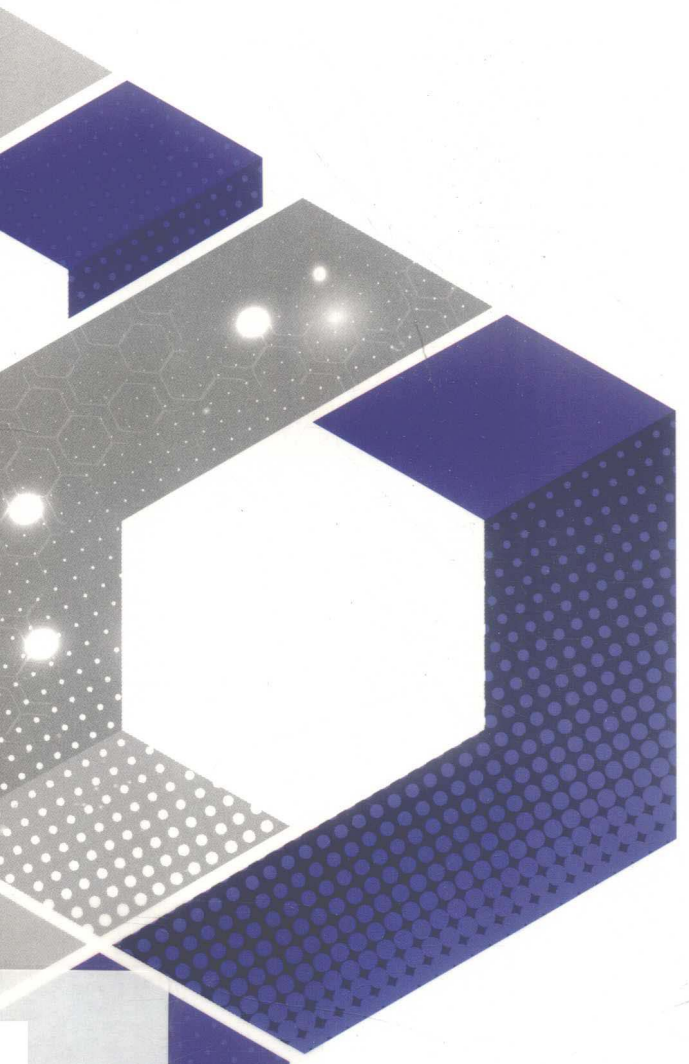
21世纪高等学校网络空间安全专业规划教材

# 网络空间安全素养导论

◎ 黄波 主编　马颜军 副主编

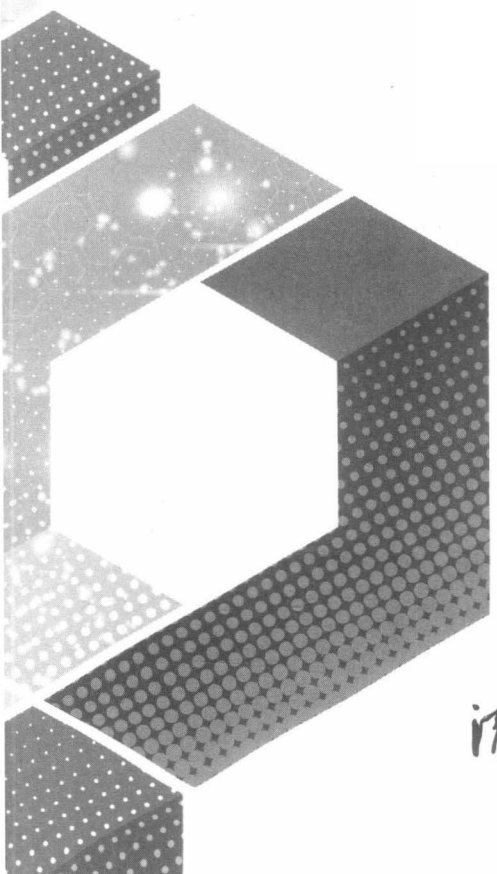


清華大學出版社

21世纪高等学校网络空间安全专业规划教材

# 网络空间安全素养导论

◎ 黄波 主编　马颜军 副主编



清華大學出版社
北京

## 内 容 简 介

网民是网络社会的细胞，只有网民的网络素养普遍提高，网络社会的机体才能始终保持健康。大学生是网民的重要组成群体，其网络及网络安全素养会影响当下和未来的网络空间安全。编写一本基础性较强的网络空间安全使用及管理教材将有利于学生深入了解网络安全知识体系，对网络空间安全方面的个人素养及未来职业素养的培养及教育起到引领作用。

