网络空间安全实践能力分级培养系列教材

网络空间安全实践能力分级培养

（I）

陈凯　付才　刘铭　主编
邹德清　主审

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

网络空间安全实践能力分级培养系列教材

网络空间安全实践能力分级培养

（I）

■ 陈凯 付才 刘铭 ▌主编
■ 邹德清 ▌主审

人民邮电出版社
北京

图书在版编目（CIP）数据

网络空间安全实践能力分级培养. Ⅰ / 陈凯，付才，刘铭主编. -- 北京 : 人民邮电出版社，2019.8
网络空间安全实践能力分级培养系列教材
ISBN 978-7-115-51500-1

Ⅰ. ①网… Ⅱ. ①陈… ②付… ③刘… Ⅲ. ①计算机网络－网络安全－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2019)第121066号

内 容 提 要

为应对当前网络空间安全人才培养的需求，根据学生的学习规律和认知过程，突破传统以理论课堂教学为主的学习方式，提炼总结网络空间安全实践知识和技能，采取分级模式设计教学内容，并以实战通关的方式进行课程考核，构建分级通关式综合实践培养课程体系。该体系根据不同级别学生所具备的能力基础，按“感知能力”“分析能力”“系统能力”“创新能力”4个方面分为四级，本书为第一级培养方案提供教学素材。

本书的读者对象为高校网络安全与信息安全专业低年级本科生，也可为职专技能培训提供参考。

◆ 主　　编　陈　凯　付　才　刘　铭
主　　审　邹德清
责任编辑　邢建春
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：12.5　　2019年8月第1版
字数：305千字　　2019年8月北京第1次印刷

定价：69.00元

读者服务热线：(010)81055493　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前言

《中华人民共和国网络安全法》的颁布与实施，标志着网络空间安全已经上升到国家安全的战略高度，从某种意义上说，网络空间和领土、领海、领空一样，正在逐渐成为一个国家主权的象征。“实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院”是当下开展网络安全高等教育的重要内容，而培养一流的网络空间安全人才需要一流的培养体系。

目前高校中大多数网络空间安全人才培养采用传统的课程教学模式，以专业方向为课程开设的指导，相关实践课程作为理论课程的附属，仅作知识验证。但实际中，任何一次网络攻击，都不会是某一种或者少数几种网络攻击手段的应用，而是一项综合利用多种网络攻击原理、方法、技术和工具的复杂系统工程。因此，无论是从“攻”还是“防”的角度，都要求培养的人才不仅拥有深厚的理论基础和高超的实践技能，还需要有深刻的洞察力、敏锐的系统分析能力和快捷的反应力，以及从工程的视角看待和解决问题的能力。传统的高校人才培养模式很难让学生真正具备综合系统分析能力、解决问题的创新能力和快速的应变能力。

网络空间安全人才的培养，在新的时期有新的要求，需要以全局意识构建网络空间安全课程体系，注重学习过程中系统性的知识掌握和综合性的技能发挥，才利于培养出具有强创新性和竞争性的高素质人才，由此我们提出一套分级通关式综合实践能力培养教学体系。该教学体系将现有教学课程中的各知识点通过案例场景的方式衔接、关联和融合，从学生的感知能力、分析能力、系统能力和创新能力 4 个层面展开，对应将实践教学过程分为 4 级。同时，引入游戏通关的方式对培养过程进行考察和评测，通过学习过程中的阶段评测关卡来评估学生阶段性实践能力的掌握。

本书基于分级通关式综合实践能力培养教学体系中的第一级教学计划编制，为教学过程提供素材。综合实践分级通关的第一级课程面向不具备专业基础的低年级学生，以网络空间安全基础实验为主，让学生对网络空间安全的知识体系有系统的认知及初步了解，通过一些入门实验、基础工具的使用培养动手能力，激发学习兴趣，提升对网络空间安全威胁感知与理解能力。教学内容包括网络空间安全基本概念、主机安全、桌面安全软件、加密解密软件的文件保护及破解、钩子技术基础、计算机网络安全基础、数据库安全基础、Web SQL 注入攻击初步、计算机病毒基础、防火墙基础。

