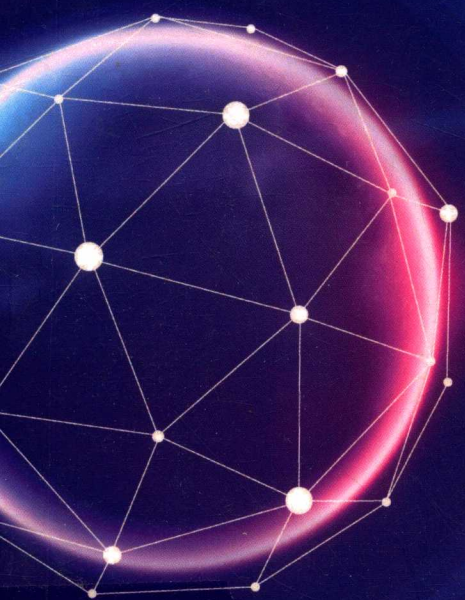
普通高等教育网络空间安全系列规划教材

网络空间安全系统科学与工程

闫怀志◎编著



科学出版社

普通高等教育网络空间安全系列规划教材

网络空间安全系统科学与工程

闫怀志　编著

科学出版社
北京

内 容 简 介

本书主要论述网络空间安全及其保障体系构建的系统科学与工程问题，内容包括网络空间安全系统科学与工程绪论，系统论、信息论、控制论、耗散结构理论、协同论、突变论以及复杂系统等理论及其在网络空间安全中的应用，霍尔结构、综合集成、MBSE 等系统工程方法、体系工程及其在网络空间安全中的应用，定性、定量、定性与定量相结合的安全分析、评估与决策方法，基于系统科学与工程的网络空间安全保障技术体系与管理体系构建方法。最后给出了大型信息系统安全保障系统工程实践过程实例。本书是作者长期从事相关领域科研与教学成果的高度凝练和系统总结，并融合了本领域的最新理论与技术。

本书可作为高等院校网络空间安全类、系统工程类、计算机类等专业高年级本科生和研究生教材，也可作为相关专业人员的参考书。

图书在版编目(CIP)数据

网络空间安全系统科学与工程 / 闫怀志编著. — 北京：科学出版社，2019.6

普通高等教育网络空间安全系列规划教材

ISBN 978-7-03-061028-7

Ⅰ. ①网… Ⅱ. ①闫… Ⅲ. ①计算机网络-网络安全-高等学校-教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2019)第 068979 号

责任编辑：潘斯斯 刘 博 董素芹 / 责任校对：郭瑞芝
责任印制：张 伟 / 封面设计：迷底书装

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京虎彩文化传播有限公司 印刷

科学出版社发行 各地新华书店经销

*

2019 年 6 月第 一 版 开本：787×1092 1/16
2019 年 6 月第一次印刷 印张：16 1/4
字数：400 000

定价：68.00 元

(如有印装质量问题，我社负责调换)

前　言

网络空间是人类自然与社会以及国家的公域空间，已成为人类除陆、海、空、天之外的第五维活动空间，具有全球空间的性质。因此，网络空间安全(Cyberspace Security)及其保障体系构建成为了一个复杂的系统问题。构建网络空间信息系统的安全保障体系，首先要认知网络空间安全，认知的手段和方法至关重要。德国著名物理学家普朗克指出，科学是内在的统一整体，它被分解为单独的“个体”不是源自事物本身，而是源自人类认识能力的局限。网络空间安全领域也是如此。

随着研究的不断深入，人们逐渐认识到网络空间安全问题需要采用系统科学与系统工程的方法来解决。系统科学理论和系统工程方法论当之无愧地成为了网络空间安全的重要理论基础。考察网络空间安全的概念及其相关联系，既离不开信息论、系统论和控制论等系统科学经典理论(老三论)和耗散结构论、协同论、突变论(新三论)以及复杂系统与复杂网络等新兴理论，也需要运用系统工程和体系工程等思想和方法来解决工程实践问题。而实施网络空间安全系统工程，又离不开安全分析、评估与决策方法。不难看出，网络空间安全系统科学与工程，具有鲜明的多学科交叉融合、理论与实践高度结合等特点。