本书的主要目标是通过公共基础通识课程提高大学生的网络空间安全素养。本书内容涵盖网络文化安全、网络操作技能安全、互联网应用安全、网络安全法律法规等。学习本书可以了解网络安全的重要意义，掌握网络安全基础知识、基础理论和基础技能，养成网络空间安全行为习惯，提高网络安全防范意识以及网络空间安全的个人素养和职业素养。

本书可以作为网络空间安全相关专业的入门基础教材，也可以作为其他专业的网络空间安全知识普及教材，也适合于对网络空间基本知识、安全技能、安全应用感兴趣的人员参考。



**图书在版编目(CIP)数据**

网络空间安全素养导论/黄波主编. —北京：清华大学出版社，2019
(21世纪高等学校网络空间安全专业规划教材)
ISBN 978-7-302-52766-4

Ⅰ. ①网… Ⅱ. ①黄… 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069208号

**责任编辑**：闫红梅　张爱华
**封面设计**：刘　键
**责任校对**：徐俊伟
**责任印制**：宋　林

**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**：北京富博印刷有限公司
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　　张**：14.5　　**字　　数**：346千字
**版　　次**：2019年8月第1版　　**印　　次**：2019年8月第1次印刷
**印　　数**：1～1500
**定　　价**：39.00元

产品编号：080375-01

# 前言

互联网技术与应用的迅猛发展给世界的政治、经济、文化、社会带来巨大影响，尤其是近年来网络安全事件频发，危害政治安全，威胁经济发展，侵蚀文化进步，破坏社会秩序，严重影响着网络空间安全。目前网络空间安全已然成为一个公共问题，如何提高网民整体防御网络安全事件的能力，降低信息泄露风险，保护公民个人信息数据的安全，迅速提高网民的网络安全意识和网络安全操作技能，进而提升全体网民的网络空间安全素养，是当前急需解决的重要课题，也是网络信息时代给人们提出的新要求。

国家网络空间安全的战略目标之一就是安全，其不仅包括有效控制网络安全风险，健全、完善国家网络安全保障体系，保证核心技术装备安全可控，保证网络和信息系统运行稳定、可靠等，而且要有满足需求的网络安全人才，大幅提高全社会的网络安全意识、基本防护技能和使用网络的信心。提高全体网民的网络空间安全素养已然成为当务之急。本书在探索网络空间安全理论的基础上，根据课程基本要求，深入浅出地介绍了网络文化与网络空间安全的关系，提出个人网民的基本网络空间安全素养的构成，进而讲述了加密应用、系统安全、互联网应用安全、安全工具使用等基本技能，并将网络空间安全法律体系展现给读者，帮助读者提高网络空间安全意识并掌握网络空间安全的基本技能和法律知识。

网络空间安全素养隶属普及型内容，全体网民都应提高网络空间安全意识和技能。目前关于网络安全的教材与参考书已经很多，但大多数都是网络空间安全的重要理论和技术原理介绍，这样的教材适合于网络空间安全专业、信息安全专业的本科生或研究生使用。而对于非网络空间安全相关专业的学生来说，网络安全知识及技能的培养同样是十分重要的，当前涉及网络文化、网络基本知识、网络安全应用实例、网络安全操作技能、网络空间安全治理等交叉学科知识的网络空间安全的教材较少，本书解决了这一实际问题。本书本着基础理论知识必需、够用的原则，结合目前网络空间安全应用及网民网络生活实际，将近年来出现的实用技术、新型技术及互联网安全使用写入教材，并融入网络空间文化、网络空间法律等基础知识。

本书是编者在多年教学、研究积累的基础上，紧密围绕提高大学生的网络空间安全素养这一基本目标，结合网络空间实际应用的主体安全知识架构，编写的一本涵盖网络文化安全、网络操作技能安全、互联网应用安全、网络安全法律法规等多学科交叉、侧重实际应用的教材。本书共8章，其中：

