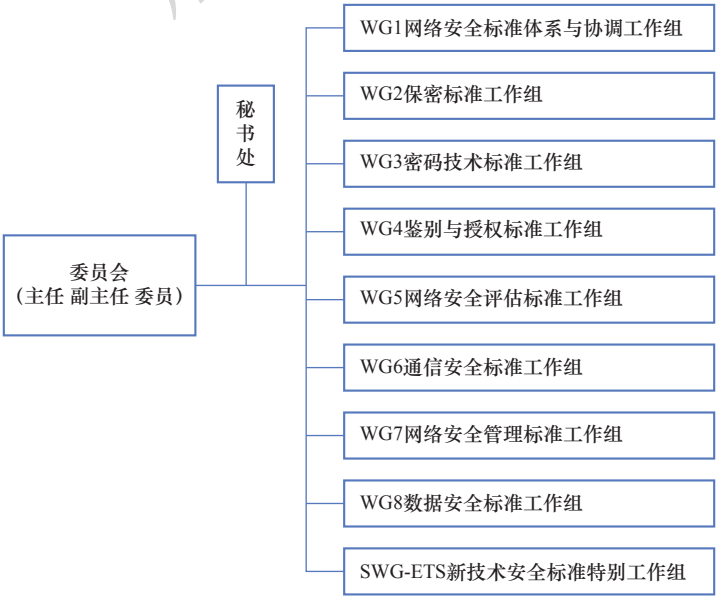

图 1-1　网安标委组织结构图

（2）密码行业标准化技术委员会

为满足密码领域标准化发展需求，充分发挥密码科研、生产、使用、教学和监督检验等方面专家作用，更好地开展密码领域的标准化工作，2011 年 10 月，经国家标准化管理委员会和国家密码管理局批准，成立密码行业标准化技术委员会（以下简称密标委）。

密标委是在密码领域内从事密码标准化工作的非法人技术组织，由国家密码管理局领导和管理，主要从事密码技术、产品、系统和管理等方面的标准化工作。密标委委员由政府、企业、科研院所、高等院校、检测机构和行业协会等有关方面的专家组成。密标委目前下设秘书处和总体、基础、应用、测评四个工作组。

1.3.2 主要国际标准

1. ISO/IEC 27000 标准族

ISO/IEC 27000 标准族是一组信息安全管理体系（ISMS）标准的总称，是系统化管理思维在网络安全领域的应用。目前，ISO/IEC 27000 标准族已发布或正在研制中的标准超过 90 项。以下主要介绍 27001-27005 等 5 个标准：

（1）ISO/IEC 27001：是 ISMS 的核心标准，规定了机构应如何建立、实施、维护和持续改进其 ISMS。

（2）ISO/IEC 27002：包含一系列的控制目标和建议性控制措施，提供了关于网络安全的最佳实践准则。该标准用于帮助机构设计和实现 ISO/IEC 27001 中的要求，机构可以根据自身的需要和情况选择性地采用其中的建议。

（3）ISO/IEC 27003：提供了实施 ISO/IEC 27001 的指南，机构可以参考该标准规划、执行并持续改进其 ISMS。

（4）ISO/IEC 27004：提供了评估和度量 ISMS 的方法、指标等，机构可以通过该标准提供的量化方法来评估和持续改进其 ISMS。

（5）ISO/IEC 27005：提供了网络安全风险评估的指南，该标准可以帮助机构识别、评估和管理网络安全风险。

2022 年 10 月，新版 ISO/IEC 27001 发布，机构一方面可参考该标准建立机构内部的网络安全管理体系，另一方面可以选择经认可的第三方认证机构，进行审核认证，以确保其网络安全管理体系符合 ISO 27000 标准，获得认证证书，从而提高机构在行业、合作伙伴、客户中的信任度和声誉。

2.《信息技术安全评估通用准则》

《信息技术安全评估通用准则》（简称 CC 标准）是评估信息技术产品和系统安全性的国际通用准则，是信息技术安全性评估结果国际互认的基础。

CC 标准是 ISO 在美国和欧洲等国分别自行推出并实践测评准则及标准的基础上，通过相互间的总结和互补发展起来的。1985 年，美国国防部公布《可信计算机系统评估准则》（TCSEC）即橘皮书，1991 年法、英、荷、德等 4 国公布《信息技术安全评估准则》

（ITSEC），1993 年，加拿大公布《加拿大可信计算机产品评估准则》（CTCPEC），同年，美国公布《美国信息技术安全联邦准则》（FC）。1996 年，TCSEC、ITSEC、CTCPEC、FC 标准涉及的 6 个国家联合发布《信息技术安全性评估通用准则》（CC）的 1.0 版本，1998 年，发布 CC 标准 2.0 版本。1999 年 12 月，ISO 接受 CC 2.0 版本为 ISO/IEC 15408 标准，并正式发布。2022 年 11 月，ISO/IEC 15408 的第四个版本发布。

我国参考 TCSEC 于 1999 年发布《计算机信息系统 安全保护等级划分准则》（GB 17859—1999），等同采用 ISO/IEC 15408 标准发布《网络安全技术 信息技术安全评估准则》（GB/T 18336—2024）。

CC 标准定义了安全功能要求（SFR）和安全保证要求（SAR）两类要求，SFR 是信息技术产品和系统具备的安全功能，SAR 是为保证安全功能实现的正确性所需要的活动。同时，CC 标准预定义了 7 个保障等级，从 EAL1 到 EAL7，数字越大代表级别越高。

机构可以依据 CC 标准中保护配置文件（PP）指定的 SFR 和 SAR，实施和声明其信息产品和系统的安全属性，并通过第三方认证机构的评估，从而获得 CC 等级认证。

1.3.3　我国主要标准

1. 网络安全等级保护标准

为了配合《网络安全法》的实施和落地，指导机构按照网络安全等级保护制度的新要求，履行网络安全保护义务。2018 年以来，国家相继完成《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449—2018）、《信息安全技术 网络安全等级保护安全管理中心技术要求》（GB/T 36958—2018）、《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》（GB/T 36959—2018）、《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627—2018）、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239—2019）、《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070—2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）、《信息安全技术 网络安全等级保护定级指南》（GB/T 22240—2020）、《信息安全技术 网络安全等级保护实施指南》（GB/T 25058—2019）等标准的编制/修订和发布，构成了等级保护 2.0 标准体系。

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058—2019）规定，等级保护的基本流程包括等级保护对象定级与备案阶段、总体安全规划阶段、安全设计与实施阶段、安全运行与维护阶段和定级对象终止阶段。

对于一个机构而言，在等级保护对象定级与备案阶段，首先通过收集分析等级保护对象的有关信息，整理确定等级保护对象的业务及服务范围，合理划分确定定级对象。然后，依据行业/领域定级指导意见等有关文件要求和《信息安全技术 网络安全等级保护定级指南》（GB/T 22240—2020），确定定级对象的安全保护等级，形成定级报告，并组织进行专家评审，报主管部门审核。最后，整理相关备案材料，将定级结果提交公安机关进行备案审核。