近年来，作者在国家重点研发计划(2016YFB0800700、2016YFC1000301)的支持下，持续开展了网络空间安全系统科学与工程领域的科学研究和工程实践，并为研究生和高年级本科生开设了相关课程，北京理工大学“十三五”规划专项也给予了大力支持。全书的主要架构和很多思想源自作者在承担相关领域国家级、省部级和企业课题中的理论和实践探索。本书还参考了国内外该领域的最新研究成果，力图反映最新的理论和技术方法。全书以系统科学和工程的理论和方法为指导，围绕系统科学理论与系统工程方法、网络空间安全保障体系构建两条主线，分 7 章论述网络空间安全保障体系构建中的系统科学与工程问题。

第 1 章绪论部分主要讨论网络空间安全系统科学与工程的基本问题，主要包括：网络空间安全概述(网络空间、信息安全、网络空间安全)；系统科学与系统工程(系统与整体性、系统科学与系统工程概述及其研究对象、内容与方法)；系统科学与系统工程视角下的网络空间安全等。

第 2 章主要论述系统论、信息论与控制论及其在网络空间安全中的应用，主要包括：系统论与网络空间安全(还原论与整体论的思想、方法及其历史贡献与历史局限，系统论的提出及其发展，系统概念的内涵和外延及其辩证分析，线性动态系统与非线性动态系统，开放系统、孤立系统与封闭系统，整体性、关联性、层次性、统一性、目的性、动态开放性以及自组织原理，结构功能相关、信息反馈、竞争协同、涨落有序以及优化演化等基本规律，系统论在网络空间安全宏观、中观、微观层面的应用)；信息论与网络空间安全(信息论的基本思想及其发展，信息的概念、特征及传输模型及度量，香农三大定理，信息论在密码学、数据压缩、信息隐藏、隐私保护以及可认证性、可信性和完整性保护中的应用)；控制论与网络空间安全(控制论的提出及其发展，控制论的科学思维与方法，经典控制理论、现代控制理论以

及大系统理论与智能控制的基本思想与分析方法，控制论在网络空间安全控制、攻防对抗、动态防御和主动防御中的应用等)。

第 3 章讨论耗散结构理论、协同论与突变论及其在网络空间安全中的应用，主要包括：耗散结构理论、协同论、突变论的基本思想及其发展、基本概念与方法，及其在网络空间安全中的应用。同时还讨论了复杂系统理论、复杂适应系统理论、复杂网络理论的概念、基本思想、模型，及其在网络空间安全中的应用。

第 4 章系统工程与体系工程方法及其在网络空间安全中的应用部分，主要分析霍尔三维结构方法论、切克兰德方法论、综合集成方法论、MBSE 方法论以及体系工程方法论，以及上述方法在网络空间安全领域的典型应用分析和示例。

第 5 章讨论了网络空间安全系统分析、评估与决策方法，主要内容有：定性与定量问题的研究方法与途径；定性方法(逻辑分析法、德尔菲法主要步骤及其应用)；定量方法(主成分分析法、因子分析法、聚类分析法、时间序列模型分析法、回归分析法、决策树分析法的基本思想与基本步骤)；定性与定量相结合的方法(层次分析法 AHP、网络分析法 ANP、模糊综合评价法、灰色综合分析法、数据包络分析法、神经网络分析法和深度学习分析法的基本思想、基本步骤和应用领域等)。

第 6 章阐述了基于系统科学与工程的网络空间安全保障体系构建方法，主要包括：信息系统安全保障系统工程(安全保障系统工程过程，信息系统安全保障体系总体、技术保障体系、管理保障体系的设计，信息系统安全保障体系测评)；安全技术体系与管理体系通用框架(通用安全保护能力、对象、等级与要求，云计算平台、移动互联网络、物联网、工业控制系统及工业互联网的功能架构、安全威胁及安全防护架构)；安全技术体系构建(技术体系架构与总体技术要求，物理和环境、网络和通信、设备和计算、应用和数据的问题及技术措施)；安全管理体系构建(管理体系架构与总体管理要求，安全策略和管理制度，安全管理机构和人员，安全建设及运维管理等)；基于系统工程的网络空间安全整体防护能力形成(纵深防御体系的构建，安全技术与管理措施的协调、互补与融合，OODA 循环在网络空间安全攻防对抗中的应用等)。

