高等学校网络空间安全专业“十三五”规划教材

网络空间安全法律法规解读

主编　王永全　廖根为

西安电子科技大学出版社
http://www.xduph.com

XDUP 538500
封面设计：倚天

高等学校网络空间安全专业“十三五”规划教材

- 网络空间安全导论
- 操作系统安全
- 数据库安全
- 系统安全
- 信息论基础
- 信息安全数学基础
- 现代密码学与网络安全技术
- 密码学基础教程
- 新编密码学
- 信息安全技术
- 网络空间安全基础
- 网络安全技术
- 网络安全技术原理与实训教程
- 软件安全技术
- 硬件安全威胁与防范技术
- 通信网与安全
- 网络安全与保密
- 无线网络安全系统设计
- 信息内容安全
- 网络内容安全
- 协议理论安全及其分析
- 信息安全风险评估
- 信息安全管理与风险评估
- 网络对抗原理与技术
- 入侵检测技术
- 逆向工程及分析技术
- 恶意代码原理、对抗与防范
- 漏洞分析与应用
- 大数据安全
- 物联网安全
- 电子商务安全与管理
- 电子数据证据理论与实务
- 电子数据取证技术
- 电子数据取证与司法鉴定
- 信息隐藏与数字水印
- 图像隐写于分析技术
- 工业控制安全
- 工业控制系统网络安全
- 区块链与加密货币
- 移动智能终端安全
- 网络舆情分析概论
- 网络空间安全法律法规解读
- 应用密码学实验
- 密码安全实践
- 网络空间安全技术实践教程
- 网络对抗实验教程

ISBN 978-7-5606-5083-8
9 787560 650838 >
定价：50.00元

高等学校网络空间安全专业“十三五”规划教材

网络空间安全法律法规解读

主　编　王永全　廖根为

撰写人员(以撰写章节为序)

廖根为　黄道丽　王永全

龙　敏　詹　毅　沈臻懿

西安电子科技大学出版社

内 容 简 介

本书以网络空间安全法律保护为视角，分析了网络空间安全法律保护特征和法律体系，对现有网络空间安全法律体系进行深入解读，分别从国家政策、行政处罚、刑事处罚、民事侵权、诉讼程序等五个方面共七章对现有相关法律法规进行了梳理、汇总和精选，针对重点法条、法律难点问题、法律法规衔接问题、典型案例等进行了深入分析。

本书既可以作为网络空间安全相关专业的教材，也可以作为其他专业学生自学网络空间安全法律的教程，还可以作为网络空间安全领域工作者、计算机取证与司法鉴定行业工作者、法律实务人员的参考用书。

图书在版编目(CIP)数据

网络空间安全法律法规解读/王永全，廖根为主编. —西安：西安电子科技大学出版社，2018.11
ISBN 978-7-5606-5083-8

Ⅰ. ① 网… Ⅱ. ① 王… ② 廖… Ⅲ. ① 计算机网络—科学技术管理法规—基本知识—中国 Ⅳ. ① D922.174

中国版本图书馆 CIP 数据核字(2018)第 224059 号

策划编辑 陈 婷
责任编辑 张 玮
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西天意印务有限责任公司
版 次 2018 年 11 月第 1 版 2018 年 11 月第 1 次印刷
开 本 787 毫米×1092 毫米 1/16 印张 22.25
字 数 529 千字
印 数 1～3000 册
定 价 50.00 元
ISBN 978-7-5606-5083-8/D
XDUP 5385001-1

高等学校网络空间安全专业“十三五”规划教材

编审专家委员会名单

前言

QIANYAN

随着网络应用的飞速发展和网络用户规模的不断扩大，网络空间已然和人们的社会生活紧密相连。与此同时，在这一虚拟的空间范围中所发生的侵权、违法与犯罪案件与日俱增。网络空间面临国防安全、政治安全、经济安全、文化安全等方面的风险，仅凭传统技术手段难以全面应对网络空间中的各类安全挑战，亟需综合应用法律、管理、技术、伦理、道德等多方面的途径来对网络空间安全予以保护。在此之中，网络空间安全的法律途径保护是极为重要的环节之一。这不仅需要网络空间安全和计算机等相关专业的学习、研究和工作者，对该领域的相关法律法规有较为深入的了解与掌握，而且也需要全社会各行业从业者及社会民众加以学习和了解，以引起大家充分的重视。

