网络安全法
和
网络安全等级保护
2.0

夏　冰　主编
王沛栋　郑秋生　副主编
王志奇　主审

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全法和网络安全等级保护 2.0

主　编　夏　冰
副主编　王沛栋　郑秋生
主　审　王志奇

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书围绕网络安全法和网络安全等级保护内容展开。

网络安全法部分，首先指出国家网络空间安全战略，梳理五大目标、四个原则、九项战略任务之间的关系。重点从国家、网络运营者、公民个人角度对网络安全法进行解读，剖析角色主体的安全责任和义务，明确网信、公安等部门在网络安全法的监管职责和工作内容。最后列举网络安全法相关配套法规并给出典型执法案例，提供借鉴和参考。

网络安全等级保护部分，对网络安全等级保护工作的主要内容、工作流程、工作方法、政策法规依据、技术标准等内容进行全面解读；对网络安全等级保护定级备案、安全建设整改、等级测评、监督检查等工作进行详细解释；对信息安全管理和风险评估、网络安全事件管理和应急响应、网络安全监测预警和信息通报等国家网络安全核心工作进行具体描述；同时，对网站安全监管，网络安全保障工作综治考核，融合大数据、物联网、工业控制系统、云计算等技术的新型智慧城市安全监管逐一说明。

本书主要面向关键信息基础设施主管部门、运营部门、建设使用部门学习网络安全法、网络安全等级保护系列政策和法规的人员，面向企事业单位开展风险评估、通报预警、网络安全事件处置、网络安全保障工作全国综治考核评价的人员，面向网络安全相关部门开展监督管理、执法检查工作的人员，也可以供信息安全管理人员、信息安全专业人员、信息安全服务人员、网络安全等级保护测评师等参考。

图书在版编目(CIP)数据

网络安全法和网络安全等级保护 2.0 / 夏冰主编. —北京：电子工业出版社，2017.10

ISBN 978-7-121-32765-0

Ⅰ. ① 网… Ⅱ. ① 夏… Ⅲ. ① 计算机网络－科学技术管理法规－研究－中国

Ⅳ. ① D922.174

中国版本图书馆 CIP 数据核字（2017）第 233717 号

策划编辑：章海涛

责任编辑：章海涛

印　　刷：三河市鑫金马印装有限公司

装　　订：三河市鑫金马印装有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱　邮编　100036

开　　本：787×1092　1/16　　印张：18　　字数：460 千字

版　　次：2017 年 10 月第 1 版

印　　次：2017 年 10 月第 1 次印刷

定　　价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：192910558（QQ 群）。

前　言

网络安全靠人民，网络安全为人民。2017 年 6 月 1 号实施的《中华人民共和国网络安全法》（以下称《网络安全法》）是国家安全法律制度体系中一部重要法律，是网络安全领域的基本大法。《网络安全法》完善了国家、网络运营者、公民个人等角色的网络安全义务和责任，将原来散见于各种法规、规章中的网络安全规定上升到人大法律层面，并对网络运营者等主体的法律义务和责任做了全面规定。

《网络安全法》规定，我国实行网络安全等级保护制度。网络安全等级保护制度是国家信息安全保障工作的基本制度、基本国策和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。国家法规和系列政策文件明确规定，实现并完善网络安全等级保护制度，是统筹网络安全和信息化发展，完善国家网络安全保障体系，强化关键信息基础设施、重要信息系统和数据资源保护，提高网络综合治理能力，保障国家信息安全的重要手段。

网络安全等级保护包括系统定级、系统备案、建设整改、等级测评和监督检查 5 个常规动作，贯穿信息系统的全阶段、全流程，是当今发达国家保护关键信息基础设施、保障网络安全的通行做法。对信息系统分级实施保护，在网络安全等级保护基础上，重点保护关键信息基础设施，能够有效地提高我国网络安全建设的整体水平，有利于保障网络安全与信息化同步规划、同步建设、同步使用；有利于为信息系统网络安全建设和管理提供系统性、针对性、可行性的指导和服务，有效控制网络安全建设成本；有利于优化网络安全资源的配置。

