21世纪高等学校信息安全专业规划教材

网络安全程序设计

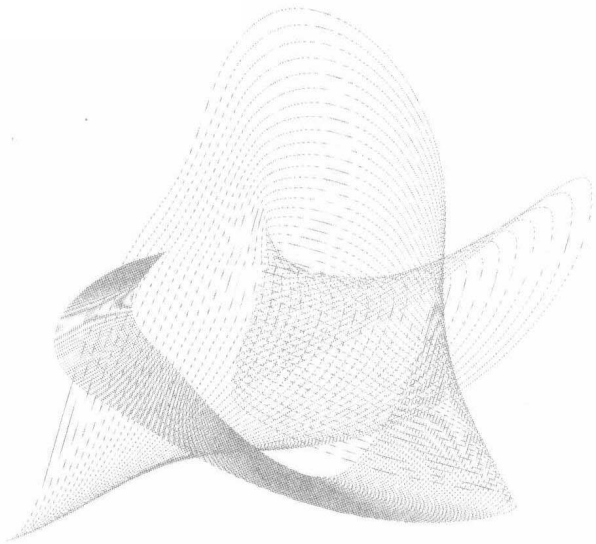
李红娇 ◎ 主　编
李晋国　李婧 ◎ 副主编
顾春华 ◎ 主　审

清華大學出版社

21世纪高等学校信息安全专业规划教材

网络安全程序设计

李红娇 ◎ 主　编
李晋国　李婧 ◎ 副主编



清华大学出版社
北京

内 容 简 介

本书以网络安全程序设计基础和主要技术为核心内容。全书共8章，主要内容包括：第1章是网络空间安全学科相关介绍；第2章是网络安全编程基础，包括Socket编程与VC++网络安全编程基础；第3～8章是全书的重点，介绍密码学编程，基于OpenSSL开发包的网络安全编程，网络扫描器设计，防火墙设计与实现，入侵检测模型的设计与实现以及应用系统安全编程。本书内容丰富、实用，涵盖网络安全程序设计的基本核心技术，并给出了代码实例，有助于读者理论结合实际地理解掌握网络安全程序设计技术。

本书可作为普通高等院校信息安全专业、计算机科学与技术专业、电子信息专业本科生和研究生的教材，也可供相关行业从业人员学习参考。

图书在版编目(CIP)数据

网络安全程序设计/李红娇主编. —北京：清华大学出版社，2017
(21世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-45180-8

Ⅰ. ①网… Ⅱ. ①李… Ⅲ. ①计算机网络－网络安全－程序设计－高等学校－教材 Ⅳ. ①TP311.1

中国版本图书馆CIP数据核字(2016)第239586号

责任编辑：魏江江　薛　阳
封面设计：刘　键
责任校对：焦丽丽
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 刷 者：三河市君旺印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：19.25　　**字　　数**：469千字
版　　次：2017年3月第1版　　**印　　次**：2017年3月第1次印刷
印　　数：1～2000
定　　价：39.50元

产品编号：068241-01

前　言

随着互联网应用的日益广泛，围绕网络信息的获取、使用、传输引发的安全问题越来越显得重要，网络空间安全也上升为国家战略，实践能力是网络空间安全创新人才培养的核心之一。本书是为高等学校的本科生、研究生提供的网络安全程序设计教材。

网络空间安全涉及数学、计算机科学与技术、信息与通信工程等多个学科，已形成了一个相对独立的教学和研究领域。网络安全程序设计对学生的要求相对比较高，需要高级语言编程、操作系统、计算机网络、密码学与信息安全等基础知识以及一些工具软件的应用。

本书从网络空间安全的必要性以及对创新人才培养的需求出发，阐述网络安全程序设计的编程基础与核心技术，对每个技术的讲述包括基本概念、基本原理及编程实例，将基础知识与编程实践结合，这对启发学生的思考以及提升动手能力是十分重要的。从而学生更能深入理解每种安全机制的实质，也有助于学生理论联系实际地根据实际应用掌握网络安全编程技术。