本书共 10 章，各章内容如下。

第 1 章主要介绍网络空间安全学科的内涵、状况、发展历程、主要研究方向及内容、安全理论及学习基础和相关的法律法规。第 2 章以 Linux 和 Windows Server 2008 R2 为例，介绍操作系统安全方面的基础知识，以及操作系统中的安全配置和管理。第 3 章介绍基本的桌面安全防护技能，包括桌面安全软件工作原理，了解进程、线程、应用程序以及网络连接的代码工作原理，介绍了钩子技术，并以实战的方式讲解钩子测试工具。第 4 章基于 Linux 中的 GnuPG，介绍使用公钥密码加密软件的各步骤，包括密钥生成、密钥管理、加密解密及签名，阐述文件保护的方法。第 5 章讲解计算机网络安全中的嗅探基础和扫描基础，介绍常用的嗅探工具和扫描工具的使用方法。第 6 章通过讲解 DBMS 的安装、配置、启动以及使用，介绍数据库、数据库安全相关概念。第 7 章介绍简单的 SQL 注入原理和初步的 SQL 注入技术，并介绍如何使用已有的程序、工具或者手工方式完成 SQL 注入的简单实验。第 8 章通过实践案例介绍基本的计算机病毒原理，分析病毒发作现象，阐述使用相关工具清除病毒的基本技能。第 9 章描述无线 AP 密码破解的方法及工具。第 10 章通过两个独具特色的防火墙实例介绍计算机网络防火墙技术。

本书在编写的过程中，得到华中科技大学网络空间安全学院和计算机科学与技术学院的各位教师和学生的支持，以及人民邮电出版社的大力帮助和支持，在此表示由衷的感谢。

作　者

2019 年 5 月

目 录

第1章 网络空间安全概论

1.1 引言

21 世纪是网络空间科学与技术飞速发展的时代。网络成为一种重要的战略资源。网络空间的安全保障能力成为一个国家综合国力的重要组成部分。在信息科学与技术空前繁荣的同时，危害网络空间安全的事件不断发生，网络空间安全的形势是严峻的。网络空间安全事关国家安全、社会稳定，必须采取措施确保我国的网络空间安全。

2004 年党的十六大文件已经把网络空间安全作为我国国家安全的重要组成部分。2012 年党的十八大文件进一步明确指出要“高度关注海洋、太空、网络空间安全”。2014 年 2 月，中央网络安全和信息化领导小组成立，习总书记担任组长，明确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。因此，加快国家网络空间安全保障体系建设，确保我国的网络空间安全，已经成为国家战略。

人才资源是第一位的资源。因此，网络空间安全人才培养是我国网络空间安全保障体系建设的必备基础和先决条件。网络空间安全学科建设则是培养高层次网络空间安全专业人才的基础平台。

1.2 网络空间安全学科的学科内涵

目前业界关于网络空间安全学科的定义和内涵，尚没有形成统一的说法。不同的学者根据自己的研究和理解，给出了不同的诠释。尽管这些诠释不尽相同，但其主要内容却是相同的。

传统的网络空间安全强调信息（数据）本身的安全属性，认为信息安全主要包含以下特性。

① 信息的秘密性：使信息不泄露给未授权者的特性。

② 信息的完整性：保护信息真实、完整和未被修改的特性。

③ 信息的可用性：已授权实体一旦需要就可访问和使用信息的特性。

信息论的基本知识告诉我们，信息不能脱离它的载体而孤立存在，因此不能脱离信息系统而孤立地谈论网络空间安全。也就是说，网络空间安全总是不可避免地关系到信息系统的安全。这是因为，如果信息系统的安全受到危害，则必然会危害到存在于信息系统之中的信息的安全，进而影响这些信息拥有者的合法权益，因此，可以从信息系统角度来全面考虑网络空间安全的内涵。