鉴于此，《网络空间安全法律法规解读》一书依托西安电子科技大学出版社“网络空间安全专业系列教材”项目，汇聚了华东政法大学、公安部第三研究所、知名律师事务所等高校、科研单位、实务部门从事网络空间安全法律与技术研究的专业人员，对网络空间安全法律体系和现有法律进行了深入探讨。全书共分 8 部分，包括绪论和 7 个章节。绪论部分论述了网络空间安全法律保护的特征和现有法律体系，提出了网络空间安全的法律保护是对信息资源的全方位保护，是对个人、社会和国家利益的全方位保护，是对信息系统整个生命周期的全过程保护，是对网络空间安全威胁行为的全过程控制与防范。第 1～7 章，从国家政策、行政处罚、刑事处罚、民事侵权、诉讼程序等 5 个方面对现有网络空间安全法律体系中所涉法律法规进行了梳理、汇总和精选，针对重点法条、法律难点问题、法律法规衔接问题、典型案例等作了深入分析。

本书在一定程度上，填补了国内在网络空间安全法律法规解读上的空白。希望通过本书的抛砖引玉，能够进一步推动网络空间安全领域法律制度的深入研究。

作者(以撰写章节为序)及其分工如下：

廖根为：绪论、第 6 章

黄道丽：第 1 章、第 5 章

王永全：第 2 章

龙　敏：第 3 章

詹　毅：第 4 章

沈臻懿：第 7 章

本书由主编王永全、廖根为负责全书设计、统稿、校对和完善。研究生史册、李文冠、赵子玉为本书的部分资料收集与校对亦做了相关工作，在此予以感谢！本书的出版得到西安电子科技大学出版社“网络空间安全专业系列教材”项目和国家社科基金重大项目“涉信息网络违法犯罪行为法律规制研究”（编号：14ZDB147）支持，在此一并致谢！

限于时间、经验和知识水平等因素，书中难免会存在一些不足之处，尚祈读者能多提供宝贵意见，以资日后进一步完善。

编　者

2018 年 3 月

目录

MULU

绪 论

信息技术的日新月异发展，极大推动了社会发展和改变了人们的生产生活方式，但与此同时也带来了较大的安全风险。随着物联网、云计算、人工智能、大数据技术的不断发展，网络空间安全风险的程度和广度也进一步加剧。运用技术和法律来保护网络空间安全均是必不可少的保护手段。而良好的法律保护不仅需要规范网络空间行为，降低安全风险，打击违法犯罪行为，更要有利于促进网络空间安全技术的发展，维护国家、社会和个人的合法利益。要达到以上目标，就需要不断发展和完善网络空间安全法律，以下从应然和实然两个角度进行分析。

一、网络空间安全法律保护的特征

1. 网络空间安全的法律保护是一种全方位的保护

(1) 网络空间安全的法律保护是对信息资源的全方位保护。

网络空间安全问题均与信息资源有关，对网络空间安全的法律保护应涵盖所有的信息资源类型。根据信息资源类型的不同，对信息资源保护可划分为信息载体的保护、信息运行的保护、信息价值的保护、信息内容的保护。

对信息载体的保护，主要是从信息载体角度出发对信息安全进行保护。信息不可能单独存在，其存储和运行均依赖一定的物理载体。如果物理载体遭受破坏，信息运行安全将受到威胁。而在信息载体保护中，信息基础设施保护十分重要，其中关键信息基础设施的保护尤为重要，它是信息安全保护的前提和基础。

对信息运行的保护，主要是从信息的运行角度对信息安全进行保护。信息社会中，能体现信息价值的重要方面之一是信息共享，共享的信息均是通过信息系统进行传输和处理的。信息不能够安全传输、转换、处理、交换、存储，便无法正常运行。只有对信息运行进行保护，信息才能够真正实现共享和交换，信息资源的优势也才能真正体现。对信息安全运行进行保护是信息安全保护的关键和核心。

对信息价值的保护，主要是从信息本身的价值出发对信息的安全进行保护。信息社会中，信息是最重要的资源，信息是有价值的。因此，破坏这种有价值的信息应给予相应的处罚。虽然信息共享与交换是信息社会中信息运行的主要目的，但有些有价值的信息同时也具有一定的专有性。为了更好地保护这些信息资源，需要对这些信息进行专门保护。在大数据时代，信息价值属性不断扩张，其呈现的价值内涵具有复杂性和综合性特点，对这些信息价值的保护是信息安全保护的重要内容。

