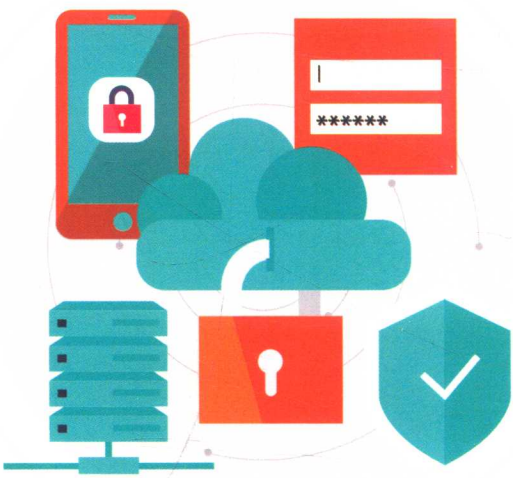
GENERAL COURSE ON CYBERSPACE SECURITY

# 网络空间安全通识教程

陈铁明◎编著




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

GENERAL COURSE ON CYBERSPACE SECURITY

# 网络空间安全通识教程

陈铁明◎编著

人民邮电出版社
北京

**图书在版编目（CIP）数据**

网络空间安全通识教程 / 陈铁明编著. -- 北京 : 人民邮电出版社, 2019.10
ISBN 978-7-115-50775-4

Ⅰ. ①网… Ⅱ. ①陈… 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023431号

## 内 容 提 要

本书系统地介绍了网络空间安全涵盖的基本概念、基础原理与技术特点。全书内容共9章，包括网络空间安全、网络协议基础、密码学与应用、网络安全防范、操作系统安全、数据安全与内容安全、互联网安全、物联网安全、新技术安全，并在相应章节中对网络空间安全基本概况与发展现状、基于TCP/IP的互联网协议基础、应用密码算法、区块链技术、网络渗透与黑客知识、网络攻防技术基础、社会工程学、操作系统发展史、数据备份与恢复、数字水印与隐写取证、Web网站应用安全、移动App安全、Wi-Fi与蓝牙安全、无线电与智能硬件安全、人工智能与大数据安全等知识内容与热点技术做了简要阐释，旨在让读者对网络空间安全所涉及的各个领域的基础知识有一个整体全面的了解。

本书内容详实，具有一定基础理论和较强的实用参考价值。本书适用于大专院校网络安全通识课程或普高中职信息技术大学先修课程，也可作为网络空间安全初学者入门教程。

◆ 编　　著　陈铁明
责任编辑　王　夏
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：700×1000　1/16
印张：12.5　　2019年10月第1版
字数：245千字　　2019年10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

网络空间已成为国家继陆、海、空、天四大疆域之后的第五疆域，网络空间安全已成为关系到国家政治、国防、社会安定等的关键因素。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和生活的重大战略问题，没有网络安全就没有国家安全。《中华人民共和国网络安全法》的施行说明国家将从法律上着手保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化的健康发展。

2015 年，“网络空间安全”一级学科的设立标志着网络空间安全进入了崭新的教科时代，体现了网络空间安全在国家教育体系中的地位。2016 年，中央网信办与发改委、教育部等六部门联合印发《关于加强网络安全学科建设和人才培养的意见》，进一步说明国家对网络安全实战型人才的培养要求迫切。第四届乌镇世界互联网大会上发布的报告指出，到 2020 年，中国网络安全人才缺口将达 150 万。2017 年，国家互联网信息办公室发布《国家网络空间安全战略》，对实现建设网络强国的战略目标产生了深远影响，而有效地开展规模化的网络空间安全人才培养也已成为当务之急。