从纵向来看，信息系统安全主要包括以下 4 个层面：设备安全，数据安全，内容安全，行为安全。其中，数据安全即传统的信息安全。

（1）设备安全：信息系统设备（硬设备和软设备）的安全是信息系统安全的首要问题。这里包括以下 3 个方面。

① 设备的稳定性。

② 设备的可靠性。

③ 设备的可用性。

（2）数据安全：采取措施确保数据免受未授权的泄露、篡改和毁坏。

① 数据的秘密性。

② 数据的完整性。

③ 数据的可用性。

（3）内容安全：内容安全是网络空间安全在政治、法律、道德层面上的要求。

① 信息内容在政治上是健康的。

② 信息内容符合国家法律法规。

③ 信息内容符合中华民族优良的道德规范。

（4）行为安全：行为安全从主体行为的过程和结果来考察是否会危害网络空间安全（或者，是否能够确保网络空间安全）。从行为安全的角度来分析和确保网络空间安全，符合哲学上实践是检验真理唯一标准的基本原理。

① 行为的秘密性：行为的过程和结果不能危害数据的秘密性，必要时行为的过程和结果也应是保密的。

② 行为的完整性：行为的过程和结果不能危害数据的完整性，行为的过程和结果是预期的。

③ 行为的可控性：当行为的过程出现偏离预期时，能够发现、控制或纠正。

根据上面的分析，要确保信息系统的安全，就必须确保信息系统的设备安全、数据安全、内容安全和行为安全。信息系统的硬件系统安全和操作系统安全是信息系统安全的基础，密码和网络安全等技术是信息系统安全的关键技术。确保信息系统安全是一个系统性的工程，只有从信息系统硬件和软件的底层做起，从整体上采取措施，才能比较有效地确保信息系统的安全。

综上所述，我们给出网络空间安全学科的内涵：网络空间安全学科是研究网络空间信息获取、存储、传输和处理中的网络空间安全保障问题的一门新兴学科。

网络空间安全学科是综合计算机、通信、电子、数学、物理、生物、管理、法律和教育等学科，并发展演绎而形成的交叉学科。网络空间安全学科与这些学科既有紧密的联系和渊源，又有本质的不同，从而构成一个独立的学科。网络空间安全学科已经形成自己的理论、

技术和应用，并服务于信息社会。

网络空间安全学科归属于工学。但考虑到现阶段我国网络空间安全专业的实际情况，允许学校给网络空间安全专业的毕业生授予工学或理学学位。

1.3　国外网络空间安全学科的状况

美国等发达国家十分重视网络空间安全，把确保信息系统安全作为国家安全战略中最重要的组成部分之一。多年来，美国一直把网络空间安全作为其国防安全的重点，多层次培养网络空间安全人才，大力发展网络空间安全技术，并且形成了庞大的网络空间安全产业，走在世界各国的前列。

美国历届政府都高度重视网络空间安全，制定和颁布了一系列的规划和计划，并加以实施。早在 1995 年，美国国家安全局（National Security Agency）委托卡耐基梅隆大学成立网络空间安全学术人才中心，以提高大学网络空间安全人才培养能力。至 2003 年 9 月，已有 50 多所教育机构被认定成为这种中心，其中一部分大学设立了网络空间安全本科专业，一部分大学设立了网络空间安全硕士专业，更多的大学设立了网络空间安全研究方向。

除此之外，美国的麻省理工学院、卡耐基梅隆大学、加州大学伯克利分校、斯坦福大学等学校长期与美国军方合作，不仅为军方完成了许多重要的研究项目，还为军方培养了大批高层次网络空间安全专业人才。

2009 年 5 月 29 日，奥巴马政府公布了名为《信息空间政策评估——保障可信和强健的信息和通信基础设施》的报告，其中，把信息安全教育和人才培养列为重点之一，正式提出了网络空间安全劳动力的概念，从而把网络空间安全作为一种新的社会职业。

2010 年 4 月，美国政府启动了“网络空间安全教育国家计划”（NICE，National Initiative for Cybersecurity Education）。该计划由美国商务部 NIST 研究所牵头，美国国土安全部、国防部、教育部、司法部等 11 个政府部门共同负责。NICE 计划的目的是通过创新网络空间安全教育，增强美国整体的网络空间安全，并制定了 3 个具体目标：