对信息内容的保护，主要是从信息的内容出发对信息的安全进行保护。信息是信息社会最重要的资源，信息内容是有使用价值的。这里的信息内容是指电子数据通过计算机系统、网络或者移动终端等设备和软件所呈现的内容。那些无用或有害的信息内容没有价值，不能成为信息社会可使用的信息资源。有害信息不仅不能推动社会的发展，反而会阻碍信

息社会的发展。但信息内容有害与否的评价又与一个国家的政治制度、社会文化有密切关系，对其保护方式与其内容和所处特定法域有密切联系，因而对信息内容的保护是信息安全保护的重要社会目标。

(2) 网络空间安全的法律保护是对个人、社会、国家利益的全方位保护。

网络空间与现实空间不同，但最终都是由现实中的人参与的。也就是说，网络空间安全的破坏，必然表现为对现实空间的人、社会、国家利益的损害。网络空间安全法律的保护应是对个人合法利益、社会公共利益和国家利益的全方位保护。

首先，网络空间安全的法律保护，必须保护国家安全利益。网络空间没有现实空间那样清晰的边界，网络空间主权容易受到忽视。在如今信息爆炸时代，哪个国家掌控了信息网络，哪个国家就占领了政治、军事和经济较量的战略制高点，因而制网权的较量成为大国之间较量的新焦点。通过法律对网络空间安全进行保护，不仅是为了宣示和明确网络空间的主权，更重要的是通过法律明确网络空间的国家安全战略，引导社会资源有效配置，将有限资源落实到网络空间的国家主权保障、关键信息基础设施的保护、关键和敏感数据的保护、个人数据安全保护以及落实国家网络空间安全保障工作的体系化和高效运作上。通过对国家安全利益的保护，将那些信息系统建设、运行、维护和使用过程中可能危及国家安全的信息活动通过行政处罚、治安处罚、刑事处罚等措施予以制裁，从而有效保护政治安全、经济安全、文化安全和军事安全，预防因网络空间安全问题引起的国家安全利益的重大损失。

其次，网络空间安全的法律保护，必须保护社会公共秩序以及公民的涉及网络的各项合法权益。由于网络在社会生活中的不可替代性和用户群的不断增长，无论其作为一项设施、一种工具、一种媒介、一个场所，还是一种财产等，若不对其相关活动进行法律规制，就有可能危及公共安全、社会公共秩序、财产以及公民的人身、民主权利。因此，应通过制定专门法律、增加刑法条文、完善治安管理处罚法、制定相关司法解释等手段予以法律规制，使其适用于新的领域。同时也要通过民法、侵权责任法、知识产权法等法律或者司法解释将网络出现的各种侵权行为予以规定和明确，确保公民的各项民事权益。

2. 网络空间安全的法律保护是一种全过程的保护

(1) 网络空间安全的法律保护是对信息系统整个生命周期的全过程保护。

当前，我国有关网络空间安全的法律尚在不断发展完善中。网络空间安全法律体系不仅仅是简单的对一般违法犯罪或者侵权行为的规制，更重要的目标应同时包括促进网络社会和相关产业的健康发展，保障国家安全和公共安全，规范网络社会活动秩序等。网络空间安全法律应贯穿于网络安全保护的各个环节、各个阶段，通过法律的规制、指引作用，使网络空间安全保护的各种要素高效组合，促使网络空间安全技术和管理的不断快速发展，有效控制网络空间安全风险因素。即网络空间安全的法律保护涉及信息系统的整个生命周期，包括系统规划、系统分析、系统设计、系统实施、运维及消亡等阶段。通过国家、行业组织和企业的管理或监督指导，按照法律设定的风险防范手段，逐一排查可能影响国家安全、社会公共利益、个人合法权益的因素，保障信息系统处于规定的安全可控的状态。

在系统建设阶段，应根据信息系统对国家安全、社会秩序和公共利益可能造成损害的程度确定合理的保护等级，并在安全产品的选择和使用上进行检查或控制；在系统运营阶段，国家信息安全监管部门应根据系统的重要程度实施相应的检查、监督或者指导工作。信息系统无论在建设、运营、报废过程中都需要依据国家管理规范、技术标准或者业务特殊安

