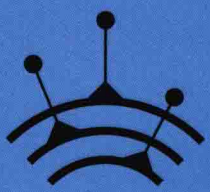
SAFEGUARDING CYBERSPACE SECURITY

AN ANALYSIS ON THE CYBERSECURITY LAW OF THE P.R.C.

维护网络空间安全

中国网络安全法解读

王春晖◎主编



形象生动的专家解读
紧贴生活的案例分析

全球信息革命的法律应对，世界网络治理的中国智慧

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

SAFEGUARDING CYBERSPACE SECURITY

维护网络空间安全

中国网络安全法解读

SAFEGUARDING CYBERSPACE SECURITY

AN ANALYSIS ON THE CYBERSECURITY LAW OF THE P.R.C.

维护网络空间安全

中国网络安全法解读

主编 ◎ 王春晖

参编 ◎ 刘　越　张素伦

范　为　赵鑫鑫

郭晓磊

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

内 容 简 介

自 2017 年 6 月 1 日起，《中华人民共和国网络安全法》（本书简称《网络安全法》）正式实施，奠定了中国网络安全保护和网络空间治理的基本框架，影响深远。为全面阐述《网络安全法》的立法背景、立法基础、立法价值及适用规则，普及维护网络安全相关法律知识，促进网络空间命运共同体的交流与合作，本书编写组精心策划编写了本书。

本书共十章，内容包括：维护网络空间安全的中国智慧、网络空间不应成为“法外之地”、网络服务的“安全红线”、“震网”病毒的“防火墙”、“全球科技巨头”关注的网络安全审查制度、个人信息使用的“高压线”、对“精准诈骗”的“精准治理”、网络违法和不良信息传播的“藩篱”、不容忽视的“违法成本”和为网络安全“定分止争”。全书内容丰富，文字生动形象，叙述深入浅出，让广大读者对中国维护网络安全的法律与政策真正读得懂、用得上，并成为网络空间命运共同体构建的参与者与见证者。

图书在版编目（CIP）数据

维护网络空间安全：中国网络安全法解读/王春晖主编. —北京：电子工业出版社，2018.1
ISBN 978-7-121-33242-5

Ⅰ. ①维… Ⅱ. ①王… Ⅲ. ①计算机网络－科学技术管理法规－中国 Ⅳ. ①D922.17

中国版本图书馆 CIP 数据核字（2017）第 307988 号

策划编辑：戴晨辰
责任编辑：戴晨辰　　文字编辑：刘　瑀
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
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：720×1 000　1/16　印张：18　字数：262 千字
版　　次：2018 年 1 月第 1 版
印　　次：2018 年 1 月第 1 次印刷
定　　价：55.00 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：dcc@phei.com.cn。

前　言
PREFACE

从世界范围看，网络安全已经成为影响全球经济安全运行、政治稳定发展、人民安居乐业的重要因素，国际社会和各国都普遍在探索如何加强对网络安全问题的治理。党的十九大报告在“坚持和平发展道路，推动构建人类命运共同体”中特别列举了“网络安全”是人类面临的诸多共同挑战之一。世界经济论坛发布的《2016年全球风险报告》指出：“对于技术方案的认知匮乏以及相关风险处理能力低下——特别是网络风险或者关键性信息基础设施破坏所带来的系统性级联效应——可能会给国家经济、各经济组织乃至全球企业带来深远的影响。”在国际网络安全形势日益严峻的时期，《中华人民共和国网络安全法》（本书简称《网络安全法》）于2017年6月1日起正式实施，显得非常及时且极为重要。

《网络安全法》是我国网络安全领域的基础性法律，以保障网络安全，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为立法目的，奠定了我国网络安全保护和网络空间治理的基本框架，引导着我国网信事业沿着健康安全的轨道运行，也为全球互联网的治理贡献了中国智慧。