第1章主要介绍网络文化与网络空间安全，网络空间安全的现状、概念与发展机遇，网络空间安全素养构成等方面的内容，由黄波编写；第2章主要介绍网络空间安全威胁、网络空间安全防护措施，由黄波编写；第3章主要介绍网络基础知识、Internet与信息系统概述，由冯晶莹编写；第4章主要介绍加密技术应用中的数据加密、密码应用，由黄波编写；第5章主要介绍Windows操作系统安全、移动终端操作系统安全，由黄波、冯晶莹共同编写；第6章主要介绍网络空间安全中的漏洞、恶意代码和网络攻击、常用安全工具的使用，由王晓强编写；第7章主要介绍互联网安全使用基础，互联网社交、商务、娱乐等方面的个人隐私保护与安全，由马颜军编写；第8章主要介绍网络空间安全法律法规体系、信息安全标准体系、网络空间安全实务，由黄波编写。全书由黄波统阅定稿。本书可以作为网络空间安全相关专业的入门基础教材，也可以作为其他专业的网络空间安全知识普及教材，也适合于对网络空间基本知识、安全技能、安全应用感兴趣的人员参考。

由于网络空间安全涉及的知识领域广泛，且编者水平有限，书中难免有疏漏之处，敬请广大读者提出宝贵意见，并恳请各位专家、学者给予批评指正。

编　者

2019年2月

# 目录

# 第1章 网络空间安全概述

网络空间安全已然成为信息时代人类共同面临的新挑战。网络作为国家关键信息基础设施和新的生产、生活工具，在政治、经济、文化、生活等方面发挥的作用日益扩大。网络的极速发展促进了信息传递、共享与交互，促进了社会生产效率、人民生活水平与经济的发展，同时维护网络空间安全的重要性也日益突出。目前，网络空间的不安全因素使得世界各行各业的安全受到严重威胁，如何实现和保障网络空间安全已成为保障国家安全与社会稳定的重要问题之一。

## 1.1 网络文化与网络空间安全

### 1.1.1 网络文化概述

网络文化是一种全新的文化表达形态，认识网络文化可以从两个角度切入：一个是从网络的角度看文化，另一个是从文化的角度看网络。前者从网络的技术性特点出发，突出技术变革引发的文化变迁；后者从文化的特性出发，强调网络内容的更迭引发网络空间的新型文化形势。网络文化是网络新兴技术与社会文化内容的综合体，是现代科技与传统文明的结晶，是传统文化在网络信息时代的创新。目前关于网络文化存在各种各样的观点，单纯强调某一方面都不妥当。

网络文化是指网络上具有网络社会特征的文化活动及文化产品，是以网络物质创造发展为基础的网络精神创造。从广义上讲，网络文化是网络时代的人类文化，是人类现实社会传统文化、传统伦理的延伸和多样化的展现。从狭义上讲，网络文化是以计算机技术、网络信息技术以及网络经济为基础，在网络空间形成的文化活动、文化方式、文化产品、文化观念的集合，包括工作、学习、交往、休闲、娱乐、商务等所形成的网络空间内容及参与者的价值观念和社会心态等各个方面。可以说，人类现实社会的文化和文明在网络时代受多种因素的影响，网络文化已经对现实社会的文化发展与传承产生巨大的影响。网络文化的主题往往就是现实社会经济生活的体现，网络内容源于现实生活，网络文化的发展归根结底是现实社会文化发展的重要体现。

自从计算机及网络出现，网络文化就伴随着世界上其他人类社会文化的特征而持续发展着。互联网的产生是国际化的，随着世界上每个国家开放互联网，世界各国的网络文化不仅有各自国家特色的社会文化内涵，而且也在世界各个国家之间相互影响。这使得网络文化不仅仅只局限于某一国家、某一地区或某一民族，世界各地的网络文化相互融