完成等级保护对象定级与备案后，机构需要按照等级保护对象的定级等级，对照《信

息安全技术 网络安全等级保护基本要求》（GB/T 22239—2019）中相应等级的保护要求，确定等级保护对象安全需求，设计合理的、满足等级保护要求的总体安全方案，并制定出安全实施计划，以指导后续等级保护对象安全建设工程实施。

完成等级保护对象总体安全规划后，机构需要进行安全方案详细设计，并通过建设项目实施落地。在进行安全方案详细设计时，机构可参考《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070—2019）进行技术措施设计，结合等级保护对象实际安全管理需要和技术建设内容，确定管理措施建设的范围和内容。

完成等级保护对象安全建设实施后，以及在运行与维护阶段，机构应按规定定期开展网络安全等级保护测评，确保等级保护对象的安全保护措施符合相应等级的安全要求。机构可参考《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）进行对照检查，可参考《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449—2018）对第三方测评机构的工作进行要求和评价。

2. 关键信息基础设施安全保护标准

《网络安全法》和《关保条例》均明确，关键信息基础设施在网络安全等级保护的基础上，实行重点保护。因此，有必要在网络安全等级保护系列标准的基础上，提出关键信息基础设施安全保护要求。2023 年 5 月 1 日，《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204—2022）正式实施。《关键信息基础设施边界确定方法》等相关标准正在编制中。

对于机构是关键信息基础设施运营者的，需要落实网络安全等级保护制度相关要求，从安全管理制度、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、供应链安全保护、数据安全防护等方面进行安全防护，落实事件处置制度、应急预案和演练、响应和处置、重新识别等要求，加强分析识别、检测评估、监测预警、主动防御等方面的建设。

一是围绕关键信息基础设施承载的关键业务，开展关键业务对外部业务的依赖性、重要性识别，梳理关键业务链。建立关键业务链相关的网络、系统、数据、服务和其他类资产的资产清单，确定资产防护的优先级。对关键业务链开展安全风险分析，识别关键业务链各环节的威胁性、脆弱性，确定风险处置优先级。

二是每年至少进行一次对关键信息基础设施安全性和可能存在风险的检测评估。应针对特定的业务系统或系统资产，采取模拟网络攻击方式，检测关键信息基础设施在面对实际网络攻击时的防护和响应能力。

三是建立并落实常态化检测预警、快速响应机制。对网络边界、网络出入口等关键节点和关键业务所涉及的系统进行监测，并采用自动化措施对不同来源、不同区域的各类信息进行关联、整合，分析整体安全态势。当发现可能危害关键业务的迹象时，进行自动报警，并自动采取相应措施。在综合分析、研判后，必要时生成内部预警信息。

四是通过采取收敛暴露面、发现阻断、攻防演练、威胁情报等主动措施，有效提升对网络威胁与攻击的识别、分析、处置等防御能力。

3. 商用密码标准

截至目前，密标委已发布商用密码相关标准 100 多项，从技术角度归类，可分为密码基础类、密码产品类、基础设施类、应用支撑类、密码应用类、密码管理类和检测认证类，如图 1-2 所示。

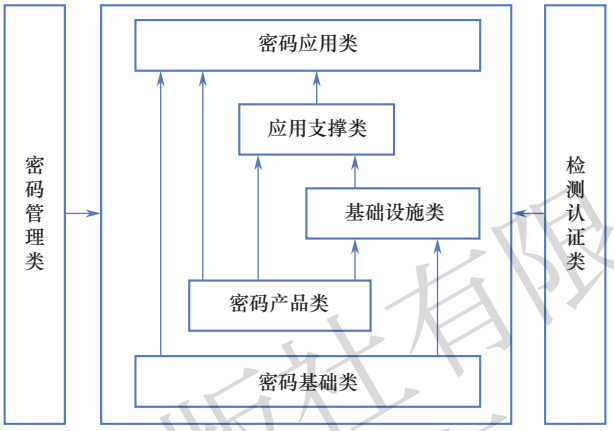

图 1-2　商用密码标准体系框架

机构在进行网络安全建设时，应将密码技术作为重要的措施之一，采用商用密码进行防护。目前，我国已制定发布 SM1、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法（ZUC）等商用密码算法。其中 SM1、SM4、SM7、ZUC 是对称算法；SM2、SM9 是非对称算法；SM3 是哈希算法。我国商用密码算法与国外密码算法对应关系如图 1-3 所示。

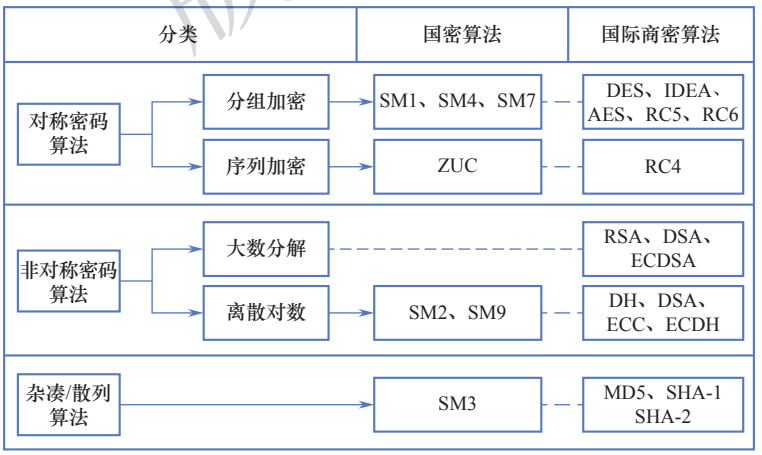

图 1-3　SM 系列密码分类及与国际商密算法对应关系

在进行商用密码建设时，机构应遵循国家标准《信息安全技术 信息系统密码应用基本要求》（GB/T 39786—2021）进行规划、设计、建设，确保合规、正确、有效应用密码。

首先，机构应按照业务实际情况确定相应级别的密码保障能力，然后，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个方面进行密码技术保障

能力建设，从管理制度、人员管理、建设运行、应急处置等四个方面进行密码管理保障能力建设。

此外，机构也可参考《信息安全技术 信息系统密码应用测评要求》（GB/T 43206—2023）、《信息系统密码应用测评过程指南》（GM/T 0116—2021）等标准，及中国密码学会密评联委会组织制定的《信息系统密码应用高风险判定指引》《商用密码应用安全性评估 FAQ（第三版）》《商用密码应用安全性评估量化评估规则（2023 版）》《商用密码应用安全性评估报告模板（2023 版）》《政务领域政务服务平台密码应用与安全性评估实施指南》《政务领域政务云密码应用与安全性评估实施指南》等指导性文件，更好地理解和掌握商用密码应用要求。