本书由我国知名信息通信战略与法律专家王春晖教授担任主编，我

国多位网络与信息法律专家参与撰写。全书共十章，围绕《网络安全法》中网络空间主权原则的确立、重要数据的本地化存储、个人信息保护、关键信息基础设施的安全保护及其范围，以及惩治网络诈骗等新型网络违法犯罪活动的规定等，突出亮点，系统地梳理了中国网络空间安全的价值观、网络安全立法与司法的中国实践；详细地阐述了网络空间主权法律制度、中国网络安全标准与等级保护制度、关键信息基础设施安全保护制度、国家网络安全审查制度的确立与实现；归纳总结出网络产品和服务提供者及网络运营者的各项安全义务和法律责任；完整地介绍了关键信息基础设施重要数据跨境传输的规定与内容；对个人信息泄露及电信网络诈骗等百姓关注的热点问题提出了有效的保护途径及治理方案。与此同时，针对当今规范网络信息传播的主要问题，书中设立专章详述国家网信部门和有关部门的监管职责及重大突发社会安全事件的网络通信管制措施。

本书聚焦习近平主席关于网络安全系列重要讲话精神，在回顾中国维护网络空间安全立法实践的基础上，全面论述《网络安全法》的立法价值及适用规则，本书不是对《网络安全法》条文的解释，而是以日常生活中的网络安全故事，以生动形象的文字描述和深入浅出的理论阐述，向广大读者普及网络安全的相关法律知识，搭建维护网络空间命运共同体的法治交流平台。

目　录

CONTENTS

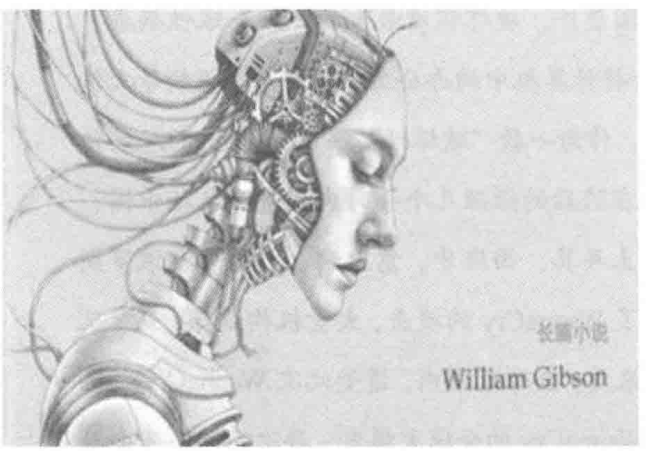
第一章 Chapter 1 维护网络空间安全的中国智慧

引 2017年5月12日，勒索病毒（WannaCry）开始爆发。此次病毒攻击事件，被业内认为是自冲击波病毒（Worm.Blaster或 Lovesan）以来，影响范围最广，破坏程度最大的一款全球性病毒。WannaCry感染计算机后，会将计算机中的办公文档、照片、视频等文件加密，并向用户勒索比特币。作为一款“破坏性”病毒，WannaCry的传播速度和影响都十分惊人。在随后的短短几个小时内，就有包括中国、英国、美国、德国、日本、土耳其、西班牙、意大利、葡萄牙、俄罗斯和乌克兰等国家被报道遭到了WannaCry的攻击，大量机构设备瘫痪。从后续国内外媒体披露的情况来看，全球范围内，遭受此次WannaCry病毒攻击的国家超过了100个。WannaCry的全球大爆发，再次为网络安全敲响了警钟。

一、我们的网络空间安全吗

（一）认识网络空间与网络空间安全

20 世纪 80 年代初，美国科幻作家威廉·吉布森（William Gibson）写下了一部当时被认为是极其离奇的长篇小说，书名叫《神经漫游者》（*Neuromancer*）。该小说出版后，得到了各国读者的一致好评，这部小说不但催生了《黑客帝国》、《攻壳机动队》等科幻影视巨片，而且还史无前例地获得包括“雨果奖”（Hugo Award）、“星云奖”（Nebula Award）与“菲利普·狄克奖”（Philip K. Dick Award）三大科幻小说大奖，且此纪录至今无人能破。在《神经漫游者》中，吉布森描写了反叛者兼网络独行侠凯斯，受雇于某跨国公司，被派往全球计算机网络构成的空间里，去执行一项极具冒险性的任务。进入这个巨大的空间，凯斯并不需要乘坐飞船或火箭，只需在大脑神经中植入插座，然后接通电极，计算机网络便被他感知。当网络与人的思想意识合而为一后，即可遨游其中。在这个广阔的空间里，人类看不到蓝天、阳光、高山、大海，也看不到城市和乡村，只有庞大的三维信息库和各种信息在高速流动。吉布森把这个空间定义为“赛伯空间”（Cyberspace），这是人们最早认识的“网络空间”。在吉布森所谓的网络空间里，客观世界和数字世界交融在一起，让进入这个空间的人类感知到一个由计算机产生的、现实中并不存在的虚拟世界，而且这个充满情感的虚拟数字世界不断地影响着人类生存的物质世界。



