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

网络安全保护制度与实施

郭启全　编著

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

内 容 简 介

网络安全保护制度是网络安全领域的“交通规则”。本书共 7 章，围绕“网络安全保护制度与实施”这一主题，系统介绍国家网络安全保护制度体系的构成，落实网络安全保护制度的主要思路、方法和重要措施，以及与其有关的法律、政策和标准。其中，第 1 章介绍国家网络安全保护制度体系的构成，第 2 章介绍网络安全等级保护制度的主要内容和主要措施等，第 3 章介绍关键信息基础设施安全保护制度的主要内容，第 4 章介绍数据安全保护制度的主要内容，第 5 章介绍网络安全法律体系，第 6 章介绍网络安全政策体系，第 7 章介绍网络安全标准体系。

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基础课教材，适合网络空间安全专业、信息安全专业及相关专业的大学生、研究生系统学习国家网络安全制度和实施办法，掌握网络安全重要规则和技能使用，也适合各单位各部门网络安全工作者、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

网络安全保护制度与实施 / 郭启全编著 . -- 北京 : 电子工业出版社 , 2025. 7. -- ISBN 978-7-121-49972-2

Ⅰ. TP393.08

中国国家版本馆 CIP 数据核字第 2025QG5022 号

责任编辑：刘御廷　　文字编辑：李晓彤
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：15.75　　字数：350 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：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

我国网络安全法律法规和政策确立了网络安全保护制度，形成了各行各业网络安全工作日常应遵守的规则规范。遵守网络安全规则规范，就像司机遵守交通规则，司机不遵守交通规则就是违法违规；同理，任何组织和个人不遵守网络安全规则规范，也是违法违规。网络安全保护制度主要包括网络安全等级保护制度、关键信息基础设施安全保护制度、数据安全保护制度、个人信息保护制度、密码保护制度、网络安全审查制度等，构成了我国网络安全保护制度体系，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根本保障。

《中华人民共和国网络安全法》（以下简称《网络安全法》）和国家有关政策文件确定的网络安全等级保护制度，是我国网络安全的基本制度、基本国策和基本方法，是我国网络安全工作的基础防线和基石。从我国网络安全工作的实际需要出发，确立的关键信息基础设施安全保护制度，是网络安全的重点保护制度。关键信息基础设施是经济社会运行的神经中枢，是网络安全保护的重中之重。《中华人民共和国数据安全法》（以下简称《数据安全法》）和国家有关政策文件确立的数据安全保护制度，也是网络安全的重点保护制度。数据作为关键生产要素和重要战略资源，在国家经济发展和社会进步中日益发挥着基础性和全局性作用。《关键信息基础设施安全保护条例》和《数据安全法》将网络安全等级保护制度延伸到关键信息基础设施安全保护领域和数据安全保护领域，并将网络安全等级保护制度作为二者的基础，从法律层面确定了三个制度之间的关系，即一个基础、两个重点。按照法律规定，应从网络安全政策层面、标准层面对三个制度进行有效衔接，协调落实，建立科学的网络安全政策体系和标准体系。

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。

本书由郭启全编著，共 7 章，主要介绍国家网络安全保护制度体系的构成，网络安全等级保护制度、关键信息基础设施安全保护制度、数据安全保护制度的主要内容及其内在关系，落实三个制度的主要方法、最新思路与理念及重要措施，网络安全法律体系、政策体系和标准体系。本书是高等院校网络空间安全专业实战化人才培养的重要教材，是学习其他专业课的基础。

王思登绘制了部分插图，在此表示衷心感谢。书中不足之处，敬请读者指正。

作者

目录 CONTENTS

第 1 章 国家网络安全保护制度体系

本章主要介绍国家网络安全保护制度体系的构成，确立这些制度的法律和政策依据，以及这些制度的内在关系，使读者对国家网络安全保护制度体系有一个清晰的了解和掌握，便于在工作中落实。国家网络安全保护制度是网络安全的规矩、规范和规则，是网络安全法律、政策的细化，是各行各业在网络安全日常工作中需要认真落实的具体要求。

1.1 网络安全保护制度的确立及其法律政策依据

国家网络安全法律法规确定的网络安全保护制度，主要包括网络安全等级保护制度、关键信息基础设施安全保护制度、数据安全保护制度和个人信息保护制度等，构成了我国网络安全保护制度体系。

1.1.1 网络安全等级保护制度的基本含义

网络安全等级保护制度是我国网络安全的基本制度、基本国策和基本方法，是我国网络安全工作的创举、网络安全界的智慧结晶、网络安全的基础防线和基石，是网络安全领域保障我国经济健康发展，维护国家安全、社会秩序和公共利益的根本保障。网络安全等级保护制度历经三十多年，从信息安全等级保护制度发展到现在的网络安全等级保护制度，进入网络安全等级保护制度 2.0 时代。

1. 信息安全等级保护制度

1994 年，国家出台《中华人民共和国计算机信息系统安全保护条例》（国务院令第 147 号发布，以下简称《计算机信息系统安全保护条例》），其中第九条明确规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。

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》（中办发〔2003〕27 号）明确指出，“实行信息安全等级保护”，“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”。

2004 年，国家网络与信息安全协调小组第三次会议讨论通过的《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号）指出，信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。