全书共 8 章。第 1 章概要介绍网络空间安全的必要性、网络空间安全对人才培养的新要求以及网络安全程序设计相关知识；第 2 章介绍网络安全编程基础，包括 Socket 编程以及 VC++网络安全编程；第 3 章阐述密码学基础知识，基于经典密码算法的安全编程实例；在此基础上，第 4 章讲述基于网络安全开发包 OpenSSL 的编程实践；第 5 章介绍网络扫描器的设计，包括 ICMP 扫描、TCP 扫描、木马扫描等基本原理与编程实现；第 6 章介绍了防火墙技术以及基于包过滤技术的防火墙实现；第 7 章介绍入侵检测系统原理、技术与实现；第 8 章介绍两种实际应用系统编程，包括基于 OpenSSL 的安全 Web 服务器设计实现及安全电子邮件编程。

本书的建议学时为 48 学时，其中课堂讲解部分为 24 学时，上机实验 24 学时。根据各专业的不同教学需求，以上学时安排和内容可根据实际需要进行调整。

本书由李红娇担任主编与统稿工作，李晋国、李婧担任副主编。李红娇负责编写第 1～4 章。第 5 章和第 6 章内容由李婧负责编写，第 7 章和第 8 章内容由李晋国负责编写。许智、陈晶晶、郭政伟参与了本书的编辑及程序代码调试工作。本书由上海电力

学院顾春华教授主审。本教材编写得到了上海市信息安全管理重点实验室开放课题(编号AGK2015005)以及上海市科委地方能力建设项目(No. 15110500700)资助。在编写过程中,也参考了一批技术文献、著作、教材及网络资源,为本书的编写奠定了宝贵的基础,在此一并表示衷心的感谢。

由于编者水平有限,书中难免有疏漏和不足之处,恳请专家和读者批评指正。

编 者

2016 年 12 月于上海

目　录

第1章 绪 论

信息技术和应用的不断发展变化，给网络空间安全带来了巨大挑战，维护网络空间安全已经成为国家安全的战略高地，国家高度重视网络空间安全人才培养，增设网络空间安全一级学科，提高学生的实践能力是培养网络安全创新人才的核心之一。因此，必须掌握网络安全程序设计基础知识。

1.1 网络空间安全的必要性

1.1.1 技术层面

20 世纪 60 年代开始，美国国防部的高级研究计划局(Advance Research Projects Agency，ARPA)开始建立 ARPANet，即因特网的前身。因特网的迅猛发展始于 20 世纪 90 年代，由欧洲原子核研究组织 CERN 开发的万维网 WWW 被广泛使用在因特网上，大大方便了广大非网络专业人员对网络的使用，成为因特网用户指数级增长的主要驱动力。今天的因特网已不再是计算机人员和军事部门进行科研的领域，而是变成了一个开发和使用信息资源的覆盖全球的信息海洋，覆盖了社会生活的方方面面，构成了一个信息社会的缩影。目前，互联网正从 IPv4 向 IPv6 跨越。然而因特网也有其固有的缺点。

(1) 因特网是一个开放的、无控制机构的网络，黑客(Hacker)经常会侵入网络中的计算机系统，或窃取机密数据和盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。

(2) 因特网的大多数数据传输是基于 TCP/IP 通信协议进行的，这些协议缺乏使传输过程中的信息不被窃取的安全措施。

(3) 因特网上的通信业务多数使用 UNIX 操作系统来支持，UNIX 操作系统中明显存在的安全脆弱性问题会直接影响安全服务。

(4) 在计算机上存储、传输和处理的电子信息，还没有像传统的邮件通信那样进行信封保护和签字盖章。信息的来源和去向是否真实，内容是否被改动，以及是否泄漏等，在应用层支持的服务协议中是凭着君子协定来维系的。

(5) 电子邮件存在着被拆看、误投和伪造的可能性。使用电子邮件来传输重要机密信息会存在很大的危险。

(6) 计算机病毒通过因特网的传播给上网用户带来极大的危害，病毒可以使计算机和计算机网络系统瘫痪、数据和文件丢失。在网络上传播病毒可以通过公共匿名 FTP 文件传送，也可以通过邮件和邮件的附件传播。