随着云计算、移动互联、大数据、物联网、工业控制系统、人工智能等新技术不断涌现，传统信息系统安全的边界和防护发生了变化。起到支撑、传输作用的基础信息网络和各类应用组成的信息系统本质没有发生变化，网络安全等级保护仍然适用。但是，计算机信息系统的概念已经不能涵盖全部，特别是互联网快速发展带来大数据价值的凸显，这些都要求等级保护外延的拓展。新的系统形态、新业态下的应用、新模式背后的服务以及重要数据和资源统统进入了等级保护视野。具体对象则囊括大型互联网企业、基础网络、重要信息系统、网站、大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等，网络安全等级保护进入了 2.0 时代。在 2.0 时代下，等级保护的内涵在信息系统安全等级保护的基础之上，风险评估、网络安全事件应急处置、网络安全监测与通报预警、网络安全保障工作综治考核、政府网站监管、新型智慧城市监管等与网络安全密切相关的措施将被全部纳入网络安全等级保护制度范畴内。

为了便于国家关键信息基础设施主管部门、运营部门、建设部门学习网络安全法、网络安全等级保护系列政策和法规内容，便于各级党委政府、企事业单位开展网络安全风险评估、

网络安全监测和通报预警、网络安全事件处置、网络安全保障工作全国综治考核评价，便于网信部门、网络安全保卫部门开展监督检查工作，在河南省公安厅网络安全保卫总队的指导下，河南省信息安全等级保护工作协调小组办公室组织编写该书。

本书由中原工学院的夏冰教授统筹协调，负责书稿的主体编写。中原工学院郑秋生教授、河南省委网信办王沛栋副研究员、河南省网络安全保卫总队的刘晓、河南省鼎信信息安全等级测评有限公司的陈宇也参与了本书的编写并提供建设性建议，在此表示感谢。河南省网络安全保卫总队的王志奇调研员对书稿审查投入大量精力，在此表示由衷的感谢。本书的编写还得到计算机信息系统安全评估河南省工程实验室和郑州市网络安全创新团队的项目资金支持，在此表示感谢。

由于水平有限，书中难免有不足之处和错误，敬请读者批评指正。

作　者

目　录

第 1 章　国家网络空间安全战略

信息技术广泛应用和网络空间兴起发展，极大促进了经济社会繁荣进步，同时带来了新的安全风险和挑战。网络空间安全（以下称“网络安全”）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。为贯彻落实习近平总书记关于推进全球互联网治理体系变革的“四项原则”和构建网络空间命运共同体的“五点主张”，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，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》。

网络空间（Cyberspace）是指由互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的空间。《国家网络空间安全战略》的重要意义是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措，是实现“两个一百年”奋斗目标、实现中华民族伟大复兴中国梦的重要保障。

网络安全战略主要包括机遇与挑战、目标、原则和战略任务 4 部分。

1.1　网络空间的新作用和新机遇

网络空间对我们的信息传播、生产生活、经济发展、文化发展、社会治理、交流合作和国家主权产生深刻影响。正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。《国家网络空间安全战略》指出网络空间有 7 个新作用，新作用也是新机遇。

1．信息传播的新渠道

网络技术的发展，突破了时空限制，拓展了传播范围，创新了传播手段，引发了传播格局的根本性变革。相对于传统的电视、电话、报刊，更精准、更有效、更快捷、更有影响力的新渠道出现在大众面前，主要包括微信、微博、博客、网络视频、网络社区、IPTV、移动电视、手机。网络已成为人们获取信息、学习交流的新渠道，成为人类知识传播的新载体。

2．生产生活的新空间

当今世界，网络深度融入人们的学习、生活、工作等方方面面，网络教育、创业、医疗、购物、金融等日益普及，越来越多的人通过网络交流思想、成就事业、实现梦想。世界因互联网而更多彩，生活因互联网而更丰富。