全需求实施相应的管理，通过法律对相关责任主体设定必要的职责和义务，违反者需承担相应的法律责任。通过法律法规对信息系统生命周期中的每一阶段涉及的安全产品或软件、人、系统实施有效管理制度，通过全过程的安全保护将网络空间安全掌握在可控状态。

(2) 网络空间安全的法律保护是对网络空间安全威胁行为的全过程控制与防范。

随着移动互联网、物联网、云计算、区块链等技术的发展和运用，网络中各种安全威胁行为越来越复杂，风险程度也越来越高。一些违法犯罪行为呈现交叉和融合趋势，犯罪产业链条十分明显。为了有效控制网络空间各类安全威胁行为，必须通过法律在国家政策、安全战略、管理制度、思想教育、技术措施、犯罪打击、国际合作等方面的安排对这些行为的意图产生过程、行为预备过程、与其他行为的结合过程、行为实施过程、行为结束和后结束等全过程予以专门控制。针对各种安全威胁行为的新特点和危害，通过政策和制度层面，加大关键信息基础设施的保护力度，健全网络安全保障体系，提高网络安全意识和水平，倡导和促进安全和谐网络环境的形成；通过提高法律处罚力度强化安全管理行为责任；通过刑事手段使一些安全威胁行为中的帮助行为正犯化、预备行为犯罪化、单位行为犯罪化，切断犯罪产业链条；通过犯罪控制手段创新违法犯罪处罚措施；通过国际合作和交流，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系；通过有针对性地对网络空间安全威胁行为各个阶段予以法律规制，阻止不同违法犯罪行为的交叉和融合，减少违法犯罪意图产生的数量，控制违法犯罪预备行为，加强安全威胁的风险预警，加大违法犯罪打击力度，减小违法犯罪行为的危害性后果，提高违法犯罪取证效率和水平，即对网络空间安全威胁行为实施全过程控制与防范。

二、网络空间安全现有法律体系

我国网络空间现有法律体系基本形成了以《中华人民共和国网络安全法》[①]、《全国人大常委会关于维护互联网安全的决定》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》等专门法律以及散见于刑法、民法、治安管理处罚法、三大诉讼法等传统法律中的相关规定为基础，以各种行政法规、部门规章为支撑的较为完善的法律体系，具体来说包括以下五个方面：

1. 网络空间安全政策相关的法律法规

没有网络安全就没有国家安全，构筑全方位的网络与信息安全治理体系是我国网络安全保障工作的重中之重。2017 年 6 月 1 日正式实施的《中华人民共和国网络安全法》，是全面规范国家网络空间安全监督与管理方面的基础性法律。它与 2016 年以来我国先后制定的《国家信息化发展战略纲要》、《“十三五”国家信息化规划》、《“十三五”信息化标准工作指南》、《国家标准化体系建设发展规划(2016—2020)》、《国家网络空间安全战略》、《网络空间国际合作战略》、《信息产业发展指南》、《网络关键设备和网络安全专用产品目录》、《互联网新业务安全评估管理办法》、《网络产品和服务安全审查办法》、《国家网络安全事件应急预案》等法律法规和规范性文件，以及《全国人大常委会关于维护互联网安全的决定》、《中华人民共和国治安管理处罚法》、《中华人民共和国刑法》、《中华人民共和国计算机信息系统安全保护条

① 特别说明：为了叙述方便，本书在以下对法条解释和分析的过程中对以“中华人民共和国”开头的部分法律法规采用简写的方式，如《中华人民共和国网络安全法》简称为《网络安全法》，其他同。