安全性问题成为困扰因特网用户发展的一个主要因素。计算机病毒、网络蠕虫的广泛传播，计算机网络黑客的恶意攻击，DDOS 攻击的强大破坏力、网上窃密和犯罪的增多，使得网络安全问题关系到未来网络应用的深入发展。当信息技术快速步入网络时代，跨地域、跨

管理域的协作不可避免，多个系统之间存在频繁交互或大规模数据流动，专一、严格的信息控制策略变得不合时宜，信息安全领域随即进入了以立体防御、深度防御为核心思想的信息安全保障时代，形成了以预警、攻击防护、响应、恢复为主要特征的全生命周期安全管理，出现了大规模网络攻击与防护、互联网安全监管等各项新的研究内容。安全管理也由信息安全产品测评发展到大规模信息系统的整体风险评估与等级保护等。因此，开始针对信息安全体系进行研究，重在运行安全与数据安全，兼顾内容安全。

尽管当前信息安全技术得到了很大的发展，但是，信息技术和应用的不断发展变化也给其带来了巨大挑战，这些挑战主要有以下 5 个方面。

1. 新型通信网络

各国大力投入对新型通信网络的研究，欧盟 FP7 计划的 Challenge One 项目目标是提升网络灵活性以及可重构，日本 AKARI 计划主旨是网络虚拟化、多样化数据接入、网络功能扩展；美国国家科学基金会(National Science Foundation，NSF)的 FIA 项目以构建网络内容为导向、具备更安全表达性的网络为主旨；斯坦福大学的 OpenFlow 旨在构建网络控制平面与数据平面相分离的体系、实现灵活控制；软件定义网络(Software Define Network，SDN)由 OpenFlow 发展而来，被 ITU 等认可为新型通信网络的主流架构。随着新型通信网络技术的发展，国际电信联盟电信标准分局(International Telecommunication Union-Telecommunication Sector，ITU-T)、国际互联网工程任务组(The Internet Engineering Task Force，IETF)、开放网络基金会(Open Networking Foundation，ONF)、欧洲电信标准化协会(European Telecommunication Standards Institute，ETSI)等正着手制定相应标准。

由于新型通信网络以用户为中心、异构、动态、虚拟、开放，网络业务需求具备应用异构性、系统可扩展性、需求动态性、服务客户化；新型通信网络的控制集中性导致安全威胁更集中、更开放，受安全威胁面更大，虚拟性导致攻击形式趋于复杂和动态；因此，新型通信网络拓扑的动态性，控制的开放性，流量的隔离性，资源的虚拟性对信息安全提出了新挑战：网络结构和安全行为关系难以准确描述，控制节点的脆弱性影响整个网络，难以对控制入侵行为进行分析，虚实资源的复杂映射导致威胁态势难以准确分析。一些重要的科学问题，如网络结构、脆弱分析、检测机理、安全态势等需要新的思路来解决。

2. 云计算

云计算的安全问题是用户不再对数据和环境拥有完全控制权，云计算的出现彻底打破了地域的概念，数据不再存放在某个确定的物理节点，而是由服务商动态提供存储空间，这些空间有可能是现实的，也可能是虚拟的，还可能分布在不同国家及区域，用户对存放在云中的数据不能像从前那样具有完全的管理权。

相比传统的数据存储和处理方式，云计算时代的数据存储和处理，对于用户而言，变得非常不可控，云环境中用户数据安全与隐私保护难以实现。传统模式下，用户可以对其数据通过物理和逻辑划分安全域实现有效的隔离和保护。在云计算环境下，各类云应用不再依靠机器或网络形成固定不变的基础设施物理边界和安全边界，数据安全由云计算提供商负责。云计算中多层服务模式同样存在安全隐患。云计算发展的趋势之一是 IT 服务专业化，即云服务商在对外提供服务的同时，自身也需要购买其他云服务商所提供的服务；用户所享用的云服务间接涉及多个服务提供商，多层转包无疑极大地提高了问题的复杂性，进一