《神经漫游者》中的网络独行侠

互联网，准确的称谓应该是 Internet，音译为“因特网”，最早起源于美国国

防部高级研究计划署（Defence Advanced Research Projects Agency，DARPA）的前身 ARPAnet，于 1969 年投入使用。由此，ARPAnet 成为现代计算机网络诞生的标志。最初，ARPAnet 主要是用于军事研究目的，它主要基于下述的指导思想：网络必须经受得住故障的考验而维持正常的工作，一旦发生战争，当网络的某一部分因遭受攻击而失去工作能力时，网络的其他部分应能维持正常的通信工作。ARPAnet 在技术上的另一个重大贡献是 TCP/IP 协议簇的开发和利用。作为 Internet 的早期骨干网，ARPAnet 的试验奠定了 Internet 存在和发展的基础，较好地解决了异种机网络互联的一系列理论和技术问题。1983 年，ARPAnet 分裂为两部分，ARPAnet 和纯军事用的 MILNET。同时，局域网和广域网的产生和蓬勃发展对 Internet 的进一步发展起了重要的作用。其中最引人注目的是美国国家科学基金会（National Science Foundation，NSF）建立的 NSFnet。NSF 在全美国建立了按地区划分的计算机广域网并将这些地区网络和超级计算机中心互联起来。NFSnet 于 1990 年 6 月彻底取代了 ARPAnet 而成为 Internet 的主干网。

这项诞生于二十世纪六七十年代的计算机互联网通信技术，发展至今，已经自下而上架构了基础“物理”层、数字“代码”层和信息“内容”层三个基本层面，这三个基本层构成一个闭合系统，塑造了世界范围内各数字行为体密切链接的网络空间。网络空间打通了虚拟与现实的联系，使信息流动速度更快、社交更加便利、文化交往更加频繁，其发展状态与人类社会未来和文明走向息息相关。

随着新一代信息科技的迅猛发展，网络突破了时间与空间的限制，模糊了国家领土边界，对国家主权安全构成了挑战。基于云计算、大数据、物联网、人工智能技术的创新和应用，使网络安全屏障的脆弱性更为凸显，加剧了各国安全领域的新关切。如今，网络空间被列为与陆、海、空、太空并列的第五空间。这个第五空间的运行规则完全不同于物质空间，例如网络空间产生的主要客体是数据和信息，数据和信息与物理空间的物质最大的不同就是没有任何重量，也没有具体的形状，但它的出现充满不确定性和变数。网络空间的数据和信息其本身没有

杀伤力，但是当人们在网络空间以邪恶的心态和手段使用和破坏它时，将会对物理世界的人类造成不可低估的杀伤力。今天的网络空间安全已经关系到一个国家的国家安全、政权稳固、社会稳定、民心安定，其重要性正随着全球信息化步伐的加快而愈加凸显。

（二）信息与数据泄露将无处不在

网络是一般双刃剑，大数据、云计算、物联网、人工智能等新技术的应用，在方便了人们的生活和提高工作、学习效率的同时，也产生了大量的网络安全风险与危机。近年来，信息与数据泄露事件频发，尤其是我们日常接触的社交网络更是信息与数据泄露的重灾区，不断给我们敲响网络安全的警钟。近几年，重大信息与数据泄露事件时有发生，既有发生在国外的事件，也有发生在国内的事件；既有政府机构被黑客攻击，也有民间组织被肆意攻击；既有合法的网络运营者泄露公民信息与数据的事件，也有不法之徒和非法网站恶意窃取公民信息与数据的事件。

国内外相继发生的域名系统遭攻击、大规模用户信息泄露、电信网络诈骗、关键基础信息设施瘫痪、智能设备被攻击等问题让我们清醒地意识到，随着万物互联时代的到来，网络安全形势将更加严峻。以下例举近期国内外比较典型的信息与数据泄露事件。