第 7 章以人类遗传资源数据管理服务系统为例，介绍了大型网络信息系统安全保障系统工程实践过程，主要包括：系统安全保障需求；安全保障技术体系设计与实施(安全域划分及边界确定，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、数据共享安全与隐私保护的设计与实施，云支撑平台安全防护功能设计、安全管理中心设计与部署、安全设备和产品选型与部署等)；安全保障管理体系设计与实施(组织管理架构、安全策略体系的设计与实施，信息安全与隐私保护标准体系建设，系统安全管理及运维服务)；系统安全测试与评估(安全合规测评，云平台安全保障能力综合评估)等。

本书得到了北京大学、清华大学、上海交通大学、北京航空航天大学、北京理工大学、国家卫健委科学技术研究所、中国科学院信息工程研究所、中国航天系统科学与工程研究院、公安部第一研究所、中国电子科学研究院、中国人民解放军战略支援部队、军事科学院等单位同行专家的大力帮助。科学出版社对本书的出版给予了大力支持。同时，本书还参阅了大量的国内外专著、科研论文以及网络学术资源，在此一并致谢。

曾佳、闫振民、卢道英、边霞、曾永歧等参加了本书的文字处理、绘图等编写工作。

感谢家人在本书著述过程中的无私奉献、无限包容和大力支持。特别感谢各位校友和朋友在我最困难的时刻给予我的无私帮助。

为方便教学，本书随附提供参考教学大纲、教案、电子课件等辅助教学和学习资源。由于教材篇幅所限，与本书内容有关的大量背景知识、辅助内容及应用案例等将通过微信公众号(公众号名："网络空间安全系统科学与工程")提供。

由于相关领域的研究和应用正处于不断深入过程当中，加之作者水平有限，本书虽已尽力避免不足，难免仍有疏漏和错误，恳请广大读者将意见和建议发至 yhzhi@bit.edu.cn，作者不胜感激。

闫怀志

2019 年春于北京中关村

目　录

第1章 绪　论

本章将结合系统科学与系统工程原理来讨论网络空间安全系统科学与工程概念的基本范畴，具体包括网络空间，信息安全，网络空间安全，系统与复杂系统，系统科学与系统工程的研究对象、内容与方法，系统科学与系统工程视角下的网络空间安全等基本内容。

1.1 网络空间安全概述

1.1.1 网络空间

人们最熟悉的空间概念来自物理空间。物理空间大多通过长度、宽度、高度等维度来表现，用来描述物体及其运动的位置、形状、方向等物理性质。物理空间是与时间相对的一种物质客观存在形式，是三维的，可以容纳物质存在与运动，也可以称为“具体空间”。与此相对应，还存在“一般空间”。“一般空间”是概念性空间，是抽象的、不可见的多维特征空间，它没有具体的长、宽、高的维度限制，也没有具体数量规定。数学空间则是物理空间概念的延伸和抽象。随着人类认知的发展，又出现了思想空间、宇宙空间、信息空间与网络空间等概念。

网络空间概念的形成，经历了较长的发展历程。20 世纪中叶以来，计算机与现代通信技术相互融合形成的互联网飞速发展，使人类对“一般空间”的认识，又增加了全新的技术特点和时代特征。20 世纪 70 年代中期问世的信息网络飞速扩张，构筑了承载政治、军事、经济、文化的全新空间，即网络空间(Cyberspace)。Cyberspace 原是哲学与计算机网络领域中的一个抽象概念，1982 年由美籍科幻作家威廉·吉布森(William Gibson)首创，由 Cybernetics(控制论)和 Space(空间)组合而得。Cyberspace 也常译为赛博空间、多维信息空间，军事应用中又称网电空间。

20 世纪末，国际学术界认为 Cyberspace 与因特网基本同义，随后，又将对其的认识扩展为“基于计算机、现代通信网络以及虚拟现实等信息技术的综合运用，以知识和信息为内容的新型空间”，认为它是人类运用知识创造的一种人工世界，而且是适用于知识交流的虚拟空间。