2007 年，公安部、国家保密局、国家密码管理局、国务院原信息化工作办公室四部门联合出台《信息安全等级保护管理办法》（公通字〔2007〕43 号），在公安部的组织领导下，全国实施信息安全等级保护制度。自 2007 年至 2017 年的 10 年间，国家建立了信息安全等级保护制度，为提升国家信息安全保障能力和水平发挥了重要作用。这个阶段称为网络安全等级保护制度 1.0 时代。

2. 网络安全等级保护制度的确立

2017 年，国家出台《中华人民共和国网络安全法》（以下简称《网络安全法》），其中第二十一条规定，国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。《网络安全法》确立了网络安全等级保护制度，也标志着网络安全等级保护制度进入 2.0 时代。

国家实行网络安全等级保护制度，对网络（包括网络基础设施、信息系统、数据资源等）实施分等级保护、分等级监管，对网络中使用的网络安全产品实行分等级管理，对网络中发生的安全事件分等级响应和处置。2017 年，中央出台关于加强网络安全和信息化工作的有关意见，要求“完善国家网络安全等级保护制度”。

国家在信息安全等级保护制度的基础上建立了网络安全等级保护制度，通过实施网络安全等级保护制度实现三个目标：

（1）确保网络运营者在网络建设过程中，同步规划、同步建设、同步使用网络安全保护措施，履行网络安全保护责任和义务。

（2）确保产品供应商在 IT 产品和网络安全产品的设计制造中落实国家网络安全要求。

（3）确保网络安全服务商在安全服务中落实国家网络安全要求，提供安全、可靠、可信的服务，为我国实施网络强国战略保驾护航。

3. 网络安全等级保护工作

网络安全等级保护制度规定的第一项内容是网络实施分等级保护、分等级监管，此项规定的内容即是网络安全等级保护工作，其具体内容如下：

（1）将网络按照重要性和遭受损坏后的危害性，分为五个安全保护等级（从第一级到第五级，逐级增高）。

（2）安全保护等级确定后，第二级（含）以上网络运营者到公安机关备案，公安机关对备案材料和定级准确性进行审核，审核合格后颁发备案证明。

（3）网络运营者选择符合国家要求的等级测评机构，开展网络安全等级保护测评（以

下简称等级测评）。

（4）根据网络的安全保护等级，按照国家有关法律、政策、标准开展网络安全建设整改，建设安全设施、落实安全措施、落实安全责任制、建立和落实安全管理制度。

（5）公安机关对第二级网络的安全保护工作进行指导，对第三、第四级网络的安全保护工作开展监督检查。

在我国境内建设、运营、维护、使用的网络，均应开展网络安全等级保护工作，并实施监督管理。有关网络安全等级保护制度的具体内容，详见第 2 章。

1.1.2　关键信息基础设施安全保护制度的基本含义

1. 关键信息基础设施安全保护制度的确立

《网络安全法》从网络安全工作的实际需要出发，对关键信息基础设施安全保护作出了法律规定，对关键信息基础设施的运行安全提出了明确要求；2017 年中央出台有关文件，要求建立关键信息基础设施安全保护制度；2021 年 7 月，国务院出台《关键信息基础设施安全保护条例》，确立了关键信息基础设施安全保护制度，标志着我国开启了关键信息基础设施安全保护时代。

2. 关键信息基础设施的定义

关键信息基础设施是指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等。

关键信息基础设施是经济社会运行的神经中枢，是网络安全保护的重中之重，日益发挥着基础性、全局性、支撑性作用。保障关键信息基础设施安全，对维护国家网络空间主权和国家安全、保障经济社会健康发展、维护公共利益和公民合法权益具有重大意义。

3. 关键信息基础设施安全保护制度的主要内容

关键信息基础设施安全保护制度是网络安全重点保护制度，国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于我国境内外的网络安全风险和威胁，保护关键信息基础设施免受非法侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。该制度规定了如下重要内容：

（1）关键信息基础设施的范围，即重要行业和领域的，以及其他涉及可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

（2）明确了关键信息基础设施的认定流程和方法。

（3）国家、网络安全职能部门、关键信息基础设施安全保护工作部门（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）、网络安全服务机构和公民个人的责任义务以及应采取的措施。

（4）网络安全职能部门、保护工作部门、运营者、网络安全服务机构、公民个人应承

担的法律责任。

（5）对关键信息基础设施安全，应从保卫、保护和保障三个方面予以加强。同时强调，运营者在落实网络安全等级保护制度的基础上，采取有效措施，保障关键信息基础设施的运行安全和数据安全。

有关关键信息基础设施安全保护制度的具体内容，详见第 3 章。

1.1.3 数据安全保护制度的基本含义

数据作为关键生产要素和重要战略资源，在国家经济发展和社会进步中发挥基础性和全局性作用。保护数据安全，是维护国家安全、经济社会发展的重要内容。

1. 数据安全保护制度的确立

党中央明确提出要加强数据安全工作，2021 年 6 月国家出台《中华人民共和国数据安全法》（以下简称《数据安全法》），对数据安全提出了明确要求，确立了数据安全保护制度。数据安全保护制度是国家网络安全领域的重点保护制度。

2. 数据安全保护制度的主要内容

一是国家建立数据安全制度和工作协调机制；二是建立数据分类分级保护制度，数据按照重要性等因素分为一般、重要、核心三个等级；三是在网络安全等级保护制度基础上，加强数据安全保卫、保护和保障工作；四是建立数据安全监管机制，加强数据在交易、出境、传输、使用中的安全监管；五是明确数据处理者的主体责任和行业主管部门的主管责任；六是在网络安全审查制度基础上，建立数据安全审查制度；七是依托国家网络与信息安全信息通报机制，建立数据安全信息通报预警机制，建立应急处置机制、事件调查机制；八是加强数据全生命周期和全流程安全保护；九是打击涉及数据安全的违法犯罪活动。有关数据安全保护制度的具体内容，详见第 4 章。