“影子经纪人”可能危及数十亿用户。[①] 据报道，2016 年 8 月，被称为“影子经纪人”（Shadow Brokers）的神秘黑客团队首次在美国出现，“影子经纪人”声称它攻入了美国国家安全局（NSA）下属黑客组织“方程式组织”的武器库，盗取了 NSA 的黑客工具和在网络间谍活动中获取的数据样本。2017 年 4 月，“影子经纪人”公开了为 NSA 提供服务专门对国外进行间谍活动的组织的黑客工具包，其中包括被称为“想哭病毒”的 Windows 漏洞，黑客曾经用它来感染两种高调勒

① 详见搜狐科技，“一年过半，战事不断——2017 年上半年网络安全灾难事件盘点”，http://www.sohu.com/a/158190767_290304。

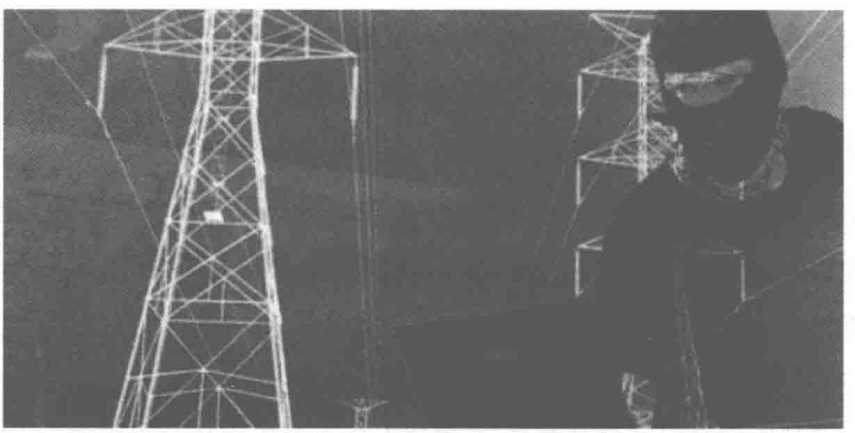
索软件（Ransomware）攻击的目标。至今为止，“影子经纪人”的身份仍然未知。但该组织还未将泄露的 NSA 的黑客工具全部公开，一旦公开，后果可能会危及数十亿的软件用户。

影子经纪人

英国 Wonga 信息泄露，影响 27 万账户。据报道，2017 年 4 月，英国发薪日贷款机构 Wonga 发布声明称，该公司部分客户信息可能遭到非法和未经授权的访问。数十万账户的个人详情可能被非法访问，有报告显示这一数字可能多达 27 万。Wonga 表示，曝光的信息包括客户的姓名、电子邮件地址、家庭住址、电话号码、银行账号，以及排序代码的最后四位数字。Wonga 此前就一直饱受争议，其所提供的发薪日贷款，指的是一至两周的短期贷款，借款人承诺在自己发薪水后即偿还贷款。如果到期无法还清贷款本金和利息，可以提出延期，年息可高达 1509%。过去两年里，该公司因重组成本、费用上限和更严苛的借款标准而备受打击。2015 年 12 月，Wonga 报告 2015 年税前亏损 8020 万英镑，比前一年高 53%。Wonga 发言人称：“Wonga 正紧急调查对部分英国和波兰用户个人数据的非法入侵。我们正与监管部门密切合作，并正在进行通知受到影响的客户的工作。我们对因此造成的不便致以诚挚的歉意。”而就在信息泄露事件发生后不久，黑客便窃取了特易购银行 9000 名在线客户总计 250 万英镑的巨款。该事件被归咎于系统和复杂的网络攻击，目前仍在该国犯罪机构和国家网络安全中心的调查之中。

贷款机构信息泄露

乌克兰电网系统遭黑客攻击。2016 年 1 月，乌克兰电网系统遭黑客攻击，数百户家庭供电被迫中断，是有史以来首次导致停电的网络攻击。此次针对工控系统的攻击影响巨大，引起国内外媒体高度关注。据 iSight Partners 网络间谍情报负责人约翰•胡尔特奎斯特（John Hultquist）表示，本次攻击来自俄罗斯黑客组织，使用的恶意软件被称为“黑暗力量”（Black Energy）。Black Energy 最早可以追溯到 2007 年，由俄罗斯地下黑客组织开发并广泛使用在 BOTNET，主要用于建立僵尸网络，对定向目标实施 DDoS 攻击。



电网系统遭黑客攻击[①]

① 图片来源于 360 企业安全微博，“乌克兰电网被黑事件的工控安全 | 企业看安全”，http://weibo.com/p/1001603943151864834672。