20 世纪以来，国际上对网络空间的认知继续深化，完成了对网络空间从抽象到具体，从单纯虚拟空间到“物理、信息、认识、社会”多维空间的认识转变。

当前，人们普遍认为，网络空间是以自然电磁能为载体，以功能、互联程度、技术复杂性以及脆弱性各不相同的人造异构网络化系统及相关的物理基础设施为平台，通过网络将信息渗透、充斥到陆、海、空、天实体空间，依托电磁信号传递、存储、处理和利用无形信息，通过协议、接口以及基础设施的标准化来实现不同分系统之间的信息交换，并经由信息控制实体行为，从而构成实体层、电磁层、虚拟层深度融合、相互贯通的，无所不在、无所不控、虚实结合、多域融合的复杂空间。网络空间的本质要素是信息、信息承载主体——信息系统以及信息环境。

具体到工程技术领域，网络空间中的信息系统，既可以指全球范围的 Internet 系统、通信基础设施等一般称作网络的信息系统，也可指有具体范围的电子信息环境，如政府、企业、军事等机构或组织的信息系统，还包括与网络空间有关的、影响重要基础设施的公共电话网、电力网、石化系统、金融、交通、广电、军事和其他政府信息系统等。网络空间的关键信息基础设施主要包括以下内容：提供公共通信、广播电视传输等服务的基础信息网络；公共服务领域的重要信息系统；军事网络；国家机关等政务网络；用户数量众多的网络服务提供者所有或管理的网络和系统。

由此可以看出，网络空间作为客观存在的人造空间，较之作为物质载体或物质运动形式的现实物理空间和传统的 IP 网络，呈现出以下新特点：①从计算机网络扩展到涉及陆、海、空、天等所有信息环境；②从计算机、网络设备扩展到使用各种芯片的嵌入式处理器和控制器；③从物理设施扩展到人的活动。这些特点，一方面体现了计算机、网络及应用的技术演变趋势；另一方面也反映出人们对网络空间内涵和外延认识的深化过程。

1.1.2　信息安全

1. 信息安全的发展历程与趋势

信息安全问题古已有之，最原始的安全问题涉及隐写术和古典密码学，尤以军事领域的应用为盛。中国古代的矾书采用明矾水书写，水干无迹、湿时方显，具备信息隐藏术的技术特征。古代西方军队也使用了很多保密通信技术，如公元前 5 世纪古希腊的斯巴达密码棒(Scytale)以及后来出现的恺撒(Kaiser)密码都是古典密码学的经典应用。虽然古代已经出现了以隐写术和古典密码学为代表的信息安全概念的雏形，但是，现代意义上的信息安全概念则是发展、形成并完善于近代信息技术飞速发展之后。国际上通常将信息安全的发展划分为三个阶段：①信息保密阶段(20 世纪初开始)；②信息保护阶段(20 世纪 80 年代开始)；③信息保障阶段(20 世纪 90 年代后期开始)。

信息的保密性(Confidentiality)是人类最先认识的安全要求，至今仍是信息安全的基础要求之一。最早的电话、电报通信安全主要是在信息交换环节，当时大多采用密码算法来实现加密传输，同时辅以访问控制和授权管理等手段。因此，这一阶段也被称为信息保密阶段。此阶段有四个里程碑式事件发生：①1949 年，美国数学家克劳德·香农(Claude Shannon)发表了《保密系统通信原理》(*Communication Theory of Secrecy Systems*)一文，标志着密码学变为一门应用科学；②1976 年，美国斯坦福大学教授迪菲(Diffie)和赫尔曼(Hellman)发表了《密码学的新方向》(*New Directions in Cryptography*)一文，标志着密码学发展到了公钥密码体制阶段，奠定了现代密码学的基础；③1977 年，美国国家标准局(NBS)采用了 IBM 研制的数据加密标准(DES)，标志着适用于计算机系统的商用密码体系的建立；④1983 年，美国国防部(DoD)公布了 TCSEC(可信计算机系统评价准则，俗称橘皮书)，标志着基于访问控制模型的可信信息系统等级化要求的形成以及计算机系统安全评估的第一个正式标准的建立。在这一阶段，人们充分认识到保密性是信息安全的一个基本要求，特别是 DES 和 TCSEC 的出现，更标志着以保密性为重点的信息安全研究及应用进入了新阶段。

