网络空间安全蓝皮书

BLUE BOOK OF CYBERSPACE SECURITY

中国网络空间安全发展报告

(2018)

上海社会科学院信息研究所
中国信息通信研究院安全研究所
主编／惠志斌　覃庆玲
副主编／张衡　彭志艺

ANNUAL REPORT ON DEVELOPMENT OF CYBERSPACE SECURITY IN CHINA (2018)

2018版

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

网络空间安全蓝皮书

BLUE BOOK OF
CYBERSPACE SECURITY

中国网络空间安全发展报告（2018）

ANNUAL REPORT ON DEVELOPMENT OF CYBERSPACE SECURITY IN CHINA (2018)

上海社会科学院信息研究所
中国信息通信研究院安全研究所
主　编／惠志斌　覃庆玲
副主编／张　衡　王志艺

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

图书在版编目(CIP)数据

中国网络空间安全发展报告.2018 / 惠志斌，覃庆玲主编. --北京：社会科学文献出版社，2018.11
（网络空间安全蓝皮书）
ISBN 978-7-5201-3898-7

Ⅰ.①中… Ⅱ.①惠… ②覃… Ⅲ.①计算机网络-安全技术-研究报告-中国-2018 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字（2018）第257129号

网络空间安全蓝皮书
中国网络空间安全发展报告（2018）

主　　编 / 惠志斌　覃庆玲
副 主 编 / 张　衡　彭志艺

出 版 人 / 谢寿光
项目统筹 / 郑庆寰
责任编辑 / 张　媛

出　　版 / 社会科学文献出版社·皮书出版分社（010）59367127
地址：北京市北三环中路甲29号院华龙大厦　邮编：100029
网址：www.ssap.com.cn
发　　行 / 市场营销中心（010）59367081　59367083
印　　装 / 三河市龙林印务有限公司

规　　格 / 开 本：787mm×1092mm　1/16
印 张：26　字 数：391千字
版　　次 / 2018年11月第1版　2018年11月第1次印刷
书　　号 / ISBN 978-7-5201-3898-7
定　　价 / 99.00元

皮书序列号 / PSN B-2015-466-1/1

上海社会科学院信息研究所

上海社会科学院信息研究所成立于1978年，是专门从事信息社会研究的国内知名智库，现有科研人员40余人，具有高级专业技术职称的25人，下设信息安全、信息资源管理、电子政府、知识管理等专业方向和研究团队。近年来，信息研究所坚持学科研究和智库研究双轮互动的原则，针对信息社会发展中出现的重大理论和现实问题，聚焦网络安全与信息化方向开展科研攻关，积极与中国信息安全测评中心、中国信息安全研究院等机构建立合作关系，承接国家社科基金重大项目“大数据和云环境下国家信息安全管理范式与政策路径”（2013）、国家社科重点项目“信息安全、网络监管与中国的信息立法研究”（2001）等十余项国家和省部级研究课题，获得由上海市政府授牌的“网络安全管理与信息产业发展”社科创新研究基地，先后出版《信息安全：威胁与战略》（2003）、《网络：21世纪的权力与挑战》（2007）、《网络传播革命：权力与规制》（2010）、《信息安全辞典》（2013）、《全球网络空间安全战略研究》（2013）、《网络舆情治理研究》（2014）等著作，相关专报获国家和上海市主要领导的批示。

中国信息通信研究院安全研究所

中国信息通信研究院安全研究所成立于2012年11月，是专门从事信息通信领域安全技术研究的科研机构，现有科研人员100余人，下设网络安全研究部、信息安全研究部、信息化与两化融合安全部、软件测评部、重要通信研究部等研究部门。中国信息通信研究院安全研究所主要开展信息通信安全防护的战略性和前瞻性问题研究，加强信息通信新技术新业务评估，为国家主管部门有关网络信息安全发展战略、决策、规范的制定提供强有力的技术支撑。近年来，中国信息通信研究院安全研究所出色地完成国家、政府委托的安全监管支撑重点工作，承担国家大量重大网络信息安全专项科研课题，牵头制定大量国际国内网络信息安全标准规范，对前沿信息安全技术的研究有深厚积累，研究领域涵盖通信网络信息安全、数据安全、互联网安全、应用安全、工业互联网安全、重要通信等各个领域。