（1）提高全民网络空间安全的风险意识；

（2）扩充网络空间安全队伍后备人才；

（3）培养一支具有全球竞争力的网络空间安全队伍。

为了实施 NICE 计划，NICE-NIST 委员会专门制定了相关的指导文件：2011 年 8 月发布了《NICE 战略计划（草案）》并在网上公开征集意见；2012 年 9 月又发布了修改草案。草案将网络空间安全技术领域分为 7 个大类：

（1）安全地提供保障；

（2）系统运行与维护；

（3）实施保护与防御；

（4）调查取证；

（5）情报收集与作战；

（6）事态与信息分析；

（7）监管与发展。

NICE 计划的启动和系统细致的组织实施充分表达了美国对信息安全问题的深刻认识和高度重视，这些值得我们借鉴。

1.4 我国网络空间安全学科的发展历程

我国在网络空间安全领域的工作和技术经历了通信保密、信息安全和网络空间安全保障 3 个阶段。

通信保密阶段：在计算机开始普遍应用之前，我国在网络空间安全领域的工作和技术主要是确保通信的保密，所使用的网络空间安全技术主要是密码技术。只有少数专业单位进行密码技术的研究和开发，而且研究开发工作本身也是秘密进行的。1982 年，西安电子科技大学邀请日本京都大学一松信教授来华讲学“计算复杂性与密码学”，1984 年 12 月在西安电子科技大学召开了“第一届中国密码学术会议”。这些活动开创了我国公开研究密码学的先河。

信息安全阶段：20 世纪 80 年代中期以后，微型计算机的应用逐渐普及。计算机病毒开始出现并广泛传播，非法复制软件的现象相当普遍。随着网络技术的发展和应用，计算机病毒、蠕虫和木马等恶意代码通过网络传播，造成了更大范围的危害。于是，防治计算机病毒等恶意代码，阻止非法复制软件，保障网络安全成为社会对网络空间安全的迫切需要。这一时期，除了通信保密之外，计算机操作系统安全、分布式系统安全和网络系统安全的重要性和紧迫性逐渐凸显出来。为了解决这些网络空间安全问题，出现了计算机安全、软件保护、网络安全等网络空间安全新内容和新技术。

网络空间安全保障阶段：进入 21 世纪，通信、计算机和消费电子（Communication, Computer, Consumer Electronics）的结合，促进了因特网、信息高速公路和全球信息基础设施（GII）的出现和应用，构成了人类生存的信息环境，即信息空间（Cyberspace）。

人们清楚地认识到，人类社会中的安全可信与信息空间中的安全可信是休戚相关的。对于人类生存来说，只有同时解决人类社会和信息空间的安全可信问题，才能保证人类社会的安全、和谐、繁荣和进步。

在信息空间时代，信息科学技术和产业空前繁荣，社会的信息化程度大大提高。电子商务和电子政务等大型应用信息系统开始广泛应用，云计算、物联网、大数据处理等新型信息系统出现。这些都对信息安全提出了更新、更高的要求。信息成为一种重要的战略资源，任何危害网络空间安全的行为都将可能造成重大损失。这时，对网络空间安全的要求不仅仅是单纯的通信保密和传统意义上的网络空间安全，而是已经上升到信息系统安全的阶段（设备安全、数据安全、内容安全、行为安全）。人们对网络空间安全内涵和属性的理解也有了很大的扩展，可信性、隐私性、强健性和可生存性等成为信息系统安全的新属性。可信计算等信息系统安全新技术出现，确保信息空间的安全可信成为新的目标。我国在网络空间安全领域的工作和技术进入网络空间安全保障阶段。