1.1.4 个人信息保护制度的基本含义

在信息化、数字化、智能化时代，个人信息保护关系到人民群众的合法权益和切身利益，保护好公民个人信息，是全社会共同关注的重点事项，也是国家必须解决的重要问题。

1. 个人信息保护制度的确立

《网络安全法》《数据安全法》对个人信息保护给出了明确规定。2021 年国家出台《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》），确立了个人信息保护制度。该制度坚持以人民为中心的法治理念，聚焦个人信息保护领域的突出问题、威胁风险和人民群众的重大关切，明确保护重点，采取有力措施，依法维护人民群众的合法权益和切身利益。

2. 个人信息保护制度的主要内容

一是确立了个人信息保护原则，二是规范了个人信息处理活动权益保障，三是禁止“大数据杀熟”并规范了自动化决策，四是严格保护敏感个人信息，五是规范了国家机关处理活动，六是赋予了公民个人充分权利，七是强化了个人信息处理者的责任义务，八是赋予了大型网络平台更多的法律义务，九是规范了个人信息跨境流动，十是健全了个人信息保护工作机制。有关个人信息保护制度的具体内容见 5.6 节“《个人信息保护法》框架和重点内容”。

1.2 网络安全保护制度的内在关系

搞清网络安全等级保护制度、关键信息基础设施安全保护制度和数据安全保护制度的内在关系非常重要，涉及开展网络安全工作的具体实践中如何进行统筹规划、顶层设计、方案制定和组织落实。在网络安全保护环节，个人信息纳入数据安全保护范畴，因此，这里只介绍上述三个制度的关系。

1.2.1 三个制度的关系是一个基础、两个重点

（1）《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，该制度是网络安全的基本制度、基本国策、基本方法，是网络与数据安全的基础。

（2）《网络安全法》第三十一条和《关键信息基础设施安全保护条例》第六条规定，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。

（3）《数据安全法》第二十七条规定，利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行数据安全保护义务。

由此可见，法律明确规定了三个制度的关系，即网络安全等级保护制度是基础，关键信息基础设施安全保护制度和数据安全保护制度是重点。《关键信息基础设施安全保护条例》和《数据安全法》将网络安全等级保护制度延伸到关键信息基础设施安全保护领域和数据安全保护领域，并将网络安全等级保护制度作为二者的基础。国家从法律层面确定了三个制度之间的关系，因此，在网络安全政策层面、标准层面，对三个制度应依据法律规定进行有效衔接，协调落实。

1.2.2 建立科学的网络安全保护制度体系

网络安全保护制度体系如图 1-1 所示。若要建立科学的网络安全保护制度体系，一是从图中的纵向看，每个制度的建立需要在法律、政策、标准等三个层面协调一致；二是从图中的横向看，三个制度间需要分别在法律、政策、标准等层面协调一致。

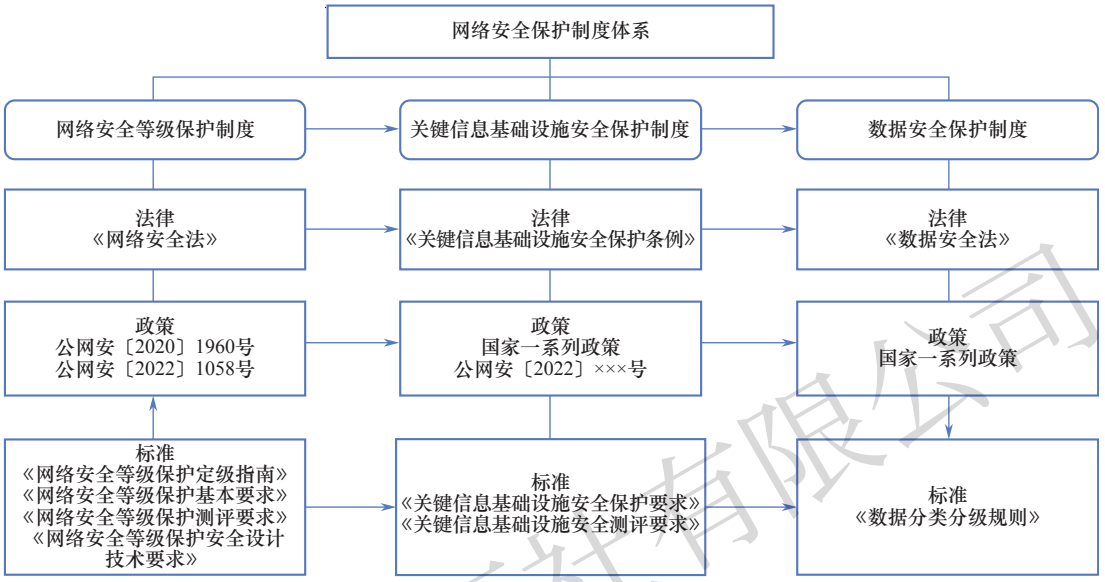

图 1-1　网络安全保护制度体系

1. 建立科学的网络安全等级保护制度

我国建立了比较完备的、科学的网络安全等级保护制度，该制度在法律、政策、标准等层面协调一致，有机衔接。

（1）《网络安全法》等法律法规以及中央政策文件对网络安全等级保护制度作出了明确规定，提出了明确要求。

（2）公安部依据法律规定和中央政策要求，出台了与法律法规和中央政策有机衔接的一系列网络安全等级保护政策文件，例如《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960 号）和《关于落实网络安全保护重点措施 深入实施网络安全等级保护制度的指导意见》（公网安〔2022〕1058 号）等，有力支撑了网络安全等级保护制度的实施。