合，在网络空间形成国际性的网络文化。

我国作为世界网络大国，在网络文化建设发展中推陈出新。我国的网络文化是中国特色社会主义文化的重要组成部分。发展健康向上的网络文化不仅是适应互联网快速发展、增强国家整体文化实力的关键，也是净化网络环境、维护社会稳定、保护国家安全的重要基础。我国发布的《2006—2020年国家信息化发展战略》中明确指出："建设积极健康的网络文化。倡导网络文明，强化网络道德约束，建立和完善网络行为规范，积极引导广大群众的网络文化创作实践，自觉抵御不良内容的侵蚀，摈弃网络滥用行为和低俗之风，全面建设积极健康的网络文化。"

《2006—2020年国家信息化发展战略》中确立了我国信息化发展的战略之一是建设先进的、积极健康的网络文化，这是我国网络文化体系建设的重要目标。随着网络空间技术的发展、利用程度及安全状况的变化，我们更应与时俱进，促进网络文化体系的新发展、新变化，努力推进网络文化建设，坚持网络文化内涵建设，提高网络文化产品及服务的质量与能力，提升网络行为的精神文明程度，建设符合我国特色的社会主义网络文化的生态环境，让我们的网络文化坚持为人民服务、为社会主义服务的方向，最大限度地满足人民群众对健康网络文化的需求，促进整个社会的和谐。

### 1.1.2 网络空间安全理解

目前网络空间已然成为人类生存的"第五空间"，网络空间既是人类的生存环境，也是信息的生存环境。网络空间是所有信息系统的集合，人在其中与信息相互作用、相互影响。国家互联网信息办公室2016年12月27日发布的《国家网络空间安全战略》指出："网络空间安全事关人类共同利益，事关世界和平与发展，事关各国国家安全。"因此，网络空间安全是人和信息对网络空间的基本要求，网络空间安全面临的问题更加综合、更加复杂。

网络空间安全由于不同的环境和应用而产生不同的类型。

**1. 系统软件安全**

系统软件安全主要是指系统级软件的安全，包括操作系统、网络系统、数据库系统等相关软件安全，主要侧重于保证各类系统软件的正常运行与安全运维，避免系统软件崩溃、系统漏洞、物理运维等因素对存储、处理和传输的数据信息造成破坏和损失。

**2. 信息系统安全**

信息系统安全主要包括各类网络应用服务、各行业各部门应用的信息系统安全。它既要能保证信息系统的运行安全，又要能保证信息系统中的数据存储、处理和传输的安全，避免网络攻击、信息泄露、系统功能等因素对存储、处理和传输的数据信息造成破坏和损失。其中涉及的主要应用包括用户认证、口令鉴别、信息数据加密、数据存取权限、用户访问控制、行为安全审计、计算机病毒防治等方面。

**3. 信息内容安全**

信息内容安全主要包括保证互联网传播的信息内容符合国家法律法规、规章规范，符合普遍认可的社会道德伦理，避免出现绝密或私密信息、各类恶意代码、淫秽色情信息、暴力邪恶视频等内容的处理、存储与传播。其本质是保护国家利益、社会意识形态、社会公

共秩序和用户个人隐私。

不同层面、不同用户对网络安全的具体理解和需求也不同。

从国家安全及保密部门的角度，要对网络上传播的非法的、有害的或涉及国家机密的信息进行监测、过滤和处置，避免有害信息被传播、重要信息被泄露，避免国家关键信息基础设备遭受破坏，避免对国家、社会产生危害或造成巨大损失。

从社会教育和意识形态的角度，要对网络上有害的、低俗的、暴力的信息内容进行治理、管理和引导，这些不良信息会对社会秩序的稳定和人类的发展造成阻碍，必须避免网民接触不良网络信息，抵制有害信息传播，提升网络文化的底蕴与内涵。

从网络运行和管理者的角度，要对网络运营者建设、运营、管理的信息系统的访问、读写等操作进行保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务、资源非法占用和非法控制等网络威胁和网络攻击。

从网络用户的角度，要对网民在网络上传输的涉及个人隐私或商业利益的信息进行机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯或损坏用户的利益和隐私，避免其他人对用户自身的设备或使用的信息系统进行非法访问和破坏。

### 1.1.3　网络文化与网络空间安全的关系

网络文化与网络空间安全之间存在重要关系，可以说网络文化与网络空间安全之间相互影响、相互制约。网络文化能够充分体现网络空间整体的文明程度，健康的网络文化发展有利于网络空间安全的良性发展。我们应从多重角度思考网络文化与网络空间安全的关系，对于世界上任何一个进入网络时代的国家，网络文化与网络空间安全应体现一个国家、一个民族的伦理观、道德观、价值观，且很多传统文化会慢慢地在网络空间意识形态下被传播与继承。