步增加了安全风险；虚拟运算平台的安全漏洞不断涌现，直接威胁云安全根基；云端大量采用虚拟技术，虚拟平台的安全无疑关系到云体系的架构安全；虚拟运算平台变得越来越复杂和庞大、管理难度也随之增大，如果黑客利用安全漏洞获得虚拟平台的管理控制权，后果将不堪设想。

3. 大数据

随着互联网/移动互联网、社交网络、数码设备、物联网/传感器等技术的发展，各种设备产生的数据量将会急剧增长。根据互联网数据中心(Internet Data Center，IDC)预测，未来10 年内全球数据量将以超过 40%的速度增长，2020 年全球数据量将达到 35ZB。

大数据的概念在学术界由来已久，但真正进入公众视野是在 2011 年麦肯锡发布的研究报告——《大数据：创新、竞争和生产力的下一个新领域》以后。普遍的观点认为，大数据是指规模大且复杂，以至于很难用现有数据库管理工具或数据处理方法来处理的数据集。大数据的常见特点包括大规模(volume)、高速性(velocity)和多样性(variety)。根据来源的不同，大数据大致可分为如下几类。

(1) 来自于人。人们在互联网活动以及使用移动互联网过程中所产生的各类数据，包括文字、图片、视频等信息。

(2) 来自于机。各类计算机信息系统产生的数据，以文件、数据库、多媒体等形式存在，也包括审计、日志等自动生成的信息。

(3) 来自于物。各类数字设备所采集的数据，如摄像头产生的数字信号、医疗物联网中产生的人的各项特征值、天文望远镜所产生的大量数据等。

大数据从概念走向实践，引发个人隐私安全问题。2011 年 4 月初，全球最大的电子邮件营销公司艾司隆(Epsilon)发生史上最严重的黑客入侵事件，导致许多企业客户名单以及电子邮件地址因此外泄。2011 年年底有网友爆料有黑客在网上公开了知名程序员网站CSDN 的用户数据库，2014 年年初携程网被怀疑储存用户信用卡信息存在泄漏风险。根据智能手机存储、显示的位置信息等多种数据组合，已可相对精准地锁定个人，用户个人隐私信息安全问题堪忧。

大数据时代国家安全将受到信息战与网络恐怖主义的威胁，大数据成为网络攻击的显著目标，并成为高级可持续攻击(Advancel Persistent Threat，APT)的载体，各国信息基础设施和重要机构都可能成为打击目标，而保护其免受攻击早已超出军事职权和能力范围，庞大海量的大数据涉及的方面之广，使得大数据也将为网络恐怖主义提供新的资源支持。

因其体量巨大、产生高速、类型多样、分布协同等特征，大数据面临严峻的信息安全挑战。传统的信息安全技术难以直接应用，发展一套全新的大数据系统安全理论和技术目前还不现实。因此，应采用现有安全技术，结合具体应用，利用新的思路，将大数据变成小数据，研究相关的安全关键技术，包括大数据中的用户隐私保护，大数据的可信性，大数据的访问控制技术，大数据可信度量技术，高效的大数据密码学以及针对不同结构的结构化、半结构化和非结构化数据，研究如何有效地进行安全管理、访问控制和安全通信。此外，在多租户的模式下，需要在保证效率的前提下，实现租户数据的隔离性、保密性、完整性、可用性、可控性和可追踪性。

4. 物联网与可穿戴设备

物联网的广泛应用将规避因特网应用上的局限性与安全性问题，通过射频识别(Radio

Frequency Identification,RFID)、红外感应器、全球定位系统、激光扫描器等信息传感设备,按约定的协议,把特定区域里的任何物品与虚拟网络连接起来,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理。物联网实质上是传感网与因特网、移动通信网,"三网"高效融合的产物,建立本地化的相对保密的传感网络与物联网络,可提升本土信息流通的安全性。国家的各个关键部门、产业领域以及一些关键性基础设施的控制系统逐步实现网络化,可增强在国际信息竞争中的话语权,为解决信息安全问题提供方案。