后来，单纯的密码技术已无法满足计算机和网络系统的安全需求。人们对信息安全的关

注逐渐扩展到完整性(Integrity)和可用性(Availability)方面。这一阶段称为信息保护阶段，国际上出现了两个著名的标准：

(1)ITSEC(欧洲信息安全评价准则)。该标准由欧洲多国于 1991 年联合制定，分为功能需求与评估两部分，此标准最重要的贡献是将完整性、可用性与保密性视为同等重要的安全要求。

(2)CC(信息技术安全评价通用准则)。该标准由美国、加拿大、欧洲共同体等于 1993 年制定，分安全功能需求和安全保证需求两方面。CC 综合了美国 TCSEC、欧洲 ITSEC、加拿大 CTCPEC、美国 FC 等信息安全标准和指南，给出了一个更全面的信息技术安全性评估框架。

20 世纪末，网络信息技术飞速发展，信息安全不再局限于传统的保密性、完整性和可用性问题，人们使用信息与信息系统的身份和需要承担的责任成为必须考虑的重要问题，可认证性(Authenticity)、抗抵赖性(Non-repudiation)、可追溯性(Accountability)和可控性(Controllability)等安全性概念应运而生。因此，美国国防部于 20 世纪 90 年代提出了信息保障(IA)的概念，并得到了国际上的广泛认可，标志着信息安全进入了信息保障的新阶段。信息保障旨在保证信息系统能够安全运行，从整体角度来考虑信息安全保障体系建设，是信息安全适应信息时代的新发展。此阶段主要采用技术、管理等综合性手段，使信息以及处理、管理、存储、传输信息的信息系统具备保密性、完整性、可用性、可认证性、抗抵赖性、可追溯性等，并具备遭受攻击后的可恢复性，其核心是实现具备保护、检测、响应和恢复等能力的“深度防御”思想。信息保障阶段的标志性事件是 1998 年美国国家安全局(NSA)颁布的信息保障技术框架(IATF)V1.1。信息保障的内涵和外延十分丰富，一直有效地指导信息安全保障体系的建设，网络空间安全时代仍然处于信息保障阶段。

2. 信息安全的概念和基本要求

关于信息领域安全的定义，国际上有不同的版本，分别侧重于计算机安全、网络安全和信息安全。国际标准化组织(ISO)的定义侧重于计算机信息系统信息的静态保护。美国国家标准与技术研究所(NIST)的定义侧重于信息安全，尤其是其中对可用性的要求，暗含了对系统动态运行的安全保护要求。

本书采用如下定义：“信息安全是指对信息系统的硬件、软件及其数据信息实施安全防护，保证在意外事故或恶意攻击情况下系统不会遭到破坏、敏感数据信息不会被篡改和泄露，保护信息的保密性、完整性、可用性以及可认证性、抗抵赖性、可追溯性、可控性等，并保障系统能够连续可靠地正常运行，信息服务功能不中断。”这个定义，既强调了信息安全的防护对象——信息和信息系统，也强调了安全属性方面的具体要求，同时强调了对系统运行的动态防护。

前述定义中提到的保密性、完整性、可用性、可认证性、抗抵赖性、可追溯性以及可控性等，称为信息安全要求或信息安全属性。其中，保密性、完整性、可用性最为基础，是信息安全的基本要求，并称为信息安全 CIA 三要素。而可认证性、抗抵赖性、可追溯性以及可控性等则称为信息安全的扩展要求。对上述安全要求的任何破坏，都是对信息和信息系统安全的破坏，换言之，如果无法有效满足上述安全要求，那么该信息或信息系统就是不安全的。

1)保密性

保密性(机密性)是人们最先认识到的安全要求，它是指信息按给定要求不泄露给非授权(非法)的个人、实体或过程，或提供其利用的特性，即杜绝有用信息泄露给非授权个人或实体，强调有用信息只被授权(合法)对象使用的特征。保密性针对的是防止对信息进行未授权的“读”，其核心是通过各种技术和手段来控制信息资源开放的范围。