网络文化包含各种信息内容的安全，立足于网络空间安全的角度，可以通过物质技术、管理制度和精神文明三个层面来保障。对于网络文化与网络空间安全的关系，实际上要站在不同层面、不同角度来理解。

从国家层面上来说，网络文化是以网络为载体的文化，一个国家能在网络上独立自主地决定自己国家的政治制度、经济制度、文化制度、社会制度以及适合本国意识形态的伦理观、道德观和价值观，同时也能够保护本国人民自有的传统文化在网络空间上的表现形态，并扩大优秀文化的传承与发展，那么这个国家的网络文化就是安全的。

从行业层面上来说，网络文化传播依托于网络空间服务平台，各类网站上的论坛、博客、播客、音乐、游戏、视频、新闻等信息服务，各类网络即时通信中的群组交流、用户互通等交互交流，这些服务内容不能危害国家安全，不能损害国家荣誉和利益，并且不能散布谣言、淫秽色情、暴力恐怖信息等一切法律、行政法规禁止的内容。

从社会意识形态层面上来说，网络文化应促进社会进步，以伦理道德、社会先进文化知识为传承，维护网民权益，通过多种宣传形式对网民进行培训、引导、教育以及社区服务。往往社会意识形态层面的网络文化也能影响现实社会文化，能够弘扬新时代网络主流旋律，倡导社会精神文明、优秀传统文化和现代文化精华。

从网络信息技术的层面上来说，网络文化依赖于网络信息技术的支撑，保证网络空间中信息传播的完整性、可用性、可控性、不可抵赖性、合法性等特性，这些特性是评价网络文化健康程度及安全性的重要因素。通过网络信息技术措施，可避免网络空间中有害信息传播、网民权益侵害、网络攻击侵入等事件。

## 1.2 网络和网络空间安全现状

### 1.2.1 网络及互联网发展现状

网络是计算机技术与通信技术紧密结合的产物，一般说来，网络是一个复合性的系统，其通过各种通信手段、网络终端、连通设备及介质相互连接起来，进行信息交换、资源共享、协同工作等。最早的网络就是因特网(Internet)，是由美国国防部高级研究计划局(ARPA)建立的。现代计算机网络的许多概念和方法都来自阿帕网(ARPANET)。早在1977年，ARPANET推出了TCP/IP体系结构和协议，这使得ARPANET可以通过TCP/IP协议进行转换工作。1980年以ARPANET为主干网建立了初期的Internet。1988年Internet开始对外开放。1991年在连接Internet的计算机中商业用户首次超过学术界用户，这是Internet发展史上的一个里程碑，从此Internet的成长速度一发不可收拾。

2018年1月30日，互联网数据研究机构We Are Social和Hootsuite共同发布的“数字2018”互联网研究报告中指出，全世界的网民总数约为40.21亿人。目前，全世界范围内新增的网民大多来自移动终端，随着智能手机的售价和移动流量资费的降低，越来越多的人选择通过移动智能终端进入互联网。仅2017年就有超过2亿人拿到第一台移动设备。全球的总人口中超过2/3的人至少拥有一台移动设备，唯一移动用户(Unique Mobile Users)的总数达到51.35亿，移动互联网的渗透率已经高达68%。不仅上网的人数在增多，而且人们在网上花费的时间也越来越长。整体上网民对互联网的依赖度越来越高，据报告数据显示，全球网民的平均上网时间已经达到每天6小时，说明每一个上网的网民除睡觉以外至少有1/3的时间都用来上网。