物联网感知层的电子标签和传感网络节点资源有限——存储空间、计算资源、通信能力、运算速度有限,难以采用复杂的安全机制,给传统的密码学和信息安全提出了挑战;感知层采用无线通信——传递信息暴露于大庭广众之下,给攻击者带来更多机会;物联网系统对应用完全开放将带来更多安全隐患。

可穿戴设备的隐蔽性和智能尘埃(intelligent mote)电子标签不可见给用户隐私保护带来极大的困难;谷歌眼镜和普通眼镜直观上难于区别,但却能拍摄尺寸极小的电子标签(尺寸为长 0.1mm,宽 0.1mm,厚 0.01mm),用户很难在物理上发现已经被跟踪,因此,保护用户隐私难度更大;认证过程需要物品的身份和位置信息,这加大了隐私保护难度。

物联网应用层信息安全问题来自物联网的安全体系架构带来的挑战。物联网中数亿计的设备接入,海量的数据信息,大量异构网络的存在,大规模的分布式应用系统,使物联网的安全体系架构面临着更加艰巨的挑战;物联网的访问控制存在难点,由于物联网部署的可扩展性、移动性和复杂性,使得对物品的访问控制很难有效地进行;物品间集群概念的引入,还需要解决群组认证的问题;物联网网络态势感知与评估理论和技术需求迫切,如何从大数据中升华智慧,对大规模物联网正常运转进行全面的态势感知和安全评估,以保障其安全运行和故障报警是正在开展的研究热点。

5. 量子网攻

美国《纽约时报》曝光的"量子"项目让舆论大吃一惊——美国国家安全局(National Security Agency,NSA)能够将一种秘密技术成功植入没有联网的计算机,对其数据进行任意更改。NSA 至少从 2008 年就开始使用这项名为"高科技广播频率"(High-tech radio frequency technology)的技术,并利用该技术成功入侵了全球近十万台计算机。一般来说,计算机间谍软件都是通过网络进行传播、植入的,但据悉 NSA 已经开始使用一种可以在计算机不接入互联网的情况下接入并修改其中数据的秘密技术。NSA 所使用的其中一件装备就是外形同普通 USB 设备无异的 Cottonmouth,只是该装置内嵌一个微型发射/接收器。

值得注意的是,在 2008—2010 年夏天美国对伊朗核设施采取的网络攻击中,美国就利用了这项技术向伊朗核设施植入"震网"病毒,这也是该技术第一次参与实战,据《纽约时报》透露,美国还出于反恐目的在沙特阿拉伯、印度和巴基斯坦网络中植入了这一间谍软件。

1.1.2 网络安全与国家战略

21 世纪是信息的时代,信息成为重要的战略资源。信息技术改变着人们的生活和工作方式。社会对计算机和网络的依赖越来越大。敌对势力的破坏、恶意软件的攻击等已对计算机和网络系统的安全构成极大的威胁,如果计算机和网络系统的安全受到破坏,不仅会造

成巨大的经济损失，甚至会导致社会混乱。信息安全关系到国家安全、社会稳定、经济发展、人民生活等各个方面，必须确保我国的信息安全。要建设国家信息安全保障体系，政府、军队和企业都需要大量信息安全专门人才。

1. 电子政务、电子党务对信息安全的需求

电子政务网、电子党务网是政府与党务办公、联系社会、服务社会的关键基础设施。政务网、党务网上的信息涉密程度高，对信息的保密性、完整性和可用性的要求也较高。电子政务、电子党务信息网络的建设和维护需要一支具有较高信息安全专业水平的建设和管理队伍。

2. 国防建设对信息安全的需求

信息对抗的攻防能力已成为国防力量之一，对网络的攻击也是一种威慑力量。美国很早就提出了信息战的概念，在“海湾战争”期间美军成功地对伊拉克发动了信息战。2009 年 6 月美国国防部长签署命令，正式成立美军的网络司令部。我国也应有自己的网络安全队伍，保障关系国计民生的重要网络信息系统的安全，防范可能的入侵和攻击，并具有必要的信息对抗能力，这些都需要大量的高级信息安全专业人才。