2)完整性

完整性是指网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等行为破坏和(或)丢失的特性，用以保证数据的一致性。简而言之，完整性是指信息未经授权不能进行改变。完整性要面对的是防止或者至少是检测出未授权的“写”(对数据的改变)，其核心是保证信息不被修改、不被破坏以及不丢失。完整性的破坏可能来自未授权、非预期、无意这三个方面的影响。也就是说，除了恶意破坏之外，还可能出现误操作以及没有预期到的系统误动作，它们也会对完整性产生影响。

3)可用性

可用性是在信息保护阶段针对信息安全提出的新要求，在网络空间也必须要满足。可用性用来保证合法用户对信息、信息系统和系统服务的使用不会被不正当地拒绝。攻击者通常会采取资源占用的方式来破坏可用性，使授权者的正常使用受到阻碍。信息和资源在授权主体需要时可以提供正常访问和服务，甚至在信息系统部分受损或需要降级使用时，仍能为授权用户提供有效服务。

4)可认证性

可认证性(真实性)是对技术保证和人的责任的总体要求，不能被完整性所取代。可认证性用来核实合法的传输行为、被传输消息或消息源的真实性，用来确保实体身份或信息、信息来源真实，即保证主体或资源确系其所声称的身份的特性，以建立对该主体或资源的信心。这里的实体是指用户、信息、进程或系统等。

5)抗抵赖性

抗抵赖性(不可否认性)是指信息交换双方(人、实体或进程)在交换过程中发、收信息的行为均不可抵赖，这是面向收、发双方的信息真实同一的安全要求，包括源发证明和交付证明，用来保证信息和信息系统的使用者无法否认其行为及其结果，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的企图得逞。源发证明为信息接收者提供证据，使得发送者谎称未发送过该信息或者否认其内容的企图无法得逞；交付证明则为信息发送者提供证明，使得接收者谎称未接收过该信息或者否认其内容的企图无法得逞。与完整性不同，抗抵赖性除了关注信息内容认证本身，还可以涵盖收发双方的身份认证。

6)可追溯性

可追溯性(可核查性、可确认性)是指确保某个实体的行动能唯一地追溯到该实体，即能够追究信息资源什么时候使用、谁在使用及如何操作使用等，表征实体对自己的动作和做出的决定负责。

7)可控性

可控性是指能够保证信息管理者掌握和控制信息与信息系统的基本情况，可对其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，保证能对传播的信息及内容实施必要的控制及管理，即对信息的传播及内容具有控制能力。

1.1.3 网络空间安全

网络空间安全是人类自然与社会以及国家的公域空间，已成为人类除陆、海、空、天之外的第五维空间，具有全球空间的性质。网络空间的固有特点，对其安全保障提出了新的挑战。

1. 网络空间的特点对安全提出的新挑战

1) 网络空间与物理空间和社会空间相互交融、渗透与控制

由于物理空间和社会空间等现实空间都可以向网络空间“投影”映射，网络已深度渗透到政治、经济、社会、军事等各方面管理当中，出现了崭新形态的网络政治、网络经济、网络文化、网络军事和网络外交等，网络空间中的信息能够连续地无缝突破和穿越政治、文化、宗教和地缘的各种界限，同时，该空间的基础设施软硬件研发、生产和应用也已经实现全球化，新的计算工具和通信手段的出现、新的信息系统的建立等都会扩展和延伸网络空间的边界。社会空间等现实空间不可避免地与网络空间领域紧密联系，并实现相互交融、相互渗透与相互控制。

2) 网络空间具有显著的复杂性

随着云计算、物联网、大数据、移动通信等领域的不断发展，网络空间作为一个极度分散的空间区域，涵盖诸多非连续网络节点及其链路，因此，该区域可以视为非连续型极度分散且持续演变的动态异构域。网络空间具有日益增加的全球连接、无所不在的高度机动性，使网络与电磁空间融为一体，实现基础设施和设备操作要求的动态配置，核心是使信息从平面、线式交互发展为大纵深的网络空间立体交互。因此，网络空间具有典型的复杂性。

2. 网络空间安全的内涵本质与外延构成

网络空间安全问题与网络空间相伴相生，网络空间安全的概念也是由信息安全、计算机安全以及网络安全等概念发展和拓展而来，其关注对象包括因特网、电信网、计算机系统以及嵌入式处理器和控制器等的安全问题，并将安全的范围拓展至网络空间中所形成的一切安全问题，涉及诸多领域，具备综合性和全球性的新特点。