（3）在法律、政策的指引下，国家出台了与法律、政策有机衔接的国家标准、行业标准，例如《信息安全技术 网络安全等级保护定级指南》《信息安全技术 网络安全等级保护基本要求》《信息安全技术 网络安全等级保护测评要求》《信息安全技术 网络安全等级保护安全设计技术要求》《信息安全技术 网络安全等级保护测评过程指南》《信息安全技术 网络安全等级保护实施指南》（以下省略“信息安全技术”等前缀）等。由此，形成了科学的网络安全等级保护制度。

2. 建立科学的关键信息基础设施安全保护制度

关键信息基础设施是网络安全保护的重中之重，建立科学的关键信息基础设施安全保护制度是网络安全领域的重要任务之一。从国家层面，一是出台了《关键信息基础设施安全保护条例》；二是出台了有关政策文件，公安部也出台了有关加强关键信息基础设施安全保护的政策文件（鉴于文件涉密，不能公开）；三是出台了《关键信息基础设施安全保

护要求》国家标准。但是，关键信息基础设施安全保护标准体系尚未建立。因此，需要加快制定与法律政策相衔接、与网络安全等级保护国家标准协调一致的关键信息基础设施安全保护国家标准、行业标准，形成在法律、政策、标准等层面协调一致的关键信息基础设施安全保护制度。

3. 建立科学的数据安全保护制度

重要数据与关键信息基础设施一样，都是网络安全保护的重中之重，建立科学的数据安全保护制度也是网络安全领域的重要任务之一。国家出台了《数据安全法》，中央出台了有关加强数据安全保护的政策文件，但是，数据安全保护标准体系尚未建立。因此，需要建立与法律政策相衔接的、与网络安全等级保护国家标准协调一致的数据安全保护标准体系，加快建立科学的数据安全保护制度。

1.2.3　三个制度应从法律、政策、标准三个层面有机衔接和协调一致

网络安全等级保护制度、关键信息基础设施安全保护制度、数据安全保护制度应从法律、政策、标准三个层面有机衔接、协调一致，才能建立科学的网络安全保护制度体系。

（1）三个制度已从法律层面有机衔接、协调一致。法律确定了三个制度的关系，即网络安全等级保护制度是基础，关键信息基础设施安全保护制度、数据安全保护制度在网络安全等级保护制度基础上实施。法律确定了三个制度的关系后，有关部门需要依法制定相应政策和标准，便于全社会遵守和实施三个重要制度。

（2）三个制度在政策层面需要有机衔接、协调一致。由于法律法规对三个制度的关系做出了明确规定，政策方面必然要依据法律要求，协调一致、有机衔接。一是国家出台的关键信息基础设施安全保护政策、数据安全保护政策与网络安全等级保护政策进行了有机衔接；二是公安部出台的关键信息基础设施安全保护政策与网络安全等级保护政策进行了有机衔接。有关部门在按照职责分工，出台数据安全保护有关政策文件时，也应与网络安全等级保护政策有机衔接、协调一致。

（3）三个制度在标准层面需要有机衔接、协调一致。由于法律、政策对三个制度的关系做出了明确规定，因此，三个制度在标准方面必然要依据法律、政策要求，有机衔接、协调一致。一是国家出台的《网络安全等级保护定级指南》《网络安全等级保护基本要求》《网络安全等级保护测评要求》《网络安全等级保护安全设计技术要求》《网络安全等级保护实施指南》等一系列标准，体系化强，经过多年检验和实践，证明是科学实用的。二是关键信息基础设施安全保护方面，出台了《关键信息基础设施安全保护要求》等国家标准，数据安全方面出台了《数据分类分级规则》等国家标准，这两个制度方面的标准，需要科学制定，与网络安全等级保护标准有机衔接、协调一致，才能将法律规定的网络安全三个重要制度建立好并落到实处。

（4）在落实三个制度的具体措施方面需要有机衔接、协调一致。一是重要行业主管部门、重点单位在制定行业网络安全规划、管理办法、实施方案等的过程中，应将三个制

度的要求相结合。二是在安全防护、安全监测、通报预警、事件处置、检测评估、技术对抗、威胁情报等具体工作中，需要结合网络安全等级保护要求、关键信息基础设施安全保护要求、数据安全保护要求去设计和实施。三是在人才培养、经费保障、工程建设、技术攻关等保障方面，需要结合网络安全等级保护要求、关键信息基础设施安全保护要求、数据安全保护要求去设计和实施。

1.2.4 协调落实网络安全等级保护制度与关键信息基础设施安全保护制度

网络安全等级保护制度和关键信息基础设施安全保护制度是《网络安全法》和《关键信息基础设施安全保护条例》确定的基本制度和重要制度，二者关系密切，确保这两个制度科学、协调落实至关重要。为此，要深入贯彻落实网络安全等级保护制度，建立良好的网络安全保护生态，筑牢网络安全根基；建立并实施关键信息基础设施安全保护制度，突出保护重点，大力加强关键信息基础设施安全保卫、保护和保障，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力应对网络战威胁，有效处置网络安全事件，严厉打击危害网络安全的违法犯罪活动，切实保障国家网络空间主权、国家安全和社会公共利益。