我国Internet的起步以1987年通过中国学术网(CANET)向世界发出第一封E-mail为标志。经过几十年的发展，形成了四大主流网络体系，主要包括中国科技网(CSTNET)、中国公用计算机互联网(CHINANET)、中国教育和科研计算机网(CERNET)、中国金桥信息网(CHINAGBN)。据《中国互联网络发展状况统计报告》显示，截至2018年6月30日，我国共有网民8.02亿人，其中手机网民7.88亿人，我国网民使用手机上网的比例高达98.3%，移动智能终端上网使用率逐年升高，台式机、笔记本电脑上网比例下降；我国即时通信用户规模达7.56亿人；网络新闻用户规模达6.63亿人；网络购物用户规模达5.69亿人；网上外卖用户规模达3.64亿人；网上支付用户规模达5.69亿人；网络直播用户规模达4.25亿人；共享单车用户规模达2.45亿人；网络约出租车用户规模达3.63亿人；在线政务服务用户规模达4.70亿人。互联网已经发展成为我国影响最广、增长最快、市场潜力最大的产业之一，正在以超出人们想象的深度和广度迅速地发展。在规模上，我国已经成为名副其实的“网络大国”。

### 1.2.2　网络空间安全现状

随着网络信息技术的高速发展，互联网已经成为当代先进生产力的重要标志，互联网已经渗透到社会的各个方面，伴随而来的是人们对网络空间安全的需求越来越高。对网络空间安全的需求从单一的通信保密，发展到今天的网络空间安全产品、技术、手段等方面。网络和信息化的发展让人们充分享受到世界信息开放、资源共享的便利，但同时也给人们带来了众多的网络空间安全方面的困扰。

近年来，电信诈骗、黑客攻击、勒索软件、物联网攻击、APT 攻击、个人信息泄露、国家级别的网络间谍战、暗网犯罪、比特币攻击等新名词层出不穷，各种各样的网络安全事件频繁出现。从“棱镜门”事件到席卷全球的 WannaCry、暗云Ⅲ、Petya 等网络勒索病毒，从现实社会的传统犯罪到各种新型的网络犯罪，网络空间安全形势日益严峻，应对网络空间安全事件面临严峻挑战。网络信息技术创新发展的同时也伴随很多安全问题，木马与僵尸网络、移动恶意程序、拒绝服务攻击、系统安全漏洞、网站篡改侵入等各类网络安全威胁不断涌现，各种网络攻击事件层出不穷，新型安全威胁与传统安全问题相互交织，网络用户面临的网络安全风险不断加大。

当前面临的网络空间安全方面的任务日益复杂和多元，网络空间安全问题已成为信息时代人类共同面临的挑战。网络空间安全关乎人类共同利益，关乎世界各个国家的安全，关乎世界和平与发展。全世界各个国家、各个行业越来越重视网络空间安全，世界各国日益加大网络空间安全相关领域的建设。伴随着世界各国对网络空间安全的认识程度的变化，我国国内的网络空间安全问题也日益突出。如何解决这些问题，保障网络空间安全，早已成为当前全民共同的努力目标。网络已然改变了人类传统的工作、生活和生产的方式，必须努力使得网络空间健康、有序、安全发展，使其更好和更安全地为人类服务。

目前我国已初步建成了国家层面的网络空间安全的组织保障。2014 年，中央网络安全和信息化领导小组成立。领导小组将着眼国家安全和长远发展，统筹协调各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，为推动国家网络安全和信息化法治建设提供保障。同时，近年来我国也制定了一系列重要的网络信息安全管理标准和必需的网络空间安全治理的法律法规、规章规范及司法解释。为实施国家网络安全战略，加快网络空间安全高层次人才培养，我国已经增设“网络空间安全”一级学科，我们已经认识到要从根本上提高我国网络空间安全水平，在健全网络空间安全保障体系的同时，必须培养高素质的网络空间安全专业人才。

网络空间环境的复杂性、多变性以及网络信息系统的脆弱性，决定了网络空间安全威胁的客观存在。随着国际政治形势的发展以及经济全球化进程的加快，信息科技时代所引发的网络空间安全问题不仅涉及国家的经济安全、政治安全，同时也涉及社会安全、文化安全，更应该加强网络空间国际合作，促进网络空间安全。可以说“没有网络安全，就没有国家安全”。目前，我国急需建立符合要求的网络空间安全保障体系，以提升我国网络空间安全的防御能力。

## 1.3 网络空间安全基础概述

### 1.3.1 网络空间安全基本概念

网络空间安全是近年来新生的一种理论。网络空间安全的英文是 Cyberspace Security。早在 1982 年，加拿大作家威廉·吉布森在其短篇科幻小说《燃烧的铬》中就创造出 Cyberspace 一词，意指由计算机创建的虚拟信息空间。Cyberspace 是信息环境中的一个整体域，由独立且互相依存的信息基础设施和网络组成。