1.4 网络安全架构

网络安全架构通常包含拓扑结构、安全边界、访问控制策略、安全传输协议等部分，旨在帮助机构了解与管理面临的网络安全风险，保护机构的网络系统不受恶意攻击或故障影响，同时防止机构的关键信息资产损失或泄露。网络安全架构的规划与部署直接影响网络整体安全防护的效果。

本节综合考虑安全架构的实用性、独特性、知名度等因素，挑选国内外常见的 10 个网络安全架构，按照提出的时间顺序依次介绍各网络安全架构的组成要素及主要功能与特点，并详细阐述我国网络安全保护体系架构的具体内容，提出由网络安全管理体系、网络安全技术体系、网络安全运营体系、网络安全保障体系组成的网络安全建设与运营架构，简要介绍各体系的内容以及体系间的关系。

1.4.1 常见网络安全架构

1. COSO 内部控制框架

美国反欺诈财务报告委员会下属的发起人委员会（The Committee of Sponsoring Organizations of the Treadway Commission, COSO）于 1992 年首次提出 COSO 内部控制框架，并于 2013 年推出最新版本。COSO 内部控制框架具有全面性、有效性和普遍性等特点，长期以来一直作为建立旨在提高效率、降低风险、帮助保证财务状况报表可信性、遵从法律法规的内部控制框架的蓝本，在全球范围内得到了广泛的应用。

COSO 内部控制框架用以描述机构的内部控制系统，框架的三维模型图如图 1-4 所示。模型的侧面表示机构内部的组织结构，包括机构层面、分支机构、业务单元、职能部门；模型的顶部表示内部控制的三类目标：运营、报告、合规；模型的正前方表示内部控制的五个关键要素：控制环境、风险评估、控制活动、信息与沟通、监控活动。各要素具体内容如下：

（1）控制环境

控制环境是所有其他组成要素的基础，具体包括以下内容。

① 诚信和道德价值观

② 致力于提高员工工作能力及促进员工职业发展的承诺

③ 董事会和审计委员会

④ 管理层的理念和经营风格

⑤ 组织结构，包括定义授权和责任的关键领域以及建立适当的报告流程

⑥ 权限及职责分配

⑦ 人力资源政策及程序

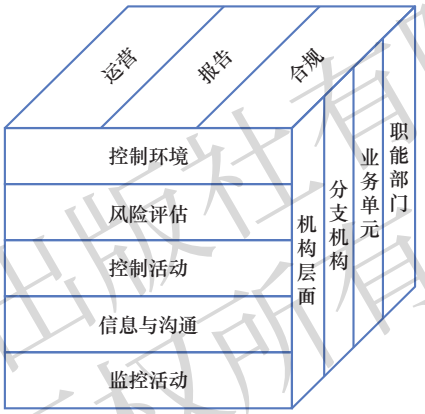

图 1-4　COSO 内部控制框架的三维模型图

（2）风险评估

风险评估具体包括以下步骤。

① 设立目标

② 识别与上述目标相关的风险

③ 评估上述被识别风险的后果和可能性

④ 根据风险评估的结果，考虑采取适当的控制行动

（3）控制活动

控制活动指为确保管理层指示得以执行而削弱风险的政策和程序，有助于相关人员采取必要措施来管理风险，以实现机构目标。控制活动贯穿于机构的所有层次和部门，包括一系列不同的活动，如批准、授权、查证、核对、复核经营业绩、资产保护以及职责分工等。

（4）信息与沟通

信息系统不仅处理内部资料，而且还处理形成机构决策和外部报告所必须的外部事件、行为和条件的信息。有效的交流应涉及机构的各个方面。所有机构人员都要从高级管理层获得明确的信息，了解各自在内部控制框架中的作用，以及个人的行为如何与其他人的工作建立联系。此外，还应与顾客、供应商、监管者和股东等机构外部人员保持长期有效的沟通。

（5）监控活动

评估系统在一定时期内运行质量的过程。这一过程通过持续的监控与独立的评估来实现。持续的监控行为发生在经营的过程中，包括日常管理和监管行为。独立评估的范围和频率主要依赖于风险评估和持续监控程序的有效性。内部控制的缺陷应自下而上进行报告，重要事项应报知高层管理人员和董事会。

2. 舍伍德商业应用安全架构

舍伍德商业应用安全架构（Sherwood Applied Business Security Architecture, SABSA）是一个基于风险和机会的业务驱动企业安全框架，于 1996 年被首次提出。在该架构提出前，大多数安全方案都具有单点特性，即只针对特定问题构建方案，而忽视企业、组织宏观业务需求，同时忽略与其他安全方案的整合与协同。为了弥补这一缺陷，需要开发一个以业务为驱动的企业安全体系结构，以描述技术方案和过程方案之间的结构化联系，进一步满足业务的长期需求。

SABSA 遵循 Zachman 架构的设计，由六个层次（五个水平面和一个垂直面）组成。五个水平层次由上到下，代表了从机构业务目标和相关背景，到安全实践落地的上下级级联设计思路，如图 1-5 所示。

图 1-5　Zachman 架构模型

（1）安全背景架构—业务视图：从机构业务规划和决策角度，为安全建设提供输入。

（2）安全概念架构—架构师视图：架构师在概念层面设计架构，满足机构业务需求。本层采用宽泛的描述，定义原则和基本概念，指导在较低的抽象层选择和组织逻辑和物理元素。

（3）逻辑安全架构—设计师视图：根据上层描述，通过工程化可实现方式，在逻辑层面进行转述和表达，定义主要的体系结构安全元素，并描述控制的逻辑流程以及逻辑元素

之间的关系。

（4）物理安全架构—建造者视图：设计者将开发过程移交给建造者。建造者采用逻辑描述和图形的形式，将其转换为可用于构建系统的技术组件。

（5）组件安全架构—技术人员视角：技术人员将技术组件按照各组件功能与上层的设计逻辑进行组合。

（6）安全服务管理架构—管理者视角：管理架构的设计交付及架构提供的各种服务，使架构处于良好状态，监视架构在满足要求方面的执行情况并将情况报告给高级管理层。管理架构与所有其他体系结构层相关，在结构上与每一层相连。

SABSA 是一套信息系统安全架构框架，以业务视角作为起点，从 6 个层面提供了机构信息系统安全架构的完整解决方案，总结了信息化或业务建设中各层面需求，并进行归类和列举。SABSA 的最新版本更新于 2018 年，各层的关键元素如表 1-1 所示。