自 2016 年开始，中央网信办已做出重要决策，将每年 9 月的第三周设立为国家网络安全宣传周，以此来推动全社会共同维护网络安全的实际行动，旨在增强网络安全意识、普及网络安全知识、提高网络安全技能。最近，教育部也修订颁发了《普通高中信息技术课程标准》，其中明确提到了了解信息系统与社会的安全风险、从数据管理与分析模块中认识和了解数据备份和数据安全、从网络技术应用模块中了解网络主要结构与协议等要求，大幅度提升了青少年对网络空间安全等知识面的要求，因此亟需配套的教程来支撑信息技术教学大纲。事实上，在目前的市场上，要么是缺乏技术细节的科普教程，要么是专业性较强的理论教程或技术性较强的实践教程。本书是对网络空间安全技术体系全面介绍的引导教程，既可满足中职高中的基础知识教学需求，也可为后续深入相应的专业技能或从事相关的研究，提供有效的导入式通识学习路径。

2017 年 9 月，浙江省率先启动了网络空间安全终身教育工程，尤其是兼顾将

青少年网络安全教育提升到战略高度。在此背景下，我们精心编写了此教程，既涵盖了新版信息技术相关课程的基础知识，又概述了网络空间安全的入门知识，有助于青少年建立对网络空间安全知识框架的基本认知，也可为大专院校学生的网络安全通识学习提供参考。

本教程在编写过程中，得到了浙江省网络空间安全创新研究中心、浙江工业大学网络空间安全协会、网络安全通在线学习平台等研究人员的大力支持，郑毓波、陈嘉烙、徐康、张灵洁、金成强、张嘉琦等参与了内容整理与实验准备工作，在此一并表示感谢！

本教程内容涵盖网络空间安全基本概念及相关技术、人才、法律等现状，网络协议基础，密码学基础及应用，网络安全防范技术基础，操作系统安全，数据与内容安全，互联网安全，物联网安全，新技术安全等，以入门引导为目的，全面系统地介绍了网络空间安全涉及的知识面，还介绍了人工智能、大数据等最新的技术面临的安全问题，可作为大专院校网络空间安全通识课程教材，也可作为中职或高中开设网络安全创新大学先修课程的参考教程。

# 目 录

# 第1章 网络空间安全

## 1.1 网络空间安全概念

### 1.1.1 起源与历史

在接触网络空间安全之前，我们不得不提到一个重要的名词——赛博空间（Cyberspace）。赛博空间指的是计算机以及计算机网络里的虚拟现实，是由科幻小说作家威廉·吉布森在他的长篇小说《神经漫游者》中首次提出的。

随着信息技术应用的发展以及计算机等技术的普及，赛博空间也从最早描述的虚拟空间逐渐延伸到人类可感知的现实生活中，例如最新提出的空天信一体化系统等，已将卫星通信系统、计算机系统、互联网等融为一体构成网络空间。赛博空间是人类科技发展创造的新型空间，但是随着赛博空间的逐步扩展，其对个人隐私、信息安全、应用安全乃至国防安全等都将产生强大的冲击，引发新的安全问题。

### 1.1.2 定义与概念

➢ 网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或恶意的原因遭到破坏、泄露，确保系统能连续可靠正常的运行，网络服务不中断。

传统的信息安全问题主要解决 CIA，即保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）。随着网络技术的发展渗透，网络安全不仅仅指网络通信层面的安全保障，广义上的网络安全已和信息安全的研究范畴没有太明确的区分，也可以说网络安全就是网络上的信息安全。

➢ 网络空间安全

针对网络空间，就有了网络空间安全。网络空间安全的概念较网络安全更为广义，不仅涵盖了传统的网络安全技术，还包括所有信息空间网络互联网环境的物理安全、系统安全、数据安全、应用安全等各类问题及其安全管理体制、法律法规等的总和。

➢ 各国对网络空间安全的定义

2008 年，美国国家安全总统令 54 号、国土安全总统令 23 号将网络空间界定为：互相依赖的信息技术基础设施，包括互联网、电信网、计算机系统以及关键行业中的嵌入式处理器和控制器。“网络空间”这个词还常用于指信息和人们互动的虚拟环境。