现如今的“网络空间安全”在早些年的提法是“计算机信息系统安全”。其中我国《中华人民共和国计算机信息系统安全保护条例》的第三条规范了包括计算机网络系统在内的计算机信息系统安全的概念：“计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。”

关于网络世界中的安全概念，普遍理论中相继提出过信息安全、网络安全、网络信息安全、网络空间安全等不同说法。20 世纪 90 年代“信息安全”被广泛使用，进入 21 世纪的十几年来，“网络安全”“网络信息安全”“网络空间安全”等逐渐被提出，近年来，“网络安全”和“网络空间安全”开始成为社会和业界普遍认同的概念。目前理论上广泛定义的“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，不因偶然的或者恶意的原因而遭受破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。继 2003 年美国发布《网络空间安全国家战略》后，2014 年我国在首届互联网大会上设立了“网络空间安全”的主题板块，“网络空间安全”这一概念成为当下最流行的说法。

无论是网络安全还是网络空间安全，理解其含义都应从不同的角度考虑。网络安全（Network Security）反映的安全问题基于网络，可以认为它是基于互联网的发展应用及网络社会面临的安全问题提出的；网络空间安全反映的安全问题基于网域空间，与陆域、海域、空域、外太空域四大空间一起作为全球全人类及世界各国的公域空间，如果从全球空间安全问题提出和思考网络空间安全，可以说其范畴更广。网络空间安全是人和信息对网络空间提出安全保障的基本需求，网络空间包含所有信息系统的集合，同时也包括人与信息系统之间的相互作用、相互影响。可以说，网络空间安全是在实现信息安全、网络安全过程中所有网络空间要素和各领域网络活动免受各种威胁的状态。因此，网络空间安全问题更加综合、更加复杂。

### 1.3.2 网络空间安全的特性

网络空间安全涉及国家、社会、企业和个人生活等各个层面，从本质上说就是保护网络空间信息系统的硬件、软件和系统数据的安全。网络空间安全保护的对象是信息，其中信息的保密性、完整性和可用性是网络空间安全的基本特性。除基本特性外，还包括可控性、不可抵赖性、合法性等特性，这些特性是实现网络空间安全所要达到的目标，也是构建网络空间安全保障体系的重要依据。

**1. 保密性**

保密性(Confidentiality)是指保证关键信息和敏感信息不被非授权者获取、解析或恶意利用。信息的保密性针对信息被允许访问对象的多少而不同。所有人员都可以访问的信息为公开信息；需要限制访问的信息一般为敏感信息或秘密，如国家秘密、企业和社会团体的商业或工作秘密、个人隐私秘密等。实际上国家秘密可以根据信息的重要性及保密要求分为不同的密级，根据秘密泄露对国家经济、安全利益产生的影响及后果不同，一般将国家秘密分为秘密、机密和绝密三个密级，各类组织可根据其网络信息安全的实际，在符合《中华人民共和国保守国家秘密法》的前提下将其信息划分为不同的密级。

**2. 完整性**

完整性(Integrity)是指保证信息从真实的信源发往真实的信宿，在传输、存储过程中未被非法修改、替换、删除，体现未经授权不能访问的特性。信息的完整性主要包括两方面：一方面是指信息在利用、传输、存储等过程中不被篡改、丢失或缺损等；另一方面是指信息处理方法的正确性，如误删除文件等不当操作有可能造成重要文件的丢失。信息的完整性是信息网络安全的基本要求，也是信息网络安全的重要特性之一。

**3. 可用性**

可用性(Availability)是指保证信息和信息系统可随时为授权者提供服务而不被非授权者滥用和阻断的特性。网络的基本功能就是为用户提供信息和通信服务。用户对于信息和通信的需求是多样化的、随机的、实时的。为保证用户的需求，网络和信息系统必须是可用的，也就是信息及相关的信息资产在授权人需要的时候，可以立即获得使用。例如，通信线路中断故障会造成信息在一段时间内不可用，影响正常的商业运作，这是网络通信可用性的破坏。