中国网络空间安全发展报告（2018）
编　委　会

主编简介

惠志斌 上海社会科学院互联网研究中心执行主任，信息研究所信息安全研究中心主任，副研究员，管理学博士，全国信息安全标准化委员会委员。主要研究方向为网络安全和数字经济，已出版《全球网络空间信息安全战略研究》《信息安全辞典》等论著共4本，发表《我国国家网络空间安全战略的理论构建与实现路径》《数据经济时代的跨境数据流动管理》等专业论文30余篇，在《人民日报》《光明日报》《解放军报》等重要媒体发表专业评论文章近10篇；主持国家社科基金一般项目“大数据时代国际网络舆情监测研究（2014）”等国家和省部级项目多项，作为核心成员承担国家社科基金重大项目“大数据和云环境下国家信息安全管理范式与政策路径”和上海社科创新研究基地“网络安全管理与信息产业发展”研究工作；提交各级决策专报20余篇，多篇获中央政治局常委和政治局委员肯定性批示，先后赴瑞士、印度、美国、德国等国家参加网络安全国际会议。

覃庆玲 中国信息通信研究院信息通信安全研究所副所长，院互联网领域副主席。主要从事电信监管、互联网管理、信息安全等研究，负责和参与了互联网行业“十二五”发展规划、互联网新技术新业务安全评估体系研究、新形势下互联网监管思路与策略建议、基础电信企业考核体系研究、全国互联网信息安全综合管理平台需求设计、重要法律法规制修订等重大课题研究，互联网行业“十二五”发展规划、互联网新技术新业务安全评估体系研究等曾获得部级科技二等奖及三等奖。在互联网行业管理、信息安全等方面有着深厚的积累和深入的研究。

摘　要

2017 年以来，人工智能、自动驾驶、区块链、工业互联网等技术飞速发展，美、英等国全球战略发生重大转向，全球贸易和科技面临新竞争格局。由于网络空间承载着技术创新突破、数据资源争夺、国家利益角逐等多重多维职能，网络空间安全的内涵和外延比以往任何时候都丰富，网络空间安全问题的战略价值日益凸显。

对我国而言，网络空间的科学治理和安全保障，不仅决定了我国能否实现从网络大国向网络强国跨越，也是我国国家治理体系和治理能力现代化的重要方面。2017 年以来，我国以习近平新时代中国特色社会主义思想为核心的网络强国战略基本确立，网络安全管理体制机制更趋完善，网络环境治理工作取得阶段性明显成效，以网络空间命运共同体为核心的网络空间国际治理主张不断得到国际社会响应。

《中国网络空间安全发展报告（2018）》延续“网络空间安全蓝皮书”系列主要框架，重点讨论全球治理变革和智能技术创新对网络空间安全的影响。全书分为总报告、风险态势篇、政策法规篇、技术产业篇、国际治理篇、附录（大事记）六大部分。总报告提出，受大国关系等国际现实政治在网络空间投射的影响，各国在网络空间国际治理上的竞合博弈日益错综复杂。我国网络强国建设事业已经步入攻坚期和深水区，我国网络空间治理需要加强系统性、整体性、协同性，更加注重统筹国内国际两个大局，深化国家网络综合治理体系建设，参与全球网络空间治理工作。

各篇章由若干子报告组成，主题包括中国网络治理权、数据管理、数据产权化、个人信息保护监管、数据出境、漏洞挖掘、区块链安全、车联网安全、网络直播生态治理、网络安全产业等；大事记对 2017 年国内外重大网