例》等法律法规中的有关规定共同组成了网络空间安全政策相关的法律体系。

2. 网络空间安全刑事处罚相关的法律法规

对于严重威胁网络空间安全，或者具有严重社会危害性的行为，需要通过刑法进行规制。与网络空间安全相关的犯罪包括与信息基础设施相关的犯罪、与信息运行相关的犯罪、与信息内容相关的犯罪、与信息价值相关的犯罪、与信息安全主体失职相关的犯罪等五类犯罪行为。其中，与信息内容相关的犯罪、与信息价值相关的犯罪这两类犯罪行为与传统犯罪比较相近，网络主要充当一个场所、工具或者媒介，例如网络色情、网络诈骗、网络盗窃、网络诽谤、网络赌博、网络知识产权侵权等，对于这一些犯罪行为不增加新的罪名，主要通过司法解释明晰其社会危害性严重程度的判断标准，使其适用于网络空间。对于与信息基础设施相关的犯罪、与信息运行相关的犯罪、与信息安全主体失职相关的犯罪在传统刑法中无对应罪名，需要通过不断在刑法中增加新的罪名以适应不断发展的新情况，我国刑法主要通过第二百八十五条、二百八十六条、二百八十七条规定了这些新型的犯罪，并通过相关司法解释对其如何适用进行了具体解释。

3. 网络空间安全行政处罚相关的法律法规

对于那些涉及网络的不构成犯罪但行政违法或治安管理违法的行为，通过行政处罚和治安管理处罚的措施予以规制。网络空间安全行政处罚相关的法律法规、部门规章较多，主要包括治安管理处罚法、行政处罚法，以及计算机信息系统安全保护条例、计算机信息网络国际联网安全保护管理办法、互联网信息服务管理办法、互联网上网服务营业场所管理条例、计算机病毒防治管理办法、互联网域名管理办法、电信条例等法律、行政法规和部门规章中的相关处罚规定。这些规定共同构成了网络空间安全行政处罚相关的法律。

4. 网络空间安全民事侵权相关的法律法规

如前所述，网络空间安全还广泛涉及民事侵权问题，包括名誉权、姓名权、隐私权、个人信息权、财产权、软件著作权、专利权等。这些侵权行为可能涉及行政处罚和刑事处罚，与此同时还应根据民事侵权责任予以分配。相关的法律法规和司法解释主要包括民法总则、民法通则、网络安全法、侵权责任法、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、计算机软件保护条例、信息网络传播权保护条例、《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》、《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》、《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》、《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》、《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》等。

5. 网络空间安全诉讼程序相关的法律法规

涉及网络的各种诉讼程序均离不开电子数据证据。电子数据的收集、鉴定、审查与判断等，与传统证据有很大区别。与网络空间安全诉讼程序相关的法律法规，除了传统的刑事诉讼法、民事诉讼法、行政诉讼法三大诉讼法外，还包括《全国人民代表大会常务委员会关于司法鉴定管理问题的决定》、《司法鉴定程序通则》、《公安机关鉴定规则》、《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》等。

第 1 章　网络空间安全政策法律法规

1.1　网络安全法解读

中华人民共和国网络安全法

（2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过）

【立法背景及目标】

信息化成为当今世界发展的主要趋势，也成为推动经济发展和社会变革的重要力量。然而，信息化带来的网络安全威胁范围和内容也在不断扩大和演化，全球网络安全形势与挑战日益严峻。世界范围内的网络安全问题在我国同样存在，除此之外，我国还面临着更为复杂的安全隐患。国内网络安全威胁和风险日益突出，并日益向政治、经济、文化、生态、国防等领域传导渗透。境外敌对势力把我国作为网络意识形态渗透与攻击的重点目标。网络空间主导权争夺激烈，数据跨境流动的监管缺失直接威胁我国网络主权和国家司法权力架构；多网域“跨际”和“供应链渗透”威胁着工控、能源、交通、金融、电力等关键信息基础设施的安全；境内大规模个人信息泄露事件不断发生，网络诈骗、非法入侵、系统攻击等更加频繁，严重威胁社会公共安全和个人的合法权益。

在“没有网络安全就没有国家安全，没有信息化就没有现代化”成为国家和民族共识之际，我国正式开启网络强国建设的一系列顶层设计和部署。2014 年 2 月 27 日中央网络安全和信息化领导小组正式成立，这标志着我国正式将网络安全提升至国家安全的高度，构筑全方位的网络与信息安全治理体系成为我国网络安全保障工作的重中之重。2016 年 7 月 27 日，中共中央办公厅、国务院办公厅发布《国家信息化发展战略纲要》。作为规范和指导我国未来 10 年国家信息化发展的纲领性文件，纲要进一步调整和发展了中期国家信息化发展战略，其中要求以信息化驱动现代化，加快建设网络强国。2016 年 12 月 27 日，我国《国家网络空间安全战略》正式发布，这是我国第一次向全世界系统、明确地宣示和阐述我国对于网络空间安全和发展的立场与主张，在我国网络空间安全领域具有里程碑意义。2017 年 3 月 1 日，外交部和国家互联网信息办公室共同发布《网络空间国际合作战略》，全面宣示了我国在网络空间国际治理问题上的基本原则和行动要点。这三个战略开启了我国网络空间治理的全新范式，为我国网络安全相关政策和法律的出台指明了方向。