表 1-1　SABSA 各层关键元素

	资产	动机	过程	人	地点	时间
背景层	业务目标与决策	业务风险	业务元过程	业务治理	业务地理布局	业务时间依赖性
概念层	业务价值与知识战略	风险管理策略与目标	过程保证策略	安全实体模型与信任框架	安全域框架	时间管理框架
逻辑层	信息资产	风险管理策略	流程图与服务	信任关系	安全域映射关系	日历与时间表
物理层	数据资产	风险管理实践	过程机制	人机界面	基础设施	进程调度
组件层	组件资产	风险管理组件及标准	过程组件及标准	人类实体组件及标准	定位器组件及标准	步骤计时排序组件及标准
管理层	业务连续性管理	运营风险管理	进程管理	应用程序与用户管理	环境管理	时间与绩效管理

SABSA 是一套开放的架构，将不同的信息安全标准方法进行整合，形成一个端到端的安全解决方案，并与其他标准（如 TOGAF 和 ITIL）无缝结合，填补了安全架构和安全服务管理之间的空隙。

3. P2DR 模型

P2DR（Policy, Protection, Detection, Response）模型是美国 ISS 公司于 20 世纪 90 年代末提出的一种动态安全模型。在整体的安全策略的控制和指导下，P2DR 模型综合运用防火墙、操作系统身份认证、加密等防护工具进行防护，利用检测工具（如漏洞评估、入侵检测等）了解和评估系统的安全状态，并通过适当的响应机制将系统调整到最安全和风险最低的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全，P2DR 模型结构如图 1-6 所示。

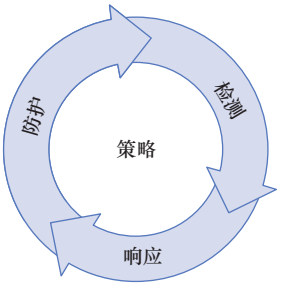

图 1-6　P2DR 模型结构

P2DR 模型包括四个主要部分：安全策略（Policy）、防护（Protection）、检测（Detection）和响应（Response）。

（1）策略：定义系统的监控周期，确立系统恢复机制，制定网络访问控制策略，明确系统的总体安全规划和原则。

（2）防护：通过修复系统漏洞、正确设计开发和安装系统来预防安全事件的发生；通过定期检查发现可能存在的系统脆弱性；通过访问控制、监视等手段防止恶意威胁。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（Virtual Private Network , VPN）技术、防火墙、安全扫描和数据备份等。

（3）检测：是动态响应和加强防护的依据，通过不断地检测和监控网络系统，来发现新的威胁和弱点，并通过循环反馈来及时做出有效的响应。当攻击者穿透防护系统时，检测功能可与防护系统形成互补，提高机构的防御效率。

（4）响应：在发生安全事件时，快速响应并采取适当的行动。具体包括隔离受感染的系统、恢复数据、修复漏洞、收集证据和通知相关方等。有效地响应可以降低损失，并帮助机构从安全事件中恢复过来。

4. STRIDE 威胁模型

STRIDE（Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege）威胁模型由 Microsoft 公司于 1999 年提出，是一种以开发人员为中心的威胁建模方法，通过此方法可识别对应用程序造成影响的威胁、攻击、漏洞，进而采取相应防护措施，以降低机构网络安全风险。其模型结构如图 1-7 所示。

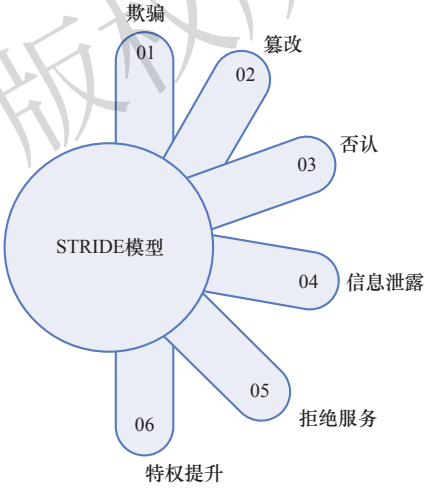

图 1-7　STRIDE 威胁模型结构

STRIDE 将网络安全威胁分为 6 类，分别是欺骗（Spoofing）、篡改（Tampering）、否认（Repudiation）、信息泄露（Information disclosure）、拒绝服务（Denial of service）与特权提升（Elevation of privilege）。每种威胁的具体描述如下：

（1）欺骗

行为涉及非法访问并使用其他用户的身份验证信息，例如用户名和密码。欺骗攻击包括 Cookie 重放攻击、会话劫持和跨站点请求伪造攻击等。可使用安全的用户身份验证方

法来防范欺骗攻击，包括安全密码要求和多因素身份验证等。

（2）篡改

对数据进行恶意修改，破坏应用程序的完整性。包括未经授权更改持久保存的数据、更改通过开放网络在两台计算机之间传输的数据等行为。跨站点脚本 、SQL（Structured Query Language）注入等都属于篡改攻击。

（3）否认

指用户拒绝执行某个操作，但其他操作方无法证实这种拒绝无效。例如，某个用户在无法跟踪受禁操作的系统中执行非法操作。否认攻击利用系统无法正确跟踪和记录用户操作的缺陷来操纵或伪造新的、未经授权的操作的标识，或将错误数据记录到日志文件中，影响系统的正常运行。

（4）信息泄露

指将信息泄露给无权访问它的访问者。信息泄露可能来自应用程序中留下的开发人员备注、提供参数信息的源代码或包含过多细节的错误消息，攻击者可能利用这些信息来获取用户数据、敏感的商业或业务数据以及有关应用程序及其基础架构的技术细节等内容。

（5）拒绝服务

让目标机器拒绝向有效用户提供服务。攻击方式包括消耗网络带宽、连通性攻击、利用协议缺陷等。拒绝服务攻击的目的是迫使服务器的缓冲区满，不接收新的请求，或者使用 IP 欺骗，迫使服务器把非法用户的连接复位，影响合法用户的连接。

（6）特权提升

无特权用户非法获取访问权限。攻击者通常利用程序中的漏洞和错误配置来获取或提升访问权限，从而入侵或破坏整个系统。

5. 攻击树威胁模型

攻击树（Attack Trees）是 Schneier 于 1999 年提出的一类威胁模型，提供了一套正式且条理清晰的建模方法来描述系统所面临的安全威胁及可能遭受的多种攻击。攻击树通过树形结构来表示系统面临的攻击，通常包括一个根节点、若干个子节点和叶节点。根节点表示攻击者的最终目标，子节点表示攻击者达成目标的不同途径，叶节点表示攻击者为达成目标所需要执行的具体任务。攻击树的一个示例如图 1-8 所示。攻击树的构建包括以下几个步骤：

（1）确定攻击者的最终目标，如破坏系统、窃取数据等。

（2）将最终目标分解为多个子目标，每个子目标表示达成上一层目标的其中一条途径，包含一个或多个具体任务，攻击者需要完成这些任务来达成对应的子目标。

（3）组合所有目标与任务节点，构建攻击树模型。

攻击树具有结构化、可重用的特点，对攻击所需的步骤进行分层表示，每一条从根节点到叶节点的路径表示一次完整的攻击过程。树中每条路径都是唯一的，并且设计中不存在循环。对于复杂的系统，还可以为每个组件单独构建攻击树。管理员通过构建攻击树来制定安全决策，确定系统是否容易受到攻击以及评估特定类型的攻击。