2015 年“双十一”活动中，天猫的总成交金额达到 912.17 亿元，比 2014 年翻一番，其中移动端占比 68%。滴滴打车、在线学习、网上挂号等日益紧密地与我们的工作、学习、生

活结合在一起。所谓中国新四大发明“高铁、网购、移动支付、共享单车”，其中三个都与互联网产业的发展息息相关。中国网购人群数量和网络购物交易额已经全球居首。

3．经济发展的新引擎

互联网日益成为创新驱动发展的先导力量，信息技术在国民经济各行业广泛应用，推动传统产业改造升级，催生了新技术、新业态、新产业、新模式，促进了经济结构调整和经济发展方式转变，为经济社会发展注入了新的动力。

党的十八大以来，国家高度重视互联网产业发展。诸如跨境电商、物联网、分享经济、大数据、云计算等大量互联网催生的新产品、新业态竞相涌现，凸显互联网产业发展的成绩，表明基于互联网技术的新市场、新业态正在成为中国经济的又一抹亮色。第 40 次《中国互联网络发展状况统计报告》显示，2017 年上半年商务交易类应用持续高速增长，网络购物、网上外卖和在线旅行预订用户规模分别增长 10.2%、41.6%和 11.5%。互联网技术以及随之而来的生产、消费、思维模式等的变革，已经深深地影响和改变着每个人。

4．文化繁荣的新载体

网络促进了文化交流和知识普及，释放了文化发展活力，推动了文化创新创造，丰富了人们精神文化生活，已经成为传播文化的新途径、提供公共文化服务的新手段。网络文化已成为文化建设的重要组成部分。

网上图书馆、博物馆、展览馆、剧场等，通过网络来传播经典，推动优秀传统文化瑰宝和当代文化精品网络传播。实施网络精品阅读工程，积极开展网上经典阅读、好书推荐等活动，丰富大众知识。同时，开办教育网站、外语网站、双语网站、文学网站、戏曲网站、科普网站，构建特色网站群，满足不同网民群体的精神文化需求。

5．社会治理的新平台

网络在推进国家治理体系和治理能力现代化方面的作用日益凸显，电子政务应用走向深入，政府信息公开共享，推动了政府决策科学化、民主化、法治化，畅通了公民参与社会治理的渠道，成为保障公民知情权、参与权、表达权、监督权的重要途径。

近年来，各地政府按照“简化手续、优化程序、在线运行、限时办结、把审批变成服务”的要求，打造线上线下政务服务大厅，严格执行审批程序和时限规定，地方政务服务中心实行集中式审批等做法得到群众认可。2016 年调查结果显示，63.1%的受访者认为现在找政府办事比以前更容易了，较 2015 年提高了 2.53 个百分点。“互联网+政务”已成为常态。

6．交流合作的新纽带

信息化与全球化交织发展，促进了信息、资金、技术、人才等要素的全球流动，增进了不同文明交流融合。网络让世界变成了地球村，国际社会越来越成为你中有我、我中有你的命运共同体。

2016 年 11 月 16 日，在第三届世界互联网大会上，习近平总书记提出：互联网发展是无国界、无边界的，利用好、发展好、治理好互联网必须深化网络空间国际合作，携手构建网络空间命运共同体。互联网连接了各行各业与所有人群，增加了有价值信息的需求，互联网让知识的交换和共享更加便捷，促进全球快速流动。

7．国家主权的新疆域

网络空间已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域，国家主权拓展到网络空间，网络空间主权成为国家主权的重要组成部分。尊重网络空间主权，维护网络安全，谋求共治，实现共赢，正在成为国际社会共识。

网络空间作为人类生活新空间，发展不平衡、规则不健全、秩序不合理等问题日益凸显，网络战阴霾密布，西方一些国家利用信息技术优势干涉别国内政、从事大规模网络监听等活动时有发生。面对网络安全这一全球性问题与挑战，任何国家都难以独善其身，必须携手应对、共同治理。这是自“构建人类命运共同体”理念首次被写入联合国决议之后，中国在全球重要治理领域对命运共同体理念的延伸和完善，彰显了中国对全球治理的重大贡献。