纵观我国网络空间领域立法进程，2014 年是一个重要分水岭。2014 年之前颁布施行的信息安全立法涉及了法律、行政法规、部门规章、地方法规及规范性文件等多个层次：从涉及的领域来看，具体包括网络与信息系统安全、信息内容安全、信息安全系统与产品、保密及密码管理、计算机病毒防治等多个领域；从权利（力）角度来看，主要包括政府维护信息安全的职责、企业权益保障和个人信息权利保护等。这些法律相比于国际立法，内容相对

滞后，且各法律文件之间相互独立，呈碎片化，由此构建的信息安全立法框架显然无法有效应对日渐严峻的网络安全威胁。“棱镜门”事件暴露出维护国家数据主权、振兴民族产业的法律保障不足；能源、交通、金融、电力等国家关键信息基础设施建设、管理法制不健全，信息安全技术研究和产品开发政策法律保障乏力，在发生重大、突发事件和紧急状态的情况下，应急响应缺乏法律保障，应急预案、违法犯罪信息和安全测试等可以用于社会安全防范的信息难以共享，严重影响了快速反应能力、安全保障能力和统一调配能力。

面对严峻的网络安全形势，各界普遍认为，仅对原有法律的解释、修订或增补，难以把握好安全与发展之间的关系，不利于国家总体安全战略目标的实现，我国亟需制定综合性“网络领域基本法”，应当明确规定网络与信息安全的基线，为部门、地方的立法和政策的制定、调整和完善提供法律依据。2014 年 4 月，全国人大常委会年度立法计划正式将《网络安全法》列为立法预备项目，由此开启了我国国家网络安全立法的新进程。2015 年 7 月 6 日，作为网络安全基本法的《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，第十二届全国人民代表大会常务委员会第二十四次会议表决通过了《网络安全法》，并于 2017 年 6 月 1 日正式施行。《网络安全法》的实施标志着我国网络空间法制化进程的实质性展开，为我国有效应对网络安全威胁和风险、全方位保障网络安全提供了基本法律支撑。

第一章　总　　则

第一条 为了保障网络安全，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健康发展，制定本法。

【重点法条解读】

本条是关于网络安全法立法目的的规定。

立法目的是法律的灵魂，明确立法目的是制定法律的第一步。作为我国网络安全领域的基础性法律，其首要目的即为保障网络安全。根据网络安全法第七十六条的定义，“网络安全”是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。此定义中的网络涵盖了互联网、局域网和工业控制系统。网络安全则涵盖了网络运行安全、网络信息安全、数据安全等。网络安全法采取了广义的网络安全定义，这是因为随着信息技术的发展，网络空间与物理世界已高度融合，不同信息系统以及数据等所面临的威胁和风险具有相似性，预防、处置这些威胁和风险的手段也类似，因此立法保护的规则也相同。

网络空间主权原则是我国维护国家安全和利益、参与国际网络治理与合作所坚持的重要原则。《联合国宪章》确立的主权平等原则是当代国际关系的基本准则，覆盖国与国交往各个领域。从 20 世纪 90 年代后期起，从“去主权化”到“再主权化”，网络空间主权原则在国际上也获得越来越多的认同与支持。2015 年 7 月 1 日施行的新《国家安全法》第二十五条在我国法律层面首次明确了“网络空间主权”概念，是我国国家主权在网络空间领域的体现、延伸和反映。网络安全法在立法目的中明确“维护网络空间主权”，进一步为我国行使网络空间主权提供法律保障。

国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国

家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。维护国家安全，就是要防范、制止和依法惩治任何利用网络进行叛国、分裂国家、煽动叛乱、颠覆或者煽动颠覆人民民主专政政权的行为；防范、制止和依法惩治利用网络进行窃取、泄露国家秘密等危害国家安全的行为；防范、制止和依法惩治境外势力利用网络进行渗透、破坏、颠覆、分裂活动，维护网络安全是事关国家安全的重大问题。