1. 网络安全等级保护制度与关键信息基础设施安全保护制度的法定关系

《网络安全法》规定，国家实行网络安全等级保护制度，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。法律规定了网络安全等级保护是关键信息基础设施安全保护的基础，开展网络安全等级保护工作是开展关键信息基础设施安全保护工作的前提和重要保障。

2. 协调一致地落实网络安全等级保护制度和关键信息基础设施安全保护制度

国家基本建立了网络安全等级保护制度体系，包括组织领导体系、法律体系、政策体系、标准体系、技术支撑体系、保护体系、人才队伍体系、教育训练体系和保障体系，网络安全等级保护制度得到进一步落实。关键信息基础设施安全保护制度是国家网络安全工作的新制度，建立关键信息基础设施安全保护制度体系，包括法律体系、政策体系、标准体系、保护体系、保卫体系和保障体系，才能确保将关键信息基础设施安全保护制度落到实处。在贯彻实施网络安全等级保护制度和关键信息基础设施安全保护制度过程中，从制定出台法律法规、政策，研究制定标准，采取重要措施等方面，两个制度应保持协调一致、有机衔接，以体现法律对两个制度的定位和要求。

3. 落实网络安全等级保护制度和关键信息基础设施安全保护制度有不同的侧重点

网络安全等级保护制度是国家网络安全的基本制度、基本国策，具有普适性和全覆盖性，全社会都要按照网络安全等级保护制度要求开展网络安全保护工作。同时，网络安全等级保护制度侧重于将保护对象分等级进行保护，不同等级的保护对象采取不同的保护措施和保护强度；关键信息基础设施安全保护制度是国家网络安全重点保护制度，强调对关键信息基础设施安全的保卫、保护和保障。在保卫方面，体现在针对危害关键信息基础设施的

违法犯罪活动，公安机关、国家安全机关等部门大力开展侦查打击，加强对关键信息基础设施的安全保卫；在保护方面，体现在对关键信息基础设施在满足网络安全等级保护基本要求、基线要求、合规要求的基础上，采取先进技术和重要措施加强保护；在保障方面，体现在发改、财政、教育、编制、科技等部门，在工程项目、经费、人才培养、机构编制、科研等方面对关键信息基础设施安全保护提供充足保障。

4. 落实网络安全等级保护制度和关键信息基础设施安全保护制度的总体要求

（1）深入贯彻实施网络安全等级保护制度。深入推进网络安全等级保护定级备案、等级测评、安全建设和检查等基础工作，有效落实网络安全保护“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，建立良好的网络安全保护生态，有力提升国家网络安全综合防护能力和水平。

（2）建立实施关键信息基础设施安全保护制度。掌握关键信息基础设施基本情况，做到底数清、情况明，健全安全保护机构，明确职责任务，强化各项保障。在贯彻落实网络安全等级保护制度的基础上，有效落实关键信息基础设施的关键岗位人员管理、供应链安全、数据安全、应急处置等重点安全保护措施，大力提升关键信息基础设施安全防护能力。

（3）提升网络安全监测预警和应急处置能力。建立跨行业、跨部门、跨地区的网络安全监测体系，建设应用网络安全综合保护平台，提升网络安全态势感知、通报预警和事件发现处置能力。制定科学的网络安全预案，完善应急处置机制，开展常态化应急演练，有效防范、遏制和处置网络安全重大事件。

（4）建立网络安全综合防控体系。健全完善网络安全保护工作机制，形成党委统筹领导、各部门分工负责、社会力量多方参与的网络安全工作格局。有效落实网络安全责任制，构建“打防管控”一体化的网络安全综合防控体系，提升网络安全管理防范、监督指导和侦查打击等能力。

1.3 落实网络安全保护制度的基本策略和重要措施

1.3.1 落实网络安全保护制度的基本策略

1. 依法进行保护，落实各方责任义务

以总体国家安全观为统领，认真贯彻实施网络强国战略，全面加强网络安全工作统筹规划和顶层设计，深入贯彻落实网络安全和数据安全的法律法规以及各项制度要求，依法落实网络安全职能部门的监管责任、行业主管（含监管，下同）部门的主管责任、网络运营者的主体责任、网络安全服务提供者的服务责任。

2. 坚持问题导向、实战引领、体系化防御

树立新理念，聚焦突出问题和薄弱环节，从网络安全、关键信息基础设施安全、数据安全、人工智能安全等方面，构建在制度、管理和技术等方面有机衔接的网络安全综合

防控体系和安全治理体系。防范和遏制重大网络安全风险、事件发生，保护云计算、物联网、新型互联网、工业控制系统、大数据、智能制造等新技术应用和新业态安全。

3. 坚持底线思维和极限思维，树立一盘棋思想

实时审视国际国内网络安全大局，立足有效应对大规模网络攻击，加强技术攻关和自主可控，以保护关键信息基础设施、重要网络和数据安全为重点，采取超常规举措，全面加强网络安全防范管理、监测预警、应急处置、侦查打击、威胁情报、检测评估、技术对抗等各项工作，切实提升技术对抗能力，守住关键，保住要害。