络空间安全事件进行了回顾扫描。

本报告认为，2017 年以来，全球网络空间发展格局进入变革调整关键时期，打击网络犯罪和恐怖主义、应对网络攻击等传统网络安全领域的结盟与对抗加剧，围绕新兴领域国际规则制定权和主导权的竞争与合作也越发激烈，我国网络空间治理的顶层设计和总体架构基本确立，高速、移动、安全、泛在的新一代网络基础设施建设持续推进，基础性、前沿性、非对称技术创新不断加速，网络化、智能化、服务化、协同化的数字经济新形态蓬勃发展，动态综合、协同高效的网络安全保障能力快速提升，网络空间国际话语权和影响力日益增强。

“网络空间安全”蓝皮书由上海社会科学院信息研究所与中国信息通信研究院安全研究所联合主编，由中国信息安全测评中心、公安部第三研究所、中国现代国际关系研究院、上海国际问题研究院、腾讯公司安全管理部等机构的学者和专家共同策划编撰。本系列蓝皮书旨在从社会科学视角，以年度报告形式，跨时空、跨学科、跨行业观测国内外网络空间安全现状和趋势，为广大读者提供较为全面的网络空间安全立体图景，为推动我国网络强国建设提供决策支持。

目　录

Ⅳ 技术产业篇

Ⅴ 国际治理篇

Ⅵ 附录

皮书数据库阅读使用指南

总 报 告

General Report

B.1

全球数字经济浪潮下网络空间安全：全球变局与中国创新

覃庆玲　惠志斌*

摘　要： 当今世界正在进入以信息产业为主导的经济发展时期，全球数字化浪潮风起云涌。特别是2017年以来，全球数字经济加速成形，并进入带动传统经济向新经济发展的爆发期和黄金期。在数字经济大潮下，网络空间安全也呈现远不同于以往的趋势特点，新型网络攻击、隐私泄露、虚假新闻等各类安全问题更加突出。网络空间安全已成为事关全球各国和地区安全的重要问题。然而，随着网络空间治理逐步深入，各国

* 覃庆玲，中国信息通信研究院信息通信安全研究所副所长，院互联网领域副主席，主要研究方向为电信监管、互联网管理、信息安全；惠志斌，上海社会科学院互联网研究中心执行主任，信息研究所信息安全研究中心主任，副研究员，管理学博士，主要研究方向为网络安全和数字经济。

围绕网络空间利益的竞合博弈更趋复杂激烈，各类国际规则制定进程更加曲折反复。中国作为全球网络大国，应积极把握新一轮产业变革和数字经济带来的机遇，主动应对网络空间安全带来的挑战。

关键词： 数字经济　网络空间　网络安全

从全球来看，以互联网为代表的新一代数字技术持续创新，与传统产业的渗透融合不断拓展和深化，正经历从局部扩散到全面融合、从量变到质变的过程，世界正在进入以数字经济为驱动的新经济发展时期。2017 年第四届世界互联网大会发布的《世界互联网发展报告 2017》指出，目前全球 22% 的 GDP 与涵盖技能和资本的数字经济紧密相关。数字技能和技术的应用到 2020 年将使全球经济实现增加值 2 万亿美元，到 2025 年全球经济总值增量一半来自数字经济。[①] 全球主要大国和地区都将发展数字经济作为新时期构建国家竞争优势、实现经济社会可持续发展的核心内容。

在 2017 年 12 月中共中央政治局关于实施国家大数据战略的第二次集体学习会上，习近平总书记指出大数据发展日新月异，应该审时度势、精心谋划、超前布局、力争主动，从推动大数据技术产业创新、构建以数据为关键要素的数字经济、运用大数据提升国家治理现代化水平及促进保障和改善民生等方面提出了中国数字化发展道路，并突出强调切实保障国家数据安全。这些重要论述和重大部署，在进一步明确我国加快推进数字中国建设、培育未来数字竞争新优势的战略支点和突破口的同时，对保障网络空间安全提出新任务、新要求。