《加拿大网络安全战略》（2010）将网络空间定义为：网络空间是由互联的信息技术网络和其上的信息构成的电子世界。它是一个全球公域，将超过 17 亿人连接在一起交换想法、提供服务和增进友谊。

《德国网络安全战略》（2011）将网络空间定义为：网络空间是全球范围内在数据层连接的所有 IT 系统组成的虚拟空间。网络空间的基础是互联网这一普遍的和公开的可接入和传输的网络，该网络可由任意数量的数据网络进行补充和进一步扩大。孤立的虚拟空间中的 IT 系统不属于网络空间的组成部分。

《法国信息系统防卫和安全战略》（2011）将网络空间定义为：由世界互联的自动数字数据处理设备构成的通信空间。

《新西兰网络安全战略》（2011）将网络空间定义为：由相互依赖的信息技术基础设施、电信网和计算机处理系统组成的进行在线通信的全球网络。

《英国网络安全战略》（2011）将网络空间定义为：网络空间是指由数字网络组成的交互式领域，用于存储、修改和交流信息。它包括互联网，还包括其他支撑我们商业、基础设施和服务的信息系统。

国际标准化组织在《信息技术——安全技术——网络安全指南》（ISO/IEC 27032：2012）中将网络空间定义为：通过连接到互联网上的技术设备和网络，由互联网上人们的互动、软件和服务所形成的不具有任何物理形态的合成环境。

➢ 网络空间的构成

1. 网络设备

网络空间是由计算机、智能终端、路由器、交换机、缆线等硬件设备联网构成的电子空间，这些硬件设备是构成网络空间的物理层。一些联网的移动终

端如手机、移动电脑也是构成网络空间的一部分。以上的所有设备都统称为网络设备。

2. 软件和协议

软件和协议用于帮助设备之间处理和传输信息，没有软件和协议的帮助，任何设备都不可能成为网络空间的一部分。

软件是一系列按照特定顺序组织的计算机数据和指令的集合。软件主要是给计算机系统或用户提供一系列的功能或特定的功能。

协议则是为了在计算机网络中进行数据交换而建立的规则、标准或约定的集合。协议主要规定了数据如何发送、设备之间如何建立连接，简单来说就是按照怎样的顺序做怎样的事。

3. 信息

从广义上来说，信息可以泛指人类社会传播的一切内容。对于计算机网络来讲，信息主要是指电子线路中传输的信号。网络最重要的意义在于处理、存储和传输信息，因此网络设备上生成、存储和传输的信息是网络空间的必备要素。网络上的信息主要表现为电子数据形态。

4. 网络主体

网络空间的主体非常广泛，包括网络建设者、运营者、服务提供者、监督管理者、用户等。其中最主要的是网络服务提供者和用户。

5. 网络行为

网络空间是虚拟的电子空间，人们通过实施各种网络行为与其他网络主体发生社会关系，形成人与人、人与计算机的互动。网络行为主要包括网络信息行为和网络技术行为。网络信息行为以信息为对象，例如，访问浏览网页信息、下载和上传信息、播放网络音/视频、接收或发送电子邮件、入侵或破坏信息系统、窃取或篡改信息等。网络技术行为主要有网络技术开发、网络维护、程序的升级等。正是因为有人的活动，才使网络社会得以形成。

➢ 网络空间的特点

1. 虚拟性

网络空间是一个电子空间，没有三维属性；网络空间的任何东西都是由计算机代码构成的。因此从三维物理空间的角度讲，网络空间是虚拟的空间。

2. 现实性

当今的互联网是一种面向公众的全球性设施。网络空间中的信息也是实实在在的信息，只是改变了传统的存储介质。通过网络，任何人或组织之间都可以互相分享信息和互动，网络空间与现实空间已经实现了融合，成为一个融合空间，即新形态的现实空间。