4. 坚持积极防御、综合防护

按照法律法规和有关国家标准规范，充分利用人工智能、大数据分析等技术，积极落实网络安全管理和技术防范措施，及时监测处置网络安全风险、威胁和网络安全突发事件，提升应对突发事件能力，保护关键信息基础设施、重要网络和数据免受攻击、侵入、干扰和破坏，切实维护国家网络空间主权、国家安全和社会公共利益，保护人民群众的合法权益，保障和促进经济社会健康发展。

5. 坚持综合保障，形成合力

坚持发展和安全并重，在安全和发展中寻找平衡点，建立可信可控的网络和数据安全屏障。在机构、人员、经费、装备、工程、科研、教育训练等方面加大投入，促进网络安全产业发展，打造世界一流的网络安全企业，全力构建网络空间安全综合保障体系。

6. 加强战略谋划，提升综合实战能力

按照国家网络和数据安全法律法规、政策文件和标准要求，根据我国多年网络安全实践经验，坚持“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，从网络安全保卫、保护、保障三个方面采取重要措施，大力提升网络安全综合实战能力。

1.3.2 采取网络安全保护措施，提升网络安全综合防御能力

（1）建立领导体系和工作体系。落实《党委（党组）网络安全工作责任制实施办法》，设立网络安全领导机构、管理机构和专职人员；建立决策机制，保障人力、财力、物力投入。

（2）开展顶层设计和规划。制定行业网络安全管理办法、标准规范、安全保护规划、年度计划，经专家评审后实施。

（3）落实行业主管责任。行业主管部门加强对本行业网络安全工作的组织领导、监督检查，督办整改；横向到边、纵向到底。

（4）落实网络运营者的主体责任。按照法律法规和有关制度要求，落实网络安全责任和各项任务要求，守土有责、守土尽责。

（5）落实网络安全等级保护制度。按照《网络安全法》要求和国家标准规范，坚持分

等级保护、分等级监管，保障各级网络系统的安全合规，筑牢网络安全基石。

（6）落实关键信息基础设施安全保护制度。按照《网络安全法》《关键信息基础设施安全保护条例》等法律法规要求，制定关键信息基础设施识别认定规则，确定关键信息基础设施，加强安全保卫、保护和保障。

（7）落实数据安全保护制度。按照《网络安全法》《数据安全法》等法律法规要求，建立数据分类分级制度、安全保护制度等一系列制度，加强重要数据安全保护。

（8）落实密码安全防护要求。落实《中华人民共和国密码法》（以下简称《密码法》）《商用密码管理条例》和密码应用相关标准规范，使用符合规定的密码技术、密码产品和服务，提高技术保护能力。

（9）开展安全检测和风险评估。将隐患识别、威胁分析、等级测评、风险评估、密码安全性检测评估等统筹安排，开展网络安全检测和风险评估，有效管控风险威胁。

（10）制定网络安全建设整改方案并实施。根据安全检测评估、风险分析、事件分析、实战检验等发现的问题、隐患，以应对大规模网络攻击为目标，制定安全建设整改方案并实施。

（11）采取多种方式检验保护措施的有效性。开展网络攻防演习、沙盘推演，聘请专门安全检测机构，远程渗透测试与现场检测相结合，对关键信息基础设施和重要网络系统进行全流程、全方位检测评估。

（12）落实实时监测预警措施。利用网络安全保护平台和技术措施，开展实时监测预警，大力提高监测发现网络攻击的能力。

（13）落实物理设施保护和电力电信保障措施。保护机房、大数据中心、云计算平台等物理设施安全，严防地震、洪灾等破坏，保障网络运行正常、数据免遭破坏。

（14）落实“三化六防”措施。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”措施，提升整体防控能力。

（15）实施“挂图作战”。建设网络安全保护平台和态势感知系统，建设平台智慧大脑，绘制网络地图，实现“挂图作战”。

（16）落实信息通报措施。依托国家网络与信息安全信息通报机制，加强各行业、各领域网络安全信息通报预警机制建设和力量保障，提升信息通报预警能力。

（17）落实责任追究制度。制定网络安全责任制管理办法和问责规范，健全完善网络安全考核评价和责任追究制度，确定问责范围，明确约谈、罚款、行政警告、记过、降级、开除等处罚措施。

（18）落实指挥调度措施。重点行业、网络运营者要建设网络安全监控指挥中心，落实 7×24 小时值班值守制度，提升网络安全指挥调度能力。

（19）落实事件处置机制。制定网络安全事件应急预案，加强应急力量建设和应急资源储备，与公安机关密切配合，建立事件报告制度和应急处置机制。

（20）定期进行“排雷”行动。针对渗透攻击、预埋木马和逻辑炸弹、开后门、网络控制权被剥夺等重大网络安全问题隐患，通过“探雷、固证、排雷、整改”等措施，及时

发现攻击，消除重大风险隐患，封堵攻击通道，有效提升网络安全防范能力水平。

（21）落实协同联动措施。建立协同联动、信息共享与会商决策机制，在机构的业务应用、系统建设、技术实施、运营运维、综合管理等部门间建立内部机制；与保护工作部门、行业内上下级单位、直属机构建立纵向配合机制；与公安机关、横向合作单位、技术支撑机构建立横向机制，形成一体化联合工作机制。

（22）落实技术对抗措施。在网络关键节点架设监测设备和蜜罐、沙箱等设备，诱捕和溯源网络攻击，构建以密码、可信计算、人工智能、大数据分析技术为核心的网络安全技术保护体系。