1.2 网络空间安全面临严峻的新挑战

《国家网络空间安全战略》指出，当前网络安全形势日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战。

1．网络渗透危害政治安全

政治稳定是国家发展、人民幸福的基本前提。利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权，以及大规模网络监控、网络窃密等活动严重危害国家政治安全和用户信息安全。典型的例子如希拉里“邮件门”，美国民主党委员会的信息系统可能遭到俄罗斯攻击，致使总统候选人希拉里的邮件泄露，直接影响了美国大选的进程和结果。另外，朴槿惠“闺蜜事件”、阿拉伯的“茉莉花革命”都是网络安全问题引发的。

2．网络攻击威胁经济安全

网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。典型案例如美国东海岸发生大规模的断网事件，大半个美国的网络陷入瘫痪。世界上首例由恶意软件而引发的大规模断电事件，造成乌克兰 70 万家庭断电。黑客入侵孟加拉银行盗走支付交易凭证，通过国际银行结算系统 SWIFT 最终转出 8100 万美元。

3．网络有害信息侵蚀文化安全

网络上各种思想文化相互激荡、交锋，优秀传统文化和主流价值观面临冲击。网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息侵蚀青少年身心健康，败坏社会风气，误导价值取向，危害文化安全。网上道德失范、诚信缺失现象频发，网络文明程度亟待提高。例如一位自称上海女孩的网友发帖称，第一次去江西农村男友家过年，因一顿年夜饭难以忍受农村的贫穷落后，连夜赶回上海。这篇帖子挑起了城乡差异、地域歧视等热门话题，在网上引发轩然大波。

4．网络恐怖和违法犯罪破坏社会安全

恐怖主义、分裂主义、极端主义等势力利用网络煽动、策划、组织和实施暴力恐怖活动，

直接威胁人民生命财产安全、社会秩序。计算机病毒、木马等在网络空间传播蔓延，网络欺诈、黑客攻击、侵犯知识产权、滥用个人信息等不法行为大量存在，一些组织肆意窃取用户信息、交易数据、位置信息以及企业商业秘密，严重损害国家、企业和个人利益，影响社会和谐稳定，如备受关注的“徐玉玉遭电信诈骗身亡”案。

5．网络空间的国际竞争方兴未艾

国际上争夺和控制网络空间战略资源、抢占规则制定权和战略制高点、谋求战略主动权的竞争日趋激烈。个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战。

2017 年 8 月 18 日，美国总统特朗普宣布美军网络司令部升格，即从目前的二级功能司令部升格为美军第十个联合作战司令部。可以预计，美方将加速此前已经纳入议事日程的跨域联合机动作战概念的持续完善，加速以俄罗斯、中国、伊朗、朝鲜为假想敌的模拟作战与推演能力的建设，加速推进积极防御、网络空间自卫反击以及国家级的网络空间威慑能力的建设。国家安全是最高意识形态的网络攻防对抗。

6．网络空间机遇和挑战并存

坚持积极利用、科学发展、依法管理、确保安全，坚决维护网络安全，最大限度利用网络空间发展潜力，更好惠及 13 亿多中国人民，造福全人类，坚定维护世界和平。

比如，“互联网+”在实体经济乃至社会上下、各行各业掀起了创新的浪潮。同时需清醒地认识到，无论对于消费者、企业，还是政府监管部门，都意味着新的信息安全风险与挑战，安全风险涉及法律、制度等问题都将逐渐暴露出来。“互联网+”火热的背后暗藏潜在的风险，网络安全便是众多风险中重之又重的一方面。随着“互联网+”的推进，众多传统行业逐步数据化、在线化、移动化、远程化，同时更多消费者卷入互联网，产生的数据和信息必将呈爆炸式增长；除此之外，在物联网和物理信息系统的发展下，网络从“人”和“机”的连接延伸至“人、机、物”的连接，将产生新的自物理世界的巨量传感数据，这些数据涉及整个社会、军事及国民经济的方方面面，与国家经济发展甚至整个国家安全都息息相关，在这样的新环境下，如何保障并提升信息安全，为社会经济健康发展保驾护航，是挑战更是机遇。