3. 维护公共安全对信息安全的需求

近年来，各种形式的网络犯罪给全球不少国家都带来了巨大损失。美国政府公布的一份国家安全报告认为，21 世纪对美国国家安全威胁最严重的是网络恐怖主义。美国中央情报局成立了一个专门负责研究遏制计算机犯罪的信息技术中心。为了遏制各种形式的网络犯罪，公安部门应当有能力通过合法监听得到通信内容；对于所得到的特定内容应当能知道其来源与去向；在必要的条件下能控制特定信息的传播。除了网络恐怖之外，一些网站传播低俗的内容，严重危害青少年的身心健康。要阻止网络犯罪和传播低俗内容，需要组建专门的网络警察队伍。因此，需要大量高素质的信息安全专业人才。

4. 企业发展对信息安全的需求

企业在利用信息化优势发展的过程中，需要把自身的网络安全风险降到最低。这就必须要求有足够的信息安全人才，企业对信息安全人员的需求不但在数量上迅速增长，而且对相关职位人才的任职能力都提出了更高的要求。国家已经颁布了《信息安全等级保护管理办法》，对企业配备信息安全人员做出了硬性规定。

5. 个人用户对信息安全的需求

个人用户在信息安全方面有通信内容机密性、用户信息隐私性、应用系统可信性等需求。这就要求信息服务提供商要能满足用户的安全需求，也需要大量专门的信息安全人才。

我国高度重视网络安全工作。2014 年 2 月 27 日，中央成立网络安全与信息化领导小组，习近平总书记亲自担任组长。习总书记在第一次会议上强调指出：“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展。”网络安全和信息化是一体之两翼、双轮之驱动，必须统一谋划、统一部署、统一推进、统一实施。“没有网络安全，就没有国家安全；没有信息化，就没有现代化。”这一科学论断阐述了网络安全与国家信息化之间的紧密关系，使我们认识到

网络安全为国家信息化建设提供安全保障的极端重要性。习总书记的重要讲话精神，为我们做好网络空间安全学科专业建设注入活力，极大地增强了我们做好网络空间安全学科的信心。网络安全已成为国家安全的重要组成部分，要从根本上提高我国网络安全水平，健全网络空间安全保障体系，必须培养高素质的网络空间安全专业人才。

没有网络安全就没有国家安全。网络安全是一个关系到国家安全和社会稳定的重要问题。其重要性正随着全球信息化的步伐与日俱增。在我国，国家高度重视网络空间安全保障工作，网络信息安全上升至国家战略。2013 年 11 月 12 日，中国共产党中央国家安全委员会成立。2014 年 2 月 2 日，中央网络安全和信息化领导小组成立，习近平指出网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。2015 年 1 月 23 日，中共中央政治局召开会议，审议通过《国家安全战略纲要》，指出要做好各领域国家安全工作，大力推进国家安全各种保障能力建设，把法治贯穿于维护国家安全的全过程。2015 年 4 月 20 日，《国家安全法（草案）》二审稿增加了国家“建设国家网络与信息安全保障体系，提升网络与信息安全保护能力”“维护国家网络空间主权”的规定。2015 年 7 月 1 日，第十二届全国人民代表大会常务委员会第十五次会议通过新的国家安全法。

1.2 网络空间安全学科研究的主要内容

网络空间（Cyberspace）是通过全球互联网和计算系统进行通信、控制和信息共享的动态（不断变化）虚拟空间，在信息时代是社会有机运行的神经指挥系统，目前已经成为继陆、海、空、太空之后的第 5 空间。在网络空间里不仅包括通过网络互联的各种计算系统（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。

与其他空间不同的特点是，网络空间没有明确的、固定的边界，也没有集中的控制权威。而网络空间安全（Cyberspace Security，CS）研究网络空间中的安全威胁和防护问题，即在有敌手（Adversary）的对抗环境下，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。网络空间安全不仅包括传统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性。这里，需要明确信息安全、网络安全、网络空间安全概念的异同，三者均属于非传统安全，均聚焦于信息安全问题。网络安全、网络空间安全的核心是信息安全问题，只是出发点和侧重点有所差别。信息安全使用范围比较广，可以指线下和线上的信息安全，既可以指称传统的信息系统安全，也可以指网络安全和网络空间安全，但无法完全替代网络安全与网络空间安全的内涵；网络安全可以指信息安全或网络空间安全，但侧重点是线上安全和网络社会安全；网络空间安全可以指称信息安全或网络空间安全，但侧重点是与陆、海、空、太空并列的空间概念。网络安全、网络空间安全、信息安全三者相比较，前两者反映的信息安全更立体、更宽域、更多层次，也更多样，更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。