**4. 可控性**

可控性(Access Control)是指对信息、信息处理过程及信息系统本身都可以实施合法的安全监控和检测，实现信息内容及传播的可控能力。信息的可控性主要指对危害国家的信息进行监控审计，控制授权范围内信息的流向及行为方式，使用授权机制控制信息传播的范围、内容。

**5. 不可抵赖性**

不可抵赖性(Non-repudiation)是指保证出现网络空间安全问题后可以有据可查，网络空间通信的过程中可以追踪到发送或接收信息的目标人或设备，又称信息的抗抵赖性。信息的不可抵赖性是对出现的安全问题提供调查的依据和手段，使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者无法抵赖，实现信息网络安全的可审计。

**6. 合法性**

合法性(Legitimacy)是指保证信息内容和制作、发布、复制、传播信息的行为符合一个国家的宪法及相关法律法规。我国网络空间传输的信息具有中国特色，不仅包括信息、数据安全的本身特性，还具有国家、社会对网络空间信息所要求的内容合法性。这一特性也是近几年国内外网络空间安全研究的一个热点。

### 1.3.3　网络空间安全发展机遇

网络空间安全涉及多学科、多领域，知识结构和体系包括的内容既宽泛又有深度。作

为一种新兴事物，网络空间安全的发展、挑战与机遇并存。世界上存在很多事物，无论是现在正在发展的，还是未来将要出现的，它们都将面临网络空间安全的巨大挑战。

**1. 大数据**

大数据(Big Data)是指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合。它需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力，适应海量、高增长率和多样化的信息资产。随着大数据在科学计算、政府服务、社会应用、商业应用等多领域的高速发展，大数据的研究及安全问题将成为未来一段时期内网络空间安全的重要内容之一。可以说对于大数据的研究，能够进一步捍卫国家网络空间的数字主权安全，对维护国家的安全稳定、经济与社会的健康发展具有重要意义。

多种流数据的存储、多源数据的混合、传感器数据的安全、分析处理数据的安全等使得目前的大数据处理面临巨大挑战。同时需要应对的大数据安全问题也日益严峻，如何建立实时、智能的大数据安全保障机制，制定大数据建设、安全等相关标准，完善大数据系统安全体系是当前十分重要的任务。

**2. 云计算**

云是互联网的一种比喻说法。云计算(Cloud Computing)基于互联网的相关服务的增加、使用和交付模式，涉及通过互联网提供动态的、易扩展的、虚拟化的资源。云计算可以实现每秒 10 万亿次的运算，在拥有强大的计算能力后，它可以模拟核爆炸、预测气候变化和市场发展趋势。一般用户通过计算机、手机等智能终端接入数据中心，按自己的需求进行云运算。云计算主要包括基础设施即服务(IaaS)、平台即服务(PaaS)、软件即服务(SaaS)等多层次的服务。

云计算服务的应用带来相应的云安全(Cloud Security)问题，云安全是一个从云计算演变而来的新名词。云安全通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序、网络攻击的信息，进而推送到服务器端进行自动分析和处理，再把针对木马病毒、网络攻击等的解决方案分发到每一个客户端。云安全的策略构想是：使用者越多，每个使用者就越安全。因为如此庞大的用户群足以覆盖互联网的每个角落，只要某个网站被挂马或某个新木马病毒出现，就会立刻被截获。

**3. 万物互联**

万物互联(Internet of Everything)的定义是将人、流程、数据和事物结合在一起，使得网络连接变得更加相关、更有价值。今天的互联网，正在从“人人相联”向“物物相联”迈进，即通过万物相联，渗透到各个产业，产业互联网呼之欲出，这就意味着各行各业，如制造、医疗、农业、交通、运输、教育，都将在未来 20 年被互联网化。万物互联加速数字世界的爆炸性增长。物理世界的数字化时代日益改变着人们的生活、工作、学习、研究的模式。

伴随着物联网的发展，它的安全问题也备受关注。网络是万物互联的通信连接基础，恶意用户可以通过万物互联的任何终端试图篡改系统后访问企业、家庭等内部网络和资源，许多设备同时访问网络资源时，也能造成网络堵塞和资源危机。万物互联后，恶意用户可以通过危害单台设备达到再逐步渗透到整个网络的目的。