在 20 世纪 70 年代之前，我国只有少数专业性学校（如军队学校）培养网络空间安全方面的专业人才，而且培养的技术内容以密码技术为主。从 20 世纪 70 年代开始，我国普通高校开始培训网络空间安全人才。例如，中国科学院数学研究所和北京大学开始为军队培训密码学的数学基础，西安电子科技大学开始为军队培训数字通信和编码。此后，在高校恢复研

究生制度以后，西安电子科技大学等少数高校开始招收密码学的研究生。1999 年西安电子科技大学等 4 所高校建立了“信息对抗”本科专业。

到目前为止，全国已经有 100 多所高校建立了信息安全或者网络空间安全本科专业。2003 年，武汉大学、华中科技大学、中国科学院软件研究所和国防科技大学率先建立了网络空间安全博士点。后来，建立网络空间安全博士点的高校又增加了很多。除了网络空间安全博士点外，西安电子科技大学、解放军信息工程大学、北京邮电大学和国防科技大学等高校还建立了密码学博士点。自此，我国形成了从本科到博士后的完整网络空间安全人才培养体系。2005 年，教育部下达了《教育部关于进一步加强网络空间安全学科、专业和人才培养工作的意见》的文件。文件提出，“不断加强网络空间安全学科、专业建设，尽快培养高素质的网络空间安全人才队伍，成为我国经济社会发展和网络空间安全体系建设中一项长期性、全局性和战略性的任务”。

当前，网络空间安全学科发展和人才培养形势得到了国家的高度重视。2015 年，国务院学位办批准设立了网络空间安全学科，全国 29 所高校获得了博士学位授予权，学科发展有了体系化的支撑；特别是 2015 年 4 月 19 日，全国网络安全与信息化工作座谈会召开，习近平总书记的讲话为国家网络安全建设发展和人才培养指明了方向，网络安全领域迎来大发展时期。2016 年 6 月，中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》（中网办发文[2016]4 号），进一步促进了我国高等学校网络安全学科专业和院系建设，必将全面提高网络空间安全人才培养质量。2017 年 2 月，教育部发布了《教育部高等教育司关于开展“新工科”研究与实践的通知》，深化工程教育改革，推进“新工科”的建设与发展。2017 年 9 月，全国有 7 所高校获批“一流网络安全学院建设示范项目”，进一步推动全国网络空间安全学科建设，2018 年又有 18 所高校获批网络空间安全专业，全国网络空间安全学科发展进入新阶段。

发展我国的网络空间安全事业，人才培养是关键。教育是人才培养的基础，高校是人才培养的基地。普遍提高我国高校学生的网络空间安全意识，提高他们对网络空间安全风险的认识和基本防护能力，已经成为我国每所高校必须高度重视的教育问题。其中，如何有效地培养出适应社会需求的、多层次高素质的网络空间安全专业人才，已经成为我国设置网络空间安全专业高校的一项重要任务。

1.5　网络空间安全学科的主要研究方向及研究内容

当前，网络空间安全学科的主要研究方向有密码学、网络安全、信息系统安全和信息内容安全。可以预计，随着网络空间安全科学技术的发展和应用，还会产生新的网络空间安全研究方向，网络空间安全的研究内容将更加丰富。下面分别介绍这 4 个研究方向的研究内容。

1.5.1　密码学

密码学由密码编码学和密码分析学组成，其中，密码编码学主要研究对信息进行编

码以实现信息隐蔽，而密码分析学主要研究通过密文获取对应的明文信息。密码学研究密码理论、密码算法、密码协议、密码技术以及密码应用等科学技术问题。其主要研究内容如下。

① 对称密码。
② 公钥密码。
③ Hash 函数。
④ 密码协议。
⑤ 新型密码：生物密码、量子密码等。
⑥ 密钥管理。
⑦ 密码应用。

1.5.2 网络安全

网络安全的基本思想是在网络的各个层次和范围内采取防护措施，以便能够对各种网络安全威胁进行检测发现，并采取相应的响应措施，确保网络的网络空间安全。其中，防护、检测和响应都需要基于一定的安全策略和安全机制。网络安全的研究包括网络安全威胁、网络安全理论、网络安全技术和网络安全应用等。其主要研究内容如下。