3. 社会性

每个上网者及网站和网页都是互联网的节点，节点连接节点，交织成网，形成网络节点联系的体系，构成互联网上的社会交往体系，即网络社会。

### 1.1.3 网络空间安全名词解释

➢ 互联网

互联网又称为因特网，始于1969年美国的阿帕网。将计算机网络互相连接在一起的方法称为“网络互联”，在这个基础上发展的覆盖全世界的全球性互联网络称为互联网。互联网并非万维网，万维网是一个基于超文本相互链接而成的全球性系统，且是互联网所能提供的服务之一。

➢ 信息安全

信息安全是指信息的机密性、完整性和可用性的保持。根据美国《可信计算机系统评价准则》TCSEC的定义，信息安全具有以下特征。

机密性：确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体。

完整性：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。

可用性：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

➢ 物联网

物联网（Internet of Things，IoT）是互联网、传统电信网等的信息承载体，可以让所有能行使独立功能的普通物体实现互联互通的网络。物联网一般为无线网，由于每个人周围的设备可以达到 1 000～5 000 个，因此物联网可能要包含500M～1 000M个物体。在物联网上，每个人都可以使用电子标签将真实的物体在网上连接，然后查出它们的具体位置。通过物联网，可以用中心计算机对机器、设备、人员进行集中管理、控制，也可以对家庭设备、汽车进行遥控，还可以搜索位置、防止物品被盗等，类似自动化操控系统。同时，通过收集这些小数据，最后可以聚集成大数据，用于包含重新设计道路以减少车祸、都市更新、灾害预测与犯罪防治、流行病控制等有关社会的重大改变。

物联网将现实世界数位化，其应用范围十分广泛。物联网拉近分散的信息，整合物与物的数字信息。物联网的应用领域主要包括运输和物流领域、健康医疗领域、智能环境（家庭、办公、工厂）领域、个人和社会领域等，具有十分广阔的市场和应用前景。

➢ 大数据

大数据又称为巨量资料，指的是传统数据处理应用软件不足以处理其规模的复杂数据集。在总数据量相同的情况下，与个别分析独立的小型数据集相比，将各个小型数据集合并后进行分析可得出许多额外的信息和数据关系，可用来察觉商业趋势、判定研究质量、避免疾病扩散、打击犯罪或测定即时交通路况等。

➢ 云计算

云计算是一种基于互联网的计算方式，通过这种方式，共享的软硬件资源和信息可以按需提供给计算机各种终端和其他设备。云计算是继 1980 年大型计算机到客户端–服务器的大转变之后的又一种巨变。用户不再需要了解“云”中基础设施的细节，不必具有相应的专业知识，也不需要直接进行控制。云计算描述了一种基于互联网的新的 IT 服务增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源。

## 1.2　网络空间安全威胁与现状

### 1.2.1　网络空间安全的威胁

随着社会对网络和信息系统依赖性的增加，网络空间面临的威胁也与日俱增。网络和信息安全牵涉国家安全和社会稳定。

从国际上看，国家或地区在政治、经济等各领域的冲突都会反映到网络空间。网络空间这个虚拟世界有其无可比拟的特点，可以对国家安全构成威胁。第一，网络空间没有明确、固定的边界，资源分配不均衡，导致网络空间的争夺异常复杂；第二，网络空间没有集中的控制权，网络武器极易扩散；第三，网络空间具有极强的隐蔽性，发动者可以藏身于一个无人知晓的地方发动门槛极低的网络攻击，并且不留下任何痕迹；第四，网络空间包含事关国计民生和国家安全的国防信息基础设施。

就社会生活而言，网络空间的安全威胁涉及网络漏洞、个人信息安全、网络冲突与攻击、网络犯罪等。网络漏洞是指计算机系统软硬件、网络协议、系统安全方面存在的缺陷，而这些缺隐可以被无授权的攻击者利用，对数据进行窃取、操控，进而破坏网络系统。服务商、员工人为泄露用户信息，黑客通过黑客技术盗取信息数据，将会导致个人信息安全受到严重威胁。除了国家之间的网络冲突与攻击之外，企业间或利益集团间也存在着网络冲突与攻击。网络信息窃取、虚假广告等网络犯罪频率也呈现出快速上升的趋势，同时其智能性、隐蔽性和复杂