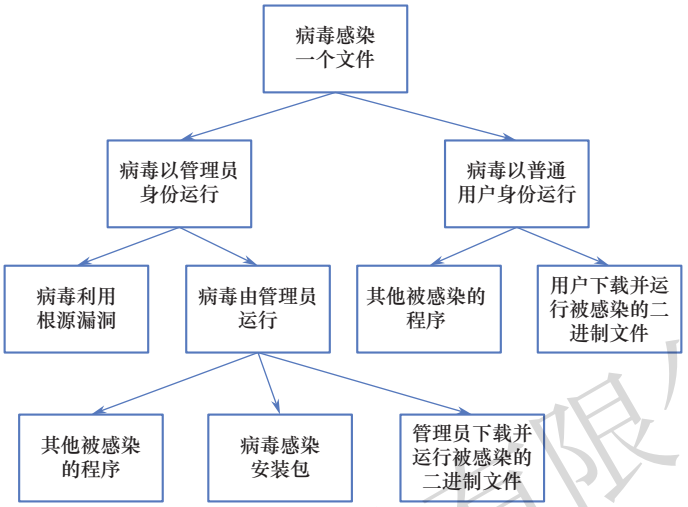

图 1-8　攻击树的一个示例

攻击树应用在具体实例中时，其结构可能变得庞大而复杂，一个完整的攻击树很可能包括成百上千的叶节点。即便如此，攻击树也可以在很大程度上帮助安全人员找出系统存在的威胁，制定应对攻击的方案。攻击树通常与其他技术与框架结合使用，如 STRIDE，CVSS 和 PASTA 模型等。

6. WPDRRC 模型

WPDRRC（Warning, Protection, Detetion, Response, Recovery, Counterattack）安全模型是我国“八六三”信息安全专家组于 2002 年在 PDR 模型、P2DR 模型及 PDRR（Protection, Detection, Response, Recovery）等模型的基础上提出的，适合我国国情的网络动态安全模型。WPDRRC 在 PDRR 模型的前后增加了预警和反击功能，其整体结构如图 1-9 所示。

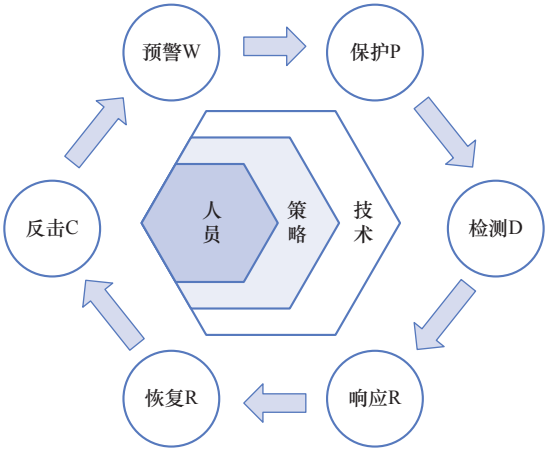

图 1-9　WPDRRC 模型整体结构

WPDRRC 模型有 6 个环节和 3 大要素。6 个环节包括预警、保护、检测、响应、恢复

和反击，它们具有较强的时序性和动态性，能够较好地反映出信息系统安全保障体系的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力。3 大要素包括人员、策略和技术。3 大要素落实在 WPDRRC 模型 6 个环节的各个方面，将安全策略变为安全现实。

WPDRRC 模型的特点是全面地涵盖了各个安全因素，突出了人、策略、管理的重要性，反映了各个安全组件之间的内在联系。该模型强调了预警和反击在信息安全保障体系中的重要作用，通过加强预警和反击能力，可以更好地应对各种网络攻击和数据泄露事件。此外，WPDRRC 模型还强调了人员的重要性，认为人员是核心，策略是桥梁，技术是保证。在实施 WPDRRC 模型的过程中，需要将安全策略变为安全现实，通过人员、策略和技术三个要素的有机结合，实现信息系统的全面安全保障。

7. 攻击模拟和威胁分析流程模型

攻击模拟和威胁分析流程（Process for Attack Simulation and Threat Analysis, PASTA）是 VerSprite Security 公司在 2012 年开发的以风险为中心的威胁建模方法，它提供了一个循序渐进的过程，从一开始就将风险分析和环境信息加入机构的整体安全策略中。PASTA 包含七个阶段，每个阶段包含了多个任务，如图 1-10 所示。

1. 定义目标	• 确定业务目标 • 确定安全合规要求 • 业务影响分析
2. 定义技术范围	• 获取技术环境的边界 • 获取设备|应用程序|软件的依赖性
3. 分解应用程序	• 确定用户案例|定义应用程序入口与信任等级 • 确定人员|资产|服务|角色|数据源 • 数据流图|信任边界
4. 威胁分析	• 概率攻击场景分析 • 安全事件回归分析 • 威胁情报相关性与分析
5. 脆弱性分析	• 现有漏洞报告查询与问题跟踪 • 使用威胁树将威胁与现有漏洞进行映射 • 对使用和滥用案例进行设计缺陷分析 • 评分|枚举
6. 攻击建模	• 攻击面分析 • 攻击树开发|攻击库管理 • 使用攻击树分析漏洞利用情况
7. 风险与影响分析	• 业务影响定性&定量 • 对策识别与残余风险分析 • ID风险缓解战略

图 1-10　PASTA 模型

（1）定义目标

目标可分为内部驱动、外部驱动及用户驱动。主要任务包括业务目标与安全合规要求的确定以及业务影响分析。

（2）定义技术范围

通过定义技术范围来了解机构的攻击面，从而明确保护对象。主要任务包括获取技术环境的边界及设备、应用程序、软件的依赖性。

（3）分解应用程序

围绕机构内所有事物间的组合关系构建隐式信任模型。具体任务包括确定用例、资产、服务、角色等信息，定义应用程序入口及信任等级，生成数据流图与信任边界等。

（4）威胁分析

对威胁进行分析，了解应用程序行为及威胁类型。主要任务包括概率攻击场景分析、安全事件回归分析、威胁情报相关性与分析等。

（5）脆弱性分析

将应用程序的漏洞与资产相关联，找出系统存在的风险与缺陷。主要任务包括漏洞报告查询、问题追踪、威胁映射、设计缺陷分析、漏洞评分等。

（6）攻击建模

针对网络攻击建立概率模型。主要任务包括攻击面分析、攻击树开发、攻击库管理、漏洞利用分析等。

（7）风险与影响分析

整合前 6 个阶段的信息，制定风险管理对策。主要任务包括业务影响定性与定量、应对措施识别、剩余风险分析等。

PASTA 致力于使技术安全要求与业务目标保持一致，在不同阶段使用了多种设计和启发工具，与其他传统威胁建模框架相比，具有较高的可扩展性与可用性，并且能够从攻击者角度，充分利用机构内部的现有流程对威胁进行分析。