① 网络安全威胁。
② 通信安全。
③ 协议安全。
④ 网络防护。
⑤ 入侵检测。
⑥ 入侵响应。
⑦ 可信网络。

1.5.3 信息系统安全

信息系统是为用户提供服务的各种软硬件系统，用户通过信息系统得到信息的服务。有的信息系统较小，但许多信息系统是复杂庞大的系统。例如，操作系统、数据库系统、电子商务系统、电子政务系统等都是复杂庞大的典型信息系统。

信息系统是信息的载体，信息系统应当确保存在于其中的信息的安全。信息系统安全的特点是从系统的整体上考虑网络空间安全威胁并采取防护措施。它研究信息系统的安全威胁、信息系统安全的理论、信息系统安全技术和应用。其主要研究内容如下。

① 信息系统的安全威胁。
② 信息系统的设备安全。
③ 信息系统的硬件系统安全。
④ 信息系统的软件系统安全。
⑤ 访问控制。
⑥ 可信计算。

⑦ 网络空间安全等级保护。
⑧ 应用信息系统安全。

1.5.4 信息内容安全

信息内容安全是网络空间安全在政治、法律、道德层面上的要求。我们要求信息内容是安全的，就是要求信息内容在政治上是健康的，在法律上是符合国家法律法规的，在道德上是符合中华民族优良道德规范的。

1995 年西方七国信息会议首次提出“数字内容产业”（Digital Content Industry）的概念。我国将“数字内容产业”定义为：基于数字化、网络化，利用信息资源创造、制作、开发、分销、交易的产品和服务的产业。显然，数字内容产业需要信息内容安全来保障。若不能确保信息内容的安全，将不能确保数字内容产业的健康发展。目前，学术界对信息内容安全的认识尚不一致。广义的信息内容安全既包括信息内容在政治、法律和道德方面的要求，也包括信息内容的保密、知识产权保护、隐私保护等诸多方面。我们这里主要强调信息内容安全中的基本概念、基本理论、基本技术和应用。其主要研究内容如下。

① 信息内容安全的威胁。
② 信息内容的获取。
③ 信息内容的分析与识别。
④ 信息内容的管控。
⑤ 信息隐藏。
⑥ 隐私保护。
⑦ 信息内容安全管理。
⑧ 信息内容安全的法律保障。

1.6 网络空间安全学科的理论和方法论基础

网络空间安全学科是在计算机、通信、电子、数学、物理、生物、法律、管理和教育等学科的基础上交叉融合发展而来的，其理论基础和方法论基础也与这些学科相关，但在学科的形成和发展过程中又丰富和发展了这些理论和方法论，从而形成了自己的学科理论和方法论。

1.6.1 理论基础

（1）数学是一切自然科学的理论基础，当然也是网络空间安全学科的理论基础。

现代密码可以分为两类：一类是基于数学的密码；另一类是基于非数学的密码。虽然某些基于非数学的密码技术开始走向应用，如基于量子物理的量子密钥分发技术。但基于非数学的密码总体上还处在发展的初期阶段。目前广泛实际应用的密码仍然主要是基于数学的密码。

对于基于数学的密码，本质上一个密码就是一个数学函数，而密码破译就是求解某一数学难题。这就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主要有代数、数论、概率统计等。

协议是网络的核心，因此协议安全是网络安全的核心。作为网络协议安全理论基础之一的数学主要有逻辑学等。

因为网络空间安全领域的斗争，本质上是对抗双方之间的斗争，因此数学中的博弈论（Game Theory）成为网络空间安全的基础理论之一。

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，以及如何找到这个最合理的方案。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。博弈论的思想古已有之，我国古代的《孙子兵法》不仅是一部军事著作，而且是最早的一部博弈论专著。博弈论已经在经济、军事、体育和商业等领域得到广泛应用。网络空间安全领域的斗争无一不具有这种对抗性或竞争性，如网络的攻与防、密码的加密与破译、病毒的制毒与杀毒、信息内容的隐藏与提取等。因为网络空间安全领域的斗争，本质上是人与人之间对抗性质的斗争，因此博弈论成为网络空间安全的基础理论之一。遵循博弈论的指导原则，我们将在网络空间安全的斗争中，避免被动，掌握主动，立于不败之地。