网络已成为公共基础设施，网络安全关涉不特定多数人的利益，承载着巨大的社会公共利益。网络安全法确立维护网络安全的系列制度，就是要保障每一主体都有接入网络和享受便利服务的权利，同时保障网络中存储、处理和传输信息的真实性、准确性和完整性，确保网络产品和服务不中断，防止网络安全事件危害公众的健康和安全，维护社会公众的共同利益。

公民、法人和其他组织是网络活动的主体，保护好公民、法人和其他组织在网络领域的合法权益，是制定网络安全法的重要目的。网络安全法规定了明确的行为规范和法律责任，为不同主体遵循法律和救济补偿提供了明确的法律依据。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

【重点法条解读】

本条是网络安全法适用范围的规定。

法的适用范围是指法在什么地域内对什么主体适用。本条确立了网络安全法适用的属地管辖原则，本法效力原则上限于中华人民共和国境内，调整对象为建设、运营、维护和使用网络以及网络安全监管管理的活动，即对凡在中华人民共和国境内从事以上活动的主体均适用。此外，根据国际惯例和我国相关规定，我国对中华人民共和国的船舶、航空器以及驻外使领馆享有管辖权，网络安全法应同样适用。值得注意的是，基于惩治来自境外针对关键信息基础设施的网络安全风险和威胁的需要，网络安全法第五条、第五十条和第七十五条规定了特定的域外效力。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

【重点法条解读】

本条是关于网络安全和信息化工作基本原则的规定。

网络空间的安全与发展是世界发达和发展中国家信息化建设共同面临的挑战，加强网络安全和信息化发展，是应对日益复杂严峻的网络安全形势的必然选择，也是各国网络与信息安全法共同的价值选择。网络安全法将我国网络安全和信息化工作的方针“积极利用、科学发展、依法管理、确保安全”上升为法律规定，并从安全与发展并重的原则出发，确立了统筹国家网络安全与信息化工作的四项内容：一是推进网络基础设施建设和互联互通，二是鼓励网络技术创新和应用，三是支持培养网络安全人才，四是建立健全网络安全保障体系。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

【重点法条解读】

本条是关于国家网络安全战略的规定。

联合国国际电信联盟(ITU)作出的《2017年网络安全指数》报告显示，目前有70多个国家发布了网络安全方面的国家战略，20多个国家正在制定过程中。网络安全战略所体现的行业直至国民经济整体的宏观发展与立法关切的直接对接，将网络安全立法的位阶提升到了前所未有的高度。2016年12月27日，我国《国家网络空间安全战略》正式发布。网络安全法践行总体国家安全观，从宏观层面明确提出国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

【重点法条解读】

本条是关于国家维护网络安全主要任务的规定。

我国面临的网络安全风险和威胁广泛来源境内外，网络空间安全风险“不可逆”的特征进一步凸显，为了维护网络安全，必须摆脱传统上将风险预防寄托于事后惩治的立法理念，确立防御、控制与惩治相结合的立法理念。国家必须采取措施监测、防御并处置网络安全风险和威胁，保障网络空间安全和秩序。尤其值得注意的是，关键信息基础设施关系国家安全、国计民生、公共利益，以美国为主的西方国家都将关键信息基础设施的保护视为网络安全的最核心部分。对关键信息基础设施实施重点保护，也是国家的一项重要任务。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

【重点法条解读】

本条是关于网络安全国际合作的规定。

“信息技术无国界”和“网络空间有主权”的国际认识日渐达成，网络安全国际合作已成为国际共识，除了联合国框架下的信息社会世界峰会、中俄等国家联合提出信息安全国际行为准则等，上海合作组织、亚太经合组织、欧盟、北约等许多国际组织都将网络安全作为重要合作领域，制定了很多合作计划，中美、中俄、中英等国家之间建立了网络安全对话与合作机制。我国参与网络安全国际合作的重点领域包括网络空间治理、网络技术研发、网络标准制定、情报共享、打击恐怖主义、网络犯罪等。2017年3月1日，外交部和国家互联网信息办公室正式发布《网络空间国家合作战略》全面宣示中国在网络空间相关国际问题上