网络空间安全涵盖了传统的信息安全和网络安全的内容，但其更加关注与陆、海、空、天并行的空间概念，安全问题具有跨时空、多层次、立体化、广渗透、深融合的新形态，而且一开始就具有鲜明的体系和对抗的性质。网络空间安全所涉及的主体、客体及其相互作用构成了一个复杂动力系统，必须基于复杂系统的观点来考察网络空间。

从外延来看，网络空间安全包括网络空间关键信息基础设施运行安全、网络空间攻防对抗、网络空间信息传播及其管控以及信息隐私保护等。

1.2 系统科学与系统工程

探讨网络空间的安全问题，首先要认知网络空间安全，而认知的手段和方法至关重要。德国著名物理学家普朗克指出，科学是内在的统一整体，它被分解为单独的“个体”不是源自事物本身，而是源自人类认识能力的局限。考察网络空间安全的概念及其相关联系，离不

开信息论、系统论和控制论等系统科学经典理论(老三论)和耗散结构理论、协同论、突变论等新兴理论(新三论)。同时还需要系统工程和体系工程等思想和方法。

1.2.1　系统与整体性

辩证唯物主义认为，世界是普遍联系的整体，任何事物之间及事物内部各要素之间均存在相互影响、相互作用和相互制约的关系，即客观世界的事物是普遍联系的。客观事物是普遍联系的整体，必然存在客观规律，考察客观事物就应该研究、认识和运用这些规律。事物的普遍联系是一个客观事实和本质特征，而系统就是能够反映与概括这个客观事实和本质特征的最基本且最重要的概念。

系统是指由相互联系、相互作用、相互依赖、相互影响的若干组成部分构成的具有特定功能的有机整体，而且其本身又是它所从属的某个更大系统的组成部分。系统在自然、社会和人类等客观世界中普遍存在。系统的结构与环境及其关联关系，决定了系统的整体性与功能，而整体性则是研究及应用系统的核心所在。系统功能是系统整体性的外在表现，而整体性是系统最重要的特点，是指系统在整体上具有其组成部分所没有的性质。

系统的整体性意味着，系统功能绝非其组成部分性质或性状的简单叠加，而是系统整体涌现的结果，遵从涌现机理和规律。也就是说，对于系统来说，其核心在于系统整体所涌现出来的功能，即便全部认识了其组成部分，也并不等于认识了系统自身。

按照前述系统原理，为使系统具备所期望的功能尤其是最优功能，可以通过调整和改变其结构或环境及其关联关系来实现。不过，系统环境通常无法任意改变或调整，多数情况下只能去适应环境，而系统的组成结构则可以通过一定的手段和方法去重新设计、组织、调整和改变。由此，便能够通过设计、组织、调整和改变系统组成部分或其间、层次结构之间及其与环境之间的关联关系，实现系统整体、部分与环境相互协调、统一与协同，因系统整体涌现而使功能甚至是最优功能得以实现。此即系统控制、管理与干预的基本内涵，属于系统管理、系统控制等研究的应用理论范畴，同时也是系统工程等要实现的核心目标。

1.2.2　系统科学与系统工程概述

1. 科学、技术与工程的关系

为讨论系统科学与系统工程问题，我们先来考察科学、技术与工程的关系，这个问题向来是国内外科学界、工程技术界和哲学界关注的核心关键问题。

科学是运用定理、定律等思维形式，反映现实世界各种现象的本质和规律的知识与理论体系，即关于事物的基本原理和事实的有组织、有系统的知识。科学的主要任务是研究世界万物变化的客观规律，解决“为什么”的问题。技术是人在改造自然、改造社会，以及改造自我的过程中所用到的一切手段、方法的总和，是在科学指导下解决实际问题的某种范围的应用单元，解决“如何实现”的问题。工程是和科学与技术有关的综合实践过程，具有特定目标并注重效益，且受政治、经济、社会、法律、人文等多种因素的影响和约束，综合集成多种技术并实现优化。

简而言之，科学是系统理论知识，可用于指导实践；技术则是在科学的指导下，直接为