（2）信息论、控制论和系统论是现代科学的理论基础，也是信息安全学科的理论基础。

信息论是香农为解决现代通信问题而建立的；控制论是维纳在解决自动控制问题中建立的；系统论是为了解决现代化大科学工程项目的组织管理问题而建立的。在开始时，它们都是独自形成的独立科学理论。但由于它们之间具有紧密的联系，因此在后来的应用和发展中互相渗透、互相作用，出现了趋向综合统一、形成统一学科的趋势。这些理论，特别是信息论构成了网络空间安全学科的理论基础。

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上，标志着密码学作为一门独立学科的形成。因此，信息论成为密码学重要的理论基础之一。

从信息论角度看，信息隐藏（嵌入）可以理解为在一个宽带信道（原始宿主信号）上用扩频通信技术传输一个窄带信号（隐藏信息）。尽管隐藏信号具有一定的能量，但分布到信道中任意特征上的能量是难以检测的。隐藏信息的检测是一个有噪信道中弱信号的检测问题。因此，信息论构成了信息隐藏的理论基础。

综上所述，信息论奠定了密码学和信息隐藏的理论基础。虽然密码学和信息隐藏已经取得了重要发展并得到了广泛应用，但是密码学、信息隐藏的发展至今没有超越信息论的理论范畴。

系统论是研究系统一般模式、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。系统论的能动性不仅在于认识系统的特点和规律，更重要的是利用这些特点和规律去控制、管理、改造或创造一个系统，使它的存在和发展符合人的需求。

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，获取一些信息，并以这种信息为基础施加作用到该对象上。由此可见，控制的基础是信息，信息的获取是为了控制，任何控制又都依赖于信息反馈。

网络空间安全遵从“木桶原理”。这“木桶原理”正是系统论的思想在网络空间安全领域的体现。

保护、检测、反应（PDR）策略是确保信息系统和网络安全的基本策略。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，从整体上采取措施，才能比较有效地确保信息系统的安全。

以上策略和观点已经经过网络空间安全的实践检验，证明是正确的、是行之有效的。它们符合系统论和控制论的基本原理。这表明，系统论和控制论是信息系统安全和网络安全的理论基础。

（3）网络空间安全学科的许多问题是计算安全问题，因此计算理论也是网络空间安全学科的理论基础，主要包括可计算性理论和计算复杂性理论等。

可计算性理论是研究计算一般性质的数学理论。它通过建立计算的数学模型，精确区分哪些问题是可计算的，哪些问题是不可计算的。对于判定问题，可计算性理论研究哪些问题是可判定问题，哪些问题是不可判定问题。

计算复杂性理论使用数学方法对计算中所需各种资源的耗费做定量的分析，并研究各类问题在计算复杂程度上的相互关系和基本性质。计算复杂性理论是计算理论在可计算性理论之后的又一个重要发展。可计算性理论研究区分哪些问题是可计算的，哪些问题是不可计算的，但这里的可计算是理论上的可计算，或原则上的可计算。而计算复杂性理论则进一步研究现实的可计算性，如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。

众所周知，授权是信息系统访问控制的核心，信息系统是安全的，其授权系统必须是安全的。可计算性的理论告诉我们：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。例如，著名的“停机问题”是不可判定问题，而具体程序的停机问题却是可判定的。由此可知，一般计算机病毒的检测是不可判定问题，而具体软件的计算机病毒检测又是可判定问题。这就说明可计算性理论是信息系统安全的理论基础之一。

本质上，密码破译就是求解一个数学难题，如果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。如果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。“一次一密”密码是理论上安全的密码，其余的密码都只能是计算上安全的密码。根据计算复杂性理论的研究，NPC 问题是最难计算的一类问题。公钥密码的构造往往基于一个 NPC 问题，以使密码是计算上安