1.3 战略目标与原则

1.3.1 五大目标

国家的总体安全观是指国家政权、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。《国家网络空间安全战略》提出了在总体国家安全观指导下，通过统筹国内国际两个大局和统筹发展安全两件大事的基础上，推进网络空间“和平、安全、开放、合作、有序”的发展战略目标。

和平：信息技术滥用得到有效遏制，网络空间军备竞赛等威胁国际和平的活动得到有效控制，网络空间冲突得到有效防范。

安全：网络安全风险得到有效控制，国家网络安全保障体系健全完善，核心技术装备安全可控，网络和信息系统运行稳定可靠。网络安全人才满足需求，全社会的网络安全意识、基本防护技能和利用网络的信心大幅提升。

开放：信息技术标准、政策和市场开放、透明，产品流通和信息传播更加顺畅，数字鸿沟日益弥合。不分大小、强弱、贫富，世界各国特别是发展中国家都能分享发展机遇、共享发展成果、公平参与网络空间治理。

合作：世界各国在技术交流、打击网络恐怖和网络犯罪等领域的合作更加密切，多边、民主、透明的国际互联网治理体系健全完善，以合作共赢为核心的网络空间命运共同体逐步形成。

有序：公众在网络空间的知情权、参与权、表达权、监督权等合法权益得到充分保障，网络空间个人隐私获得有效保护，人权受到充分尊重。网络空间的国内和国际法律体系、标准规范逐步建立，网络空间实现依法有效治理，网络环境诚信、文明、健康，信息自由流动与维护国家安全、公共利益实现有机统一。

“和平与安全”是构建“开放、合作、有序”网络空间的前提，维持国际和平与安全是《联合国宪章》的宗旨，只有在“和平与安全”得到充分保证的前提下，才能构建“开放、合作、有序”的网络空间。互联网时代，一个和平、安全、开放、合作、有序的网络空间，对一国乃至世界和平与发展越来越具有重大战略意义。

1.3.2 四项原则

《国家网络空间安全战略》整体构建了维护网络空间和平与安全的“四项原则”，即“尊重维护网络空间主权、和平利用网络空间、依法治理网络空间、统筹网络安全与发展”。“四项原则”以维护网络空间和平与安全为宗旨，不但反映了互联网时代世界各国共同构建网络空间命运共同体的价值取向，而且反映出互联网时代“安全与发展”为一体双翼的主潮流，集中体现了习近平在第二届世界互联网大会上提出的推进全球互联网治理体系的“四项原则”：尊重网络主权，维护和平安全，促进开放合作，构建良好秩序。

1．尊重维护网络空间主权

网络空间主权不容侵犯，尊重各国自主选择发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利。各国主权范围内的网络事务由各国人民自己做主，各国有权根据本国国情，借鉴国际经验，制定有关网络空间的法律法规，依法采取必要措施，管理本国信息系统及本国疆域上的网络活动；保护本国信息系统和信息资源免受侵入、干扰、攻击和破坏，保障公民在网络空间的合法权益；防范、阻止和惩治危害国家安全和利益的有害信息在本国网络传播，维护网络空间秩序。任何国家都不搞网络霸权、不搞双重标准，不利用网络干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。

2．和平利用网络空间

和平利用网络空间符合人类的共同利益。各国应遵守《联合国宪章》关于不得使用或威胁使用武力的原则，防止信息技术被用于与维护国际安全与稳定相悖的目的，共同抵制网络空间军备竞赛、防范网络空间冲突。坚持相互尊重、平等相待，求同存异、包容互信，尊重