8. 自适应安全架构

自适应安全架构（Adaptive Security Architecture, ASA）是 Gartner 于 2014 年提出的面向下一代的安全体系框架，以应对新时代网络安全所面临的严峻形势。2017 年，Gartner 在 1.0 的基础上进行扩展，提出了 ASA2.0 与 3.0 两个版本，目前国内机构主要用的是 2.0 版本。ASA 从预测、防御、检测、响应四个维度，强调安全防护是一个持续处理的、循环的过程，细粒度、多角度、持续化地对安全威胁进行实时动态分析，自动适应不断变化的网络和威胁环境，并不断优化自身的安全防御机制。ASA 整体架构如图 1-11 所示。

（1）防御：指一系列可以用于防御攻击的策略集、产品和服务。关键目标是通过减少攻击面来提升攻击门槛，并在受影响前拦截攻击动作。

（2）检测：用于发现未被成功防御的网络攻击，关键目标是降低网络攻击的威胁程度以及减少其他潜在的损失。

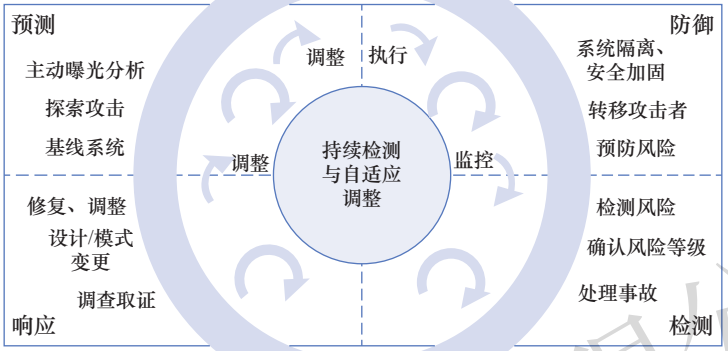

图 1-11　ASA 整体架构

（3）响应：用于调查和补救被检测分析功能（或外部服务）查出的网络安全威胁，并提供入侵认证和攻击来源分析，帮助机构采取新的预防手段避免事故发生。

（4）预测：通过防御、检测、响应结果不断优化基线系统，不断提高对未知、新型攻击的预测精度，并将预测结果反馈到防御、检测与响应功能中，从而构成整个处理流程的闭环。

9. NIST 网络安全框架

NIST 网络安全框架是美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）于 2014 年提出的一种信息安全管理框架，旨在帮助机构建立和维护有效的信息安全管理系统。该框架的 1.1 版本包括五个核心功能：识别、保护、检测、响应和恢复，在 2024 年推出的 2.0 版本中增加了第六个功能——治理，之前的五个功能围绕该功能展开。其整体结构如图 1-12 所示。

图 1-12　NIST 网络安全框架的整体结构

（1）治理

建立、传达和监控机构的网络安全风险管理战略、期望和政策。治理的目的是告知机构可以采取哪些行动来实现其他五个功能的成果，并确定行动优先顺序。治理活动对于将网络安全纳入机构更广泛的风险管理战略至关重要，能够帮助机构建立网络安全战略和网络安全供应链风险管理，确定角色、职责和权限，制定相关政策以及对反垄断战略的监督。

（2）识别

了解当前存在的网络安全风险。了解机构的资产（例如，数据、硬件、软件、系统、设施、服务、人员）、供应商和相关的网络安全风险，根据机构的风险管理战略和任务需

求确定各工作任务的优先顺序。该功能还包括对机构的政策、计划、流程、程序和实践流程进行改进，以支持网络安全风险管理。

（3）保护

采取安全措施来预防或降低网络安全风险。一旦确定了资产和风险的名单与优先级，保护功能就能够为这些资产提供担保，以减少网络安全事件出现的可能性和造成的影响。该功能涵盖的内容包括身份管理、身份验证和访问控制，安全意识培训，数据安全与平台安全（即物理和虚拟平台的硬件、软件和服务）防护以及关键信息基础设施的保护等。

（4）检测

查找并分析可能的网络安全攻击和危害。检测功能能够及时发现和分析异常、危害指标和其他可能表明网络安全攻击正在发生的潜在不良事件。此功能可以帮助机构实现及时的威胁检测和事件响应。检测措施具体包括安全监控、事件响应和漏洞管理等。

（5）响应

对检测到的网络安全事件采取行动。响应功能为机构提供了控制网络安全事件影响的能力，能够帮助机构快速响应安全事件，最小化事件对业务的影响。具体包括事件管理、分析、缓解、报告和沟通等流程。

（6）恢复

恢复受网络安全事件影响的资产和操作。恢复功能能帮助机构及时恢复信息系统的正常运行，减少突发安全事件的影响。具体包括制定并实施恢复计划、评估事件影响、进行恢复后的调查与分析等步骤。

NIST 网络安全框架可以以多种不同的方式使用，它的使用将根据机构的独特使命和风险而有所不同。通过了解利益相关者的期望、风险偏好和容忍度，机构可以优先考虑某些网络安全活动，以使他们能够就网络安全支出和行动做出明智的决定。

10. ISO/IEC 27002:2022 框架

ISO/IEC 27000 标准是由国际标准化组织（ISO）及国际电工委员会（IEC）联合制定的一系列标准，该系列标准包含了网络安全管理体系概述和词汇、网络安全管理体系实施指南、网络安全风险管理、网络安全管理系统验证机构认证规范、网络安全管理体系规范与使用指南、网络安全管理实用规则等一系列的网络安全管理系统领域中的风险及相关管控。2022 年 2 月，ISO 发布了 ISO/IEC 27002:2022 信息安全、网络安全和隐私保护—信息安全控制标准，作为组织根据信息安全管理体系认证标准制定和实施信息安全控制措施的指南。2022 版的主要变化如下：

（1）加强对业务连续性的支持。

（2）加强云环境、云服务的安全管理。

（3）加强个人数据、隐私数据等敏感数据的安全管理。

（4）提高自动化技术水平和利用自动化工具。

参照该标准所制定的 ISO/IEC 27002:2022 框架，由组织控制、人员控制、物理控制和

技术控制 4 大主题以及各主题下共计 93 个控制项组成，每一个控制项都包括控制、目的、指南和其他信息等部分，用于描述该控制项的内容以及关注的要点。此外该框架还对控制项进行了属性细分，包括控制类型、信息安全、网络安全、运营能力和安全域等 5 个属性。其框架如图 1-13 所示。