性使取证更加困难。

网络空间的安全威胁按照行为主体的不同，可划分为黑客攻击、有组织网络犯罪、网络恐怖主义以及国家支持的网络战这 4 种类型。

网络空间安全已经成为国家安全战略的重要组成部分。以互联网为基础的信息系统几乎构成了整个国家和社会的中枢神经系统，其安全可靠运行是整个社会正常运转的重要保证。如果这个系统的安全出了问题（如受到入侵或瘫痪）必将影响整个社会的正常运转。

### 1.2.2 网络空间安全的现状

随着综合国力的不断提升和互联网技术的普及，我国已成为名副其实的网络大国。截至 2017 年 12 月，我国的网民人数达到 7.5 亿人，上市互联网企业总市值突破 9 万亿元，这促使我国开始关注自身在网络空间的利益，并在国际社会提出网络主权的主张，同时也在国内进行了相关立法。2010 年，《中国互联网状况》白皮书指出，互联网是国家重要基础设施，中华人民共和国境内的互联网属于中国主权管辖范围，中国的互联网主权应受到尊重和维护。《中华人民共和国国家安全法》和《中华人民共和国网络安全法》都使用了“网络空间主权”一词，来表达以国家力量保障网络空间安全的法律意志。

2016 年 12 月 27 日经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》，阐明中国关于网络空间发展和安全的重大立场，指导中国网络安全工作，维护国家在网络空间的主权、安全、发展利益。

此外，英国、德国、法国、日本、澳大利亚、韩国等多个国家也制定了其各自的网络空间安全战略。在国际层面，2011 年，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦向联合国大会第 66 届会议联合提交了信息安全国际行为准则，指出重申与互联网有关的公共政策问题的决策权是各国的主权，对于与互联网有关的国际公共政策问题，各国拥有权利并负有责任。2013 年，联合国信息安全政府专家组（UNGGE）达成的最后报告，确认国际法，特别是《联合国宪章》适用网络空间，并表示国家主权和源自主权的国际规范和原则适用于国家进行的信息通信技术活动，以及国家在其领土内对信息通信技术基础设施的管辖权。UNGGE 在 2015 年报告中继续强调国际法、《联合国宪章》和主权原则的重要性，它们是加强各国使用信通技术安全性的基础，并指出：“各国在使用信通技术时，除其他国际法原则外，还必须遵守国家主权、主权平等、以和平手段解决争端和不干涉其他国家内政的原则。国际法规定的现有义务适用于国家使用通信技术。”

## 1.3　网络空间安全人才培养

目前，网络空间安全人才的培养得到了许多国家的高度重视，美国、俄罗斯、日本等多个国家出台了国家网络安全战略，制定了专门的网络安全人才培养计划。例如，美国启动“国家网络空间安全教育计划”，期望通过国家的整体布局和行动，在信息安全常识普及、正规学历教育、职业化培训和认证这 3 个方面建立系统化、规范化的人才培养制度，全面提高美国的信息安全能力。为加强我国高素质网络空间安全人才的培养，2015 年 6 月，“网络空间安全”正式被国务院学位委员会和教育部批准为国家一级学科。2016 年 6 月，经中央网络安全和信息化领导小组同意，中央网信办、发改委、教育部、科技部、工信部和人社部六部门联合印发了《关于加强网络安全学科建设和人才培养的意见》，该意见要求：在已设立网络空间安全一级学科的基础上，加强学科专业建设。发挥学科引领和带动作用，加大经费投入，开展高水平科学研究，加强实验室等建设，完善本专科、研究生教育和在职培训网络安全人才培养体系。有条件的高等院校可通过整合、新建等方式建立网络安全学院。通过国家政策引导，发挥各方面积极性，利用好国内外资源，聘请优秀教师，吸收优秀学生，下大功夫、大本钱创建世界一流网络安全学院。近两年，各相关高校响应国家培养网络安全人才的号召，陆续设立了“网络空间安全学院”。