网络空间安全涉及数学、计算机科学与安全、信息与通信工程等多个学科，已形成了一个相对独立的教学和研究领域。建立网络空间安全一级学科的目标是，通过网络空间安全

学科的培养，帮助学生掌握密码和网络空间安全基础理论和技术方法，掌握信息系统安全、网络基础设施安全、信息内容安全和信息对抗等相关专门知识，并具有较高网络空间安全综合专业素质、较强的实践能力和创新能力，能够承担科研院所、企事业单位和行政管理部门网络空间安全方面的科学研究、技术开发及管理工作。

如图 1-1 所示，网络空间安全学科主要研究方向及内容如下。

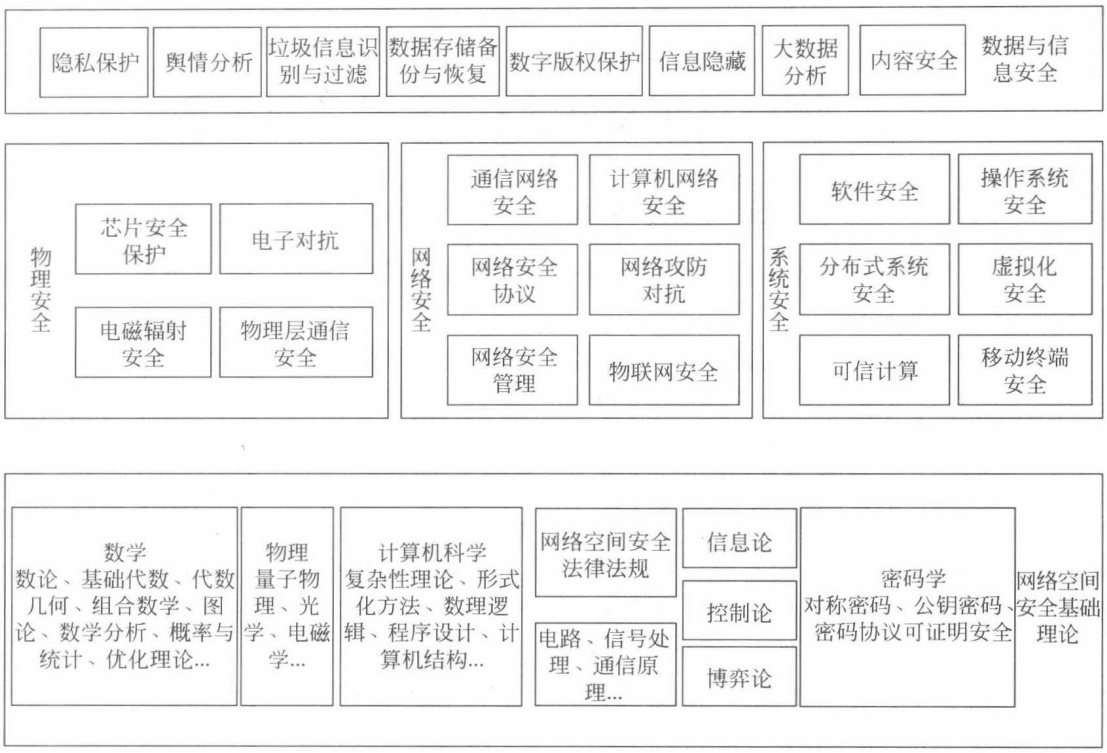


图 1-1　网络空间安全学科体系

网络空间安全基础理论：为其他方向提供理论、架构和方法学指导；包括从事网络空间安全研究工作所需要的数学、物理、电工学、计算机科学与技术、信息论、控制论、博弈论、密码学理论、网络空间安全法律法规等基础理论。