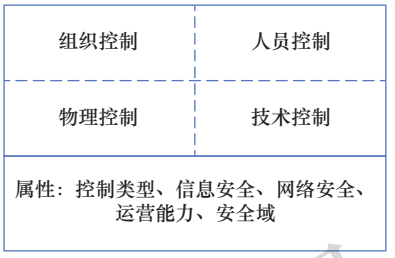

图 1-13　ISO/IEC 27002:2022 框架

2022 版的框架简单且内容详实，易于机构对网络安全控制进行分类，同时增加了控制的属性，可用来实现特定主题的划分和选择，针对性更强，以帮助机构加强网络安全控制方案的实施，支撑网络安全策略的执行。

1.4.2　我国网络安全保护体系架构

1. 网络安全等级保护体系架构

网络安全等级保护对象通常是指由计算机或者其他信息终端及相关设备组成的，按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为五个安全保护等级。网络安全等级保护是国家网络安全工作的基本制度，是实现国家对重要网络、信息系统、数据资源实施重点保护的重大措施，是维护国家关键信息基础设施的重要手段。

随着信息技术的发展，我国等级保护标准体系由 1.0 升级至 2.0，等级保护对象已经从狭义的信息系统，扩展到网络基础设施、云计算平台/系统、大数据平台/系统、物联网、工业控制系统、采用移动互联技术的系统等，基于新技术和新手段提出新的分等级的技术防护机制和完善的管理手段，是等级保护 2.0 标准体系的重点内容。等级保护 2.0 标准体系的具体特点如下：

（1）对象范围为等级保护对象，具体包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、工业控制系统和采用移动互联技术的系统等。

（2）针对云计算、移动互联、物联网、工业控制系统及大数据等新技术和新应用领域提出新要求，形成了安全通用要求加新应用安全扩展要求构成的标准要求内容。

（3）采用“一个中心，三重防护”的防护理念和分类结构，强化了建立纵深防御和精细防御体系的思想。

（4）强化密码技术和可信计算技术的使用，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求，强调通过密码技术、可信验证、安全审计和态势感知等建立主动防御体系。

基于等级保护 2.0 标准体系，我国设计了网络安全等级保护体系，其架构如图 1-14 所示。在遵循该架构的前提下，可采取以下具体措施来确保网络安全等级保护工作的有效

开展：

（1）明确等级保护对象及对应的安全保护等级。

（2）确定等级保护对象的安全保护等级后，根据不同对象的安全保护等级完成安全建设或安全整改工作。

（3）针对等级保护对象特点建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系。

（4）依据国家网络安全等级保护政策和标准，开展组织管理、机制建设、安全规划、安全检测、通报预警、应急处置、态势感知、能力建设、技术检测、安全可控、队伍建设、教育培训和经费保障等工作。

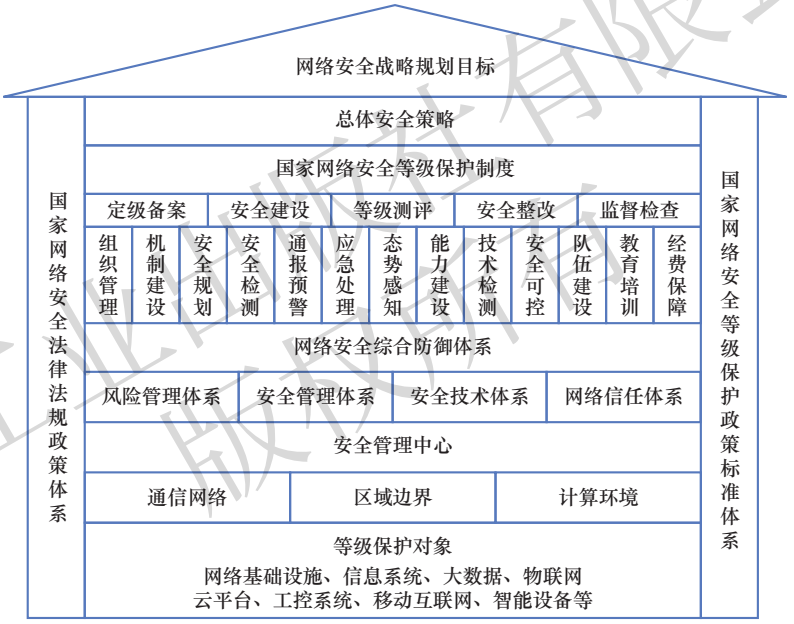

图 1-14　网络安全等级保护体系架构

2. 关键信息基础设施安全保护体系架构

我国在网络安全等级保护制度的基础上，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、丧失功能或者数据泄露，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实行重点保护，并制定《关键信息基础设施安全保护条例》，建立以国家网信部门、国务院公安部、关键信息基础设施保护工作部门（以下简称“保护工作部门”）、关键信息基础设施运营者（以下简称“运营者”）为主体的关键信息基础设施安全保护体系架构。

（1）国家网信部门和国务院公安部等国家有关职能部门

国家网信部门负责统筹协调关键信息基础设施安全保护工作，在具有全局性、方向性、基础性的问题上发挥作用。

公安机关承担打击网络违法犯罪职能，负责指导监督关键信息基础设施安全保护工作。受理关键信息基础设施认定规则和关键信息基础设施目录备案，协助运营者开展安全背景审查，为保护工作部门提供技术支持和协助等方面。

除此之外，国家安全、保密行政管理、密码管理等部门依照《关键信息基础设施安全保护条例》和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

（2）保护工作部门

在关键信息基础设施保护体系中，保护工作部门是与运营者联系最密切、具体职责最丰富的行业主管、监管部门，负责制定关键信息基础设施的认定规则。保护工作部门需要结合本行业、本领域的实际情况和不同特点，综合考虑重要程度、破坏后的危害程度、与其他行业的关联性等因素，确定关键信息基础设施保护的具体对象，进而开展关键信息基础设施保护工作。

其次，保护工作部门是运营者的主要报告对象。在遇到影响关键信息基础设施认定结果的重大变化、年度网络安全检测和风险评估情况、发生重大网络安全事件和发现重大网络安全威胁、运营者发生合并/分立/解散等情况时，运营者需要向保护工作部门进行报告。

此外，保护工作部门还具有对关键信息基础设施的保障促进职能，包括在本行业、本领域制定关键信息基础设施安全规划、建立监测预警制度、建立健全应急预案、定期组织应急演练、组织开展检查检测等。

（3）省级人民政府有关部门

省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理，根据条块管理的职责划分，在国家网信部门的统筹协调下，与国务院公安部、保护工作部门协调开展关键信息基础设施保护工作，并对本地区没有主管监管部门的运营者负指导监管责任。

（4）关键信息基础设施运营者

运营者依照《关键信息基础设施安全保护条例》和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。具体措施包括落实“同步规划、同步建设、同步使用”的安全要求、建立健全网络安全保护制度和责任制、设置专门安全管理机构、落实专门安全管理机构的各项职责、每年至少进行一次网络安全检测和风险评估、及时报告重大网络安全事件和网络安全威胁、优先采购安全可信的网络产品和服务、明确网络产品和服务提供者的技术支持和安全保密义务与责任等。