在《中华人民共和国网络安全法》颁布后的仅一个多月，2016 年 12 月 27 日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布的《国家网络空间安全战略》提出，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和创新园区，形成有利于人才培养和创新创业的生态环境。

2017 年 8 月 23 日，国家网络安全学院等六大项目的集中开工，标志着国家网络安全人才与创新基地建设进入实质性阶段。

## 1.4　网络空间法律法规

在我国网络空间安全保障体系构成要素中，网络空间安全法规与政策为其他要素和网络空间安全保障体系提供必要的法律保障和支撑，是我国网络空间安全保障体系的顶层设计，对切实加强网络空间安全保障工作、全面提升网络空间安全保障能力具有重要意义。

网络空间安全事关国家安全和经济建设、组织建设与发展，我国从法律层面

明确了网络空间安全相关工作的主管监管机构及其具体职权。

法律层面，在保护国家秘密方面有《中华人民共和国保守国家秘密法》等相关法律；在维护国家安全方面有《中华人民共和国国家安全法》等相关法律；在维护公共安全方面有《中华人民共和国警察法》和《中华人民共和国治安管理处罚法》等相关法律；在规范电子签名方面有《中华人民共和国电子签名法》。

行政法规层面，有《中华人民共和国计算机信息系统安全保护条例》对计算机系统及其安全保护进行定义；《商用密码管理条例》中，商用密码是指对不涉及国家密码内容的信息进行加密保护或安全认证所使用的密码技术和密码产品，未经许可任何单位或个人不得销售商用密码产品。

随着互联网的高速发展，2000 年，国务院令第 292 号公布《互联网信息服务管理办法》。2001 年，国务院令第 339 号公布《计算机软件保护条例》，并在 2011 年进行了第一次修订，2013 年进行了第二次修订。

2010 年 6 月 8 日发布的《中国互联网状况》白皮书中进一步提出："互联网是国家重要基础设施，中华人民共和国境内的互联网属于中国主权管辖范围，中国的互联网主权应受到尊重和维护。""同时依法保障公民在互联网上的言论自由，保障公众的知情权、参与权、表达权和监督权。""中国恪守世界贸易组织成员应履行的普遍性义务和具体承诺义务，依法保护外资企业在华合法权益，并积极为在华外资企业依法开展与互联网相关的经营业务提供良好的服务。"这些政策的宣示，初步展现出我国对于网络空间国际治理的基本主张。

2015 年 7 月，《中华人民共和国网络安全法（草案）》第一次向社会公开征求意见。2016 年 11 月 7 日，全国人大常委会表决通过《中华人民共和国网络安全法》。2017 年 6 月 1 日，《中华人民共和国网络安全法》施行。它明确了国家加强保护个人信息、打击网络诈骗的决心。

对当前我国网络安全方面存在的热点难点问题，《中华人民共和国网络安全法》都有明确规定。针对个人信息泄露问题，《中华人民共和国网络安全法》规定：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并且取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或非法向他人提供个人信息。同时，它还规定了相应的法律责任。

针对网络诈骗多发态势，《中华人民共和国网络安全法》规定：任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗、传授犯罪方法、制作或销售违禁物品、管制物品等违法犯罪活动的网站、通迅群组，不得利用网络发布涉及实施诈骗、制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。同时，它还规定了相应的法律责任。

此外，该法在关键信息基础设施的运行安全、监测预警与应急处置等方面都做出了明确规定。

所以在法律日益完善的当今社会，拥有良好的法律意识也是至关重要的。在学好网络安全技术的同时，也要做一位遵纪守法的好公民，为未来国家的网络空间安全事业贡献力量。