1.3.3 采取网络安全保卫措施，提升网络安全“打防管控”能力

（1）开展联合作战。公安机关与重要行业主管部门、企业等社会力量密切配合，建立网络安全联合作战机制，立足网络备战，打整体仗、合成仗。

（2）落实威胁情报措施。大力加强威胁情报工作，建立完善情报信息共享机制，利用威胁情报引领网络安全“打防管控”综合防控体系建设。

（3）开展网络安全执法检查。各级公安机关的人民警察，应依据《中华人民共和国人民警察法》（以下简称《人民警察法》）、《网络安全法》、《数据安全法》、《关键信息基础设施安全保护条例》等法律法规，对重点单位开展网络安全执法检查。

（4）严厉打击网络违法犯罪活动。利用事件处置、安全监测、安全检测、攻防演习、扫雷等手段，及时搜集发现危害网络和数据安全的违法犯罪线索，及时开展调查取证、追踪溯源，严厉打击危害关键信息基础设施、重要网络系统和重要数据安全的违法犯罪活动。

（5）开展比武竞赛。建设网络靶场，设立红、蓝军，组织开展网络攻防演练、比武竞赛和技术对抗，大力提升对抗反制能力。

1.3.4 采取网络安全保障措施，提升网络安全综合保障能力

（1）落实供应链安全措施。在网络的规划设计、建设、运维、服务等各环节中，加强对网络服务商和产品供应商的安全管理，防范供应链安全风险。加强互联网远程运维安全评估论证，并采取相应的管控措施。

（2）开展技术攻关。按照“理论支撑技术、技术支撑实战”的理念，开展理论研究和技术攻关，研究网络空间智能认知、资产测绘、画像与定位、可视化表达、地理图谱构建、行为认知和智能挖掘等核心技术，支撑网络安全实战。

（3）实施自主可控和技术创新工程。梳理排查网络系统中使用的国外产品和服务；加强算法的审核、运用和监督；制定国产化替代方案，在有关部门支持下，从基础软硬件、业务系统和网络安全产品等方面，逐步实现国产化替代。

（4）落实各项保障。加强统筹领导和保障，研究解决网络安全机构编制、人员、经

费、科研、工程建设等各项保障，特别要保障设备设施的改造升级经费。

（5）落实网络安全审查要求。落实 2021 年 12 月国家互联网信息办公室（以下简称国家网信办）、公安部等十三部门联合修订发布的《网络安全审查办法》。

（6）培养攻防兼备的专门队伍。建立教育训练和实战型人才发现、培养、选拔与使用机制，培养攻防兼备的人才队伍。

（7）开展网络安全保险。借鉴发达国家经验，在网络与数据安全领域引入保险机制，提高网络与数据安全风险治理能力。加强顶层设计，研究网络与数据安全保险法律、政策、标准规范，共同培育市场，试点先行，支持保险机构构建“保险 + 风险管控 + 服务”模式。

（8）实施“一带一路”网络安全战略。有关部门研究出台政策、标准规范，支持国有企业与网络安全企业走出去，让“一带一路”国家共享中国网络安全等级保护经验，同时，保护中国企业在海外的网络基础设施和数据安全，保护企业生产业务安全，保护国家的海外利益。

（9）开展人工智能安全治理。研究出台保障人工智能健康发展应用的法律、政策和标准规范，加强伦理、社会问题研究，从算法安全、数据安全、伦理安全、国家安全等维度综合研究施策，提升人工智能安全治理能力。

1.3.5　按照“理论支撑技术、技术支撑实战”理念提升网络安全综合能力

由于职责不同，高等院校、科研机构侧重于研究网络安全理论和技术，网络安全企业侧重于研究网络安全技术、产品和服务，公安机关等部门侧重于研究网络安全实战。而在网络安全的实际工作中，需要将网络安全的理论、技术和实战紧密结合起来，实战需要技术支撑，技术需要理论支撑，因此，应按照“理论支撑技术、技术支撑实战”的理念，将网络安全的理论、技术和实战密切关联，形成一个有机整体，理论研究、技术攻关最终要用于支撑实战，实现提升网络安全综合能力的目的。

1.“理论支撑技术、技术支撑实战”的总体思路

“理论支撑技术、技术支撑实战”的总体思路如图 1-2 所示。

（1）开展理论研究。按照“理论支撑技术、技术支撑实战”的理念，将地理学、网络安全学、计算机科学、人工智能技术理论等有机结合，建设交叉学科——网络空间地理学。特别是用地理学的理论、技术和重大成果，指导研究网络空间安全。研究网络空间安全图谱要素分类、代码和图形符号表达，网络空间地理图谱理论和网络空间智能认知方法体系，形成网络空间地理学基础理论。

（2）开展核心技术攻关。在理论指导下，开展技术攻关，研究突破网络空间安全图谱要素生成技术、地理环境要素获取与处理技术、地理空间和网络空间资产测绘技术、网络空间地理图谱构建技术、网络空间可视化表达技术、网络空间行为的智能认知技术、网络空间及地理空间现象的时空模拟技术，以支撑实战需求。