物理安全，包括芯片安全防护、电子对抗、电子辐射的安全、物理层通信安全等方面的理论与技术。

系统安全，保证网络空间中单元计算系统安全、可信；包括软件安全、操作系统安全、分布式系统安全、虚拟化安全、可信计算、移动终端安全、工业控制系统安全等方面的理论与技术。

网络安全，保证连接计算机的网络自身安全和传输信息安全；包括各类无线通信网络、计算机网络、物联网等的安全协议，攻防对抗、网络安全管理、取证与追踪等方面的理论与技术。

数据与信息安全，包括隐私保护、数据存储与恢复、数字版权保护、舆情分析、垃圾信息识别与过滤等方面的理论与技术。

网络空间安全一级学科的理论方法和方法论基础，涉及数学、信息论、计算复杂理论、控

制论、系统论、认知科学、博弈论、管理学等。其学科方法论基础：信息安全学科有其独特的方法论，与数学或计算机科学等学科的方法论既有联系又有区别。包括观察、实验、猜想、归纳、类比和演绎推理，以及理论分析、设计实现、测试分析等，综合形成了逆向验证的方法论。沈院士表示，信息安全保障体系是一个复杂的系统，必须从复杂系统的观点，采用从定性到定量的综合集成的思想方法，追求整体效能。从系统工程方法论的观点出发，网络空间安全不能简单地采用还原论的观点处理，必须遵循“木桶原理”，注重整体安全。

1.3 网络空间安全对人才培养的新要求

1.3.1 我国网络空间安全面临的形势

目前，网络空间和网络空间安全成为社会公众关注的话题，网络空间安全人才培养体系更成为人们关注的焦点。

近年来，随着社会信息化的不断加深，各种信息安全风险也伴随而生。国际上围绕网络空间安全的斗争愈演愈烈，争夺网络空间安全控制权是战略制高点。我国的网络空间面临着来自外部的威胁，近年来发生的许多安全事件表明，我国已经在网络空间安全方面处于极为被动的局面。“斯诺登事件”给我们的经验和教训是广泛而深刻的，在网络空间，围绕信息安全的斗争是激烈的。“斯诺登事件”也给我国敲响了一个警钟，再也不能用一般的力量、行动和认识对待网络空间安全问题。“斯诺登事件”证明美国在网络空间方面是有规划、有计划、成体系地部署和构建攻击力量，动员全社会资源发展系列化的高技术手段以达到网络空间行动绝对自由的战略目的。“斯诺登事件”给我们的启示是，不能用一般力量来对付体系力量，应采取信息化条件下的体系对抗策略，积极构建网络空间安全学科体系，使我国网络信息安全人才成体系化、规模化、系统化培养，更好地满足国家安全对网络信息安全人才的需要。

我国已成为网络大国，由于网络技术基础薄弱和网络空间安全人才不足，我国还不是网络强国。网络安全关系到国家安全、社会稳定、经济发展、人民生活等各个方面，必须确保我国的信息安全，要建设国家信息安全保障体系，政府、军队、公安等国家重要部门，以及金融、电力、能源等重要基础设施等都需要大量信息安全专门人才。据不完全统计，截至 2014 年年底，我国重要行业信息系统和信息基础设施需要各类网络空间安全人才 70 万，预计到 2020 年，需要各类网络空间安全人才约 140 万人，而目前我国高等学校每年培养的信息安全相关人才不足 1.5 万人，远远不能满足网络空间安全的需要。

1.3.2 网络空间安全一级学科

网络空间安全人才培养是国家信息安全保障体系建设的基础和先决条件，网络安全学科建设则是高层次创新型信息安全人才培养的关键。网络空间安全人才培养是一个完整的社会系统工程，只有在一级学科目录规范下，才能按学士、硕士、博士成体系、全方位地培养国家需要的网络空间安全各类人才。

事实上，网络空间安全学科在我国经过十多年的发展，理论和技术已经较为成熟。主要体现在以下几个方面：一是网络空间安全学科具有明确的研究对象，并形成了相对独立的