1.4.3　网络安全建设与运营架构

在信息化发展的初期，机构常依赖静态的控制清单和安全架构来应对网络安全威胁。

随着信息技术的发展，网络安全威胁变得更加频繁与复杂，传统网络防御策略已无法满足机构网络安全工作的需求。为了适应快速变化的数字服务和信息技术，确保网络安全策略能够灵活应对复杂多变的网络环境，机构需要以管理、技术与保障措施作为基础，构建网络安全建设与运营架构，以实现网络安全目标。本书将网络安全建设与运营分为网络安全管理体系、网络安全技术体系、网络安全运营体系和网络安全保障体系四个部分展开阐述，其架构如图 1-15 所示。

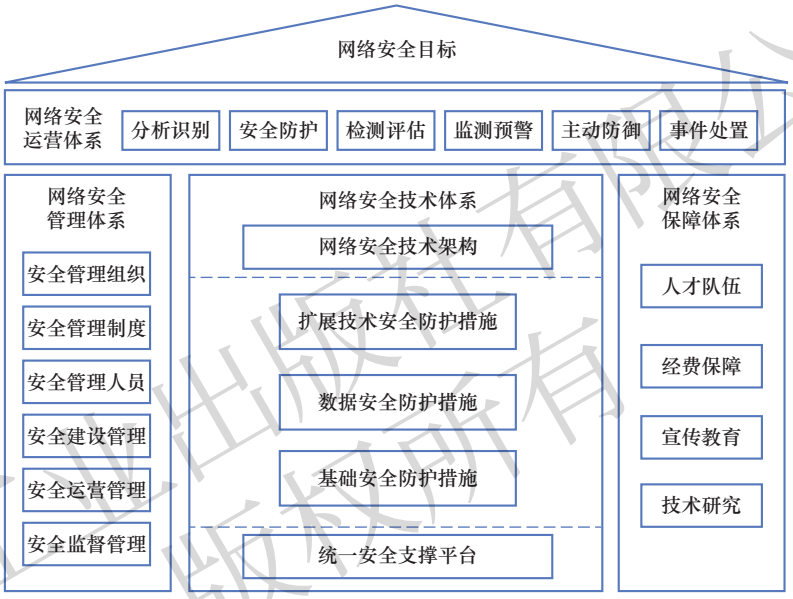

图 1-15　网络安全建设与运营架构

（1）网络安全管理体系涵盖网络安全策略、规程、指南以及相关资源和活动等，具体包括安全管理组织、安全管理制度、安全管理人员、安全建设管理、安全运营管理和安全监督管理等，是建立、实施、运行、监视、评审、维护和改进机构网络安全来实现业务目标的系统方法，旨在确保机构的网络安全各项措施遵守法律法规、符合有关规定，且能够有效控制网络安全风险。

（2）网络安全技术体系涵盖基础安全防护措施、数据安全防护措施、扩展技术安全防护措施，以及统一安全支撑平台等相关的网络安全设备与系统等，旨在为网络安全管理、运营与保障体系提供系统和工具支撑，以预防、识别并抵御外来威胁与内部风险。

（3）网络安全运营体系涵盖分析识别、安全防护、检测评估、监测预警、主动防御与事件处置等主要环节，是统筹协调机构网络安全运营团队人员，按照网络安全管理要求，利用网络安全技术体系的系统和工具，开展网络安全治理的一系列持续活动的总称，旨在发现机构已存在或未来可能会出现的安全风险，并利用高效的安全防控措施来主动化解风险，以此不断改善机构的安全状况。

（4）网络安全保障体系涵盖一系列用于支撑网络安全建设、保障网络安全工作顺利开

展的措施，具体包括人才队伍、经费保障、宣传教育、技术研究等方面，旨在为机构的网络安全管理体系、网络安全技术体系、网络安全运营体系提供支撑，为网络安全建设与运营提供人、财、物全方位保障。

四个体系相互支撑、相互促进，如图 1-16 所示。

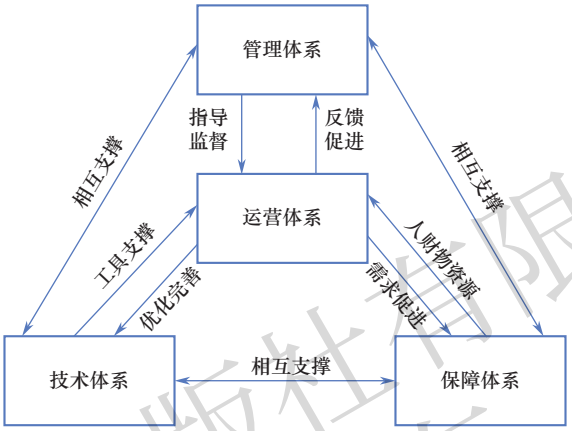

图 1-16　网络安全建设与运营各体系间的关系

网络安全管理体系通过制定和执行机构的网络安全策略、标准和流程，明确网络安全技术体系、网络安全运营体系和网络安全保障体系的制度规程，指导与监督各体系的工作。

网络安全技术体系通过技术手段为网络安全管理体系、网络安全运营体系和网络安全保障体系提供系统和工具的支撑。

网络安全运营体系将安全人员、安全技术、安全策略、安全制度和安全服务有机结合，有效串联原先相对分散、割裂的安全设备、安全管理以及安全服务。安全人员依据网络安全管理体系的标准制度、操作规范等内容，利用网络安全技术体系构建的安全组件及平台，针对资产安全、威胁预警、安全事件开展标准化、规范化、系统化的运营工作，并将结果反馈给各体系，促进各体系的完善与优化。

网络安全保障体系为网络安全管理体系、网络安全技术体系、网络安全运营体系提供人、财、物全方位支撑，确保各体系工作能持续有效开展。

习　题

1. 简述人类社会进入数字化时代前后所经历的三次数字化浪潮。
2. 什么是网络安全？
3. 网络安全威胁事件分为哪几类？
4. 简述我国《国家网络空间安全战略》的主要内容。

5.《网络安全法》提出，在网络安全保护方面国家实行_____制度。

6.《密码法》规定，我国密码分为哪几类，每一类分别保护用户哪些信息？

7.《关保条例》规定，机构的_____对关键信息基础设施安全保护负总责。

8.《网络安全审查办法》规定哪些情形需要申报网络安全审查？

9. _____对信息安全国家标准进行统一技术归口，统一组织申报、送审和报批。

10. 我国网络安全等级保护系列标准主要包括哪些？

11.《网络安全等级保护实施指南》规定，等级保护的基本流程有哪些阶段？

12. SM 系列商用密码中对称算法、非对称算法分别有哪些？

13. 常见的网络安全架构有哪些？至少列举 5 个。

14. 网络安全等级保护对象通常是指什么？

15. 网络安全建设运营架构可分为哪几大体系？描述下各体系间的关系。