（3）实施“挂图作战”。利用核心技术支撑实战，构建网络空间安全图谱，将安全防

护、安全监测、通报预警、态势感知、检测评估、应急指挥、事件处置、威胁情报、侦查打击、技术对抗上图，建立网络空间安全综合防控体系，实施“挂图作战”。

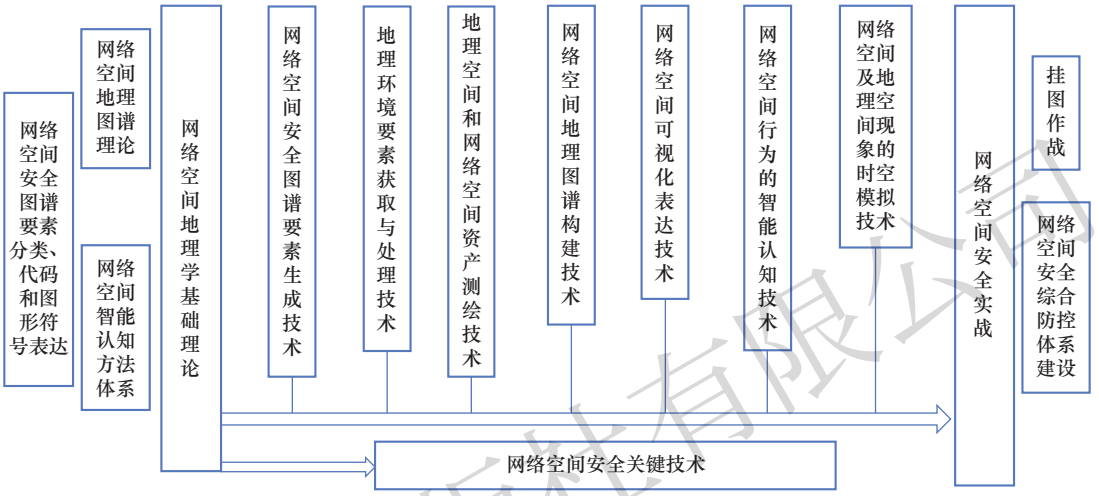

图 1-2 “理论支撑技术、技术支撑实战”的总体思路

2. 建立网络空间安全图谱，支撑“挂图作战”的路线图

建立网络空间安全图谱，支撑“挂图作战”的路线图，如图 1-3 所示。

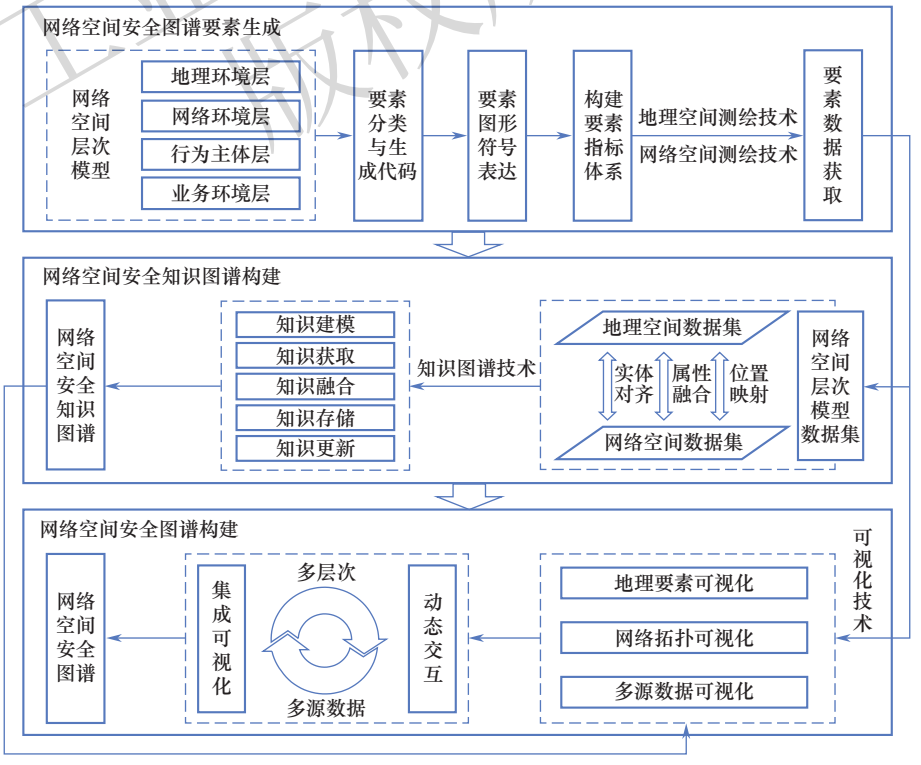

图 1-3 路线图

（1）建立网络空间层次模型，以网络空间安全图谱要素分类、代码和图形符号表达为基础，构建要素指标体系，利用网络空间测绘技术，获取要素的多源数据，生成网络空间安全图谱要素。

（2）基于知识图谱技术，分析网络空间安全大数据，对多源数据进行关联融合，形成语义网络，构建网络空间安全知识图谱。

（3）以知识图谱为基础，利用人工智能技术和可视化技术，将地理要素、网络拓扑、多源数据可视化，通过动态交互和集成可视化，构建网络空间安全图谱。

习　题

1. 我国网络安全保护制度体系主要包括哪些制度？

2. 什么是网络安全等级保护制度？《网络安全法》中的哪条对网络安全等级保护制度做出了规定？如何规定的？

3. 什么是网络安全等级保护工作？

4. 什么是关键信息基础设施？

5. 关键信息基础设施安全保护制度的主要内容是什么？

6. 数据安全保护制度的主要内容是什么？

7. 个人信息保护制度的主要内容是什么？

8. 网络安全等级保护制度与关键信息基础设施安全保护制度和数据安全保护制度的内在关系是什么？

9. 落实网络安全保护制度的基本策略是什么？

10. 落实网络安全保护制度的保卫、保护、保障措施有哪些？