一　全球数字浪潮下网络空间安全趋势与特点

当前，全球数字化、网络化、智能化浪潮深入推进，网络空间安全呈现

① 埃森哲：《数字化颠覆：实现乘数效应的增长》，2016 年 2 月。

新态势、新特点。一是交叉融合的数字技术触发网络攻防新范式。量子计算机、虚拟化、区块链等新兴数字技术的发展不断催生出新的网络攻击手段，全球网络攻防对抗的强度、频率、规模和影响力不断升级，网络空间的攻防博弈也呈现不同以往的新特性。从传统的漏洞后门、远程控制、社会工程学发展到利用人工智能技术对抗沙箱、利用暗网技术隐藏攻击身份、利用量子计算机暴力破解高强度加密，甚至是在勒索软件支付赎金环节利用加密货币逃避溯源检测等。二是泛在连接的数字基础设施打破网络空间固有边界。随着泛在接入、无线通信等信息技术快速发展，天地一体的立体化多层次网络覆盖体系逐渐成形，高空长续航浮空平台（如谷歌气球）、多轨道宽带卫星通信网络（如卫星互联网）、全球卫星导航定位系统迅猛发展。同时，工业互联网、车联网、可穿戴设备、智能家居等的普及应用，使联网对象从人人互联到万物互联，以软件为载体的网络功能虚拟化（NFV）和软件定义网络（SDN）技术使网络架构更加简化，为网络资源的充分灵活共享和业务应用的快速开发部署提供了方向。依托泛在通信技术构建的信息网络打破了网络空间固有边界，带来了网络应用形态的持续动态变化，加大了网络信息的不可预测性，给打击网络犯罪、维护网络安全、规制网络服务提供者造成管理和技术上的双重障碍。三是智能交互的数字化应用助长数据资源攫取。数字化应用全面渗透到人类生产生活各个领域，以“互联网 +”为代表的跨界融合新形态，广泛汇聚线上线下各种资源，打通研发、生产、流通、消费等各个环节的信息流，加速数据的跨界流动和融合利用，促进网络数据的集中汇聚、分析和利用。这些存储海量信息的数字化应用平台成为事实上的“信息枢纽”，成为实施数据关联分析和深度挖掘、攫取利益的重要舞台。借助海量数据的实时感知、泛在获取、云端计算、智能挖掘等数字技术的综合集成，国家、企业、组织甚至个人可以便利地通过网络空间获取具有政治、经济、社会等价值的信息。

随着以互联网为代表的数字技术应用与经济社会各领域的融合渗透持续深化，网络空间安全问题逐步上升成为各国关注的焦点议题，其在国家安全领域的战略性价值日益凸显。针对网络安全领域所出现的新问题、新

趋势和新风险，各国纷纷出台或更新网络空间战略。作为欧洲数字经济发展的先行者，英国政府在2017年3月便提出了新时期发展数字经济的顶层设计《数字战略2017》，并将解决好数字经济背景下的隐私和伦理等问题作为七大战略目标之一。同年10月，英国政府又发布了互联网安全战略绿皮书，阐明英国在处理网络危害问题上发挥政府作用的宏大目标，联合志愿组织、科技公司、学校和英国公民等社会各方力量，建立一种协调方式来解决在线安全问题。土耳其政府于2017年9月对外发布新闻称，为应对日益严峻的网络安全问题和各类全新的威胁挑战，土耳其政府正在着手制定“国家网络安全战略与行动计划”，特别针对跨境数据传输、网络反恐和企业安全职责等新生威胁或新兴问题，开展了系统的规划；哈萨克斯坦政府则于同年10月正式批复执行“国家网络安全战略”，即哈萨克斯坦网盾计划，该计划是哈国首次开展建设的一项大型网络安全系统工程，涵盖“政策措施调整”、“基础设施建设”和“国际交流合作”等多项发展任务，旨在有效应对网络空间领域不断加剧的新威胁和新挑战。美国特朗普政府在2017年12月发布的新版《国家安全战略》（以下简称《战略》）中，将网络空间安全问题提升为国家安全的重要事项。《战略》首次提出了“网络时代”的概念，并首次以单独章节的形式明确了保障美国网络时代安全的目标，突出强调“美国如何应对网络时代的机遇与挑战，将决定其未来的繁荣与安全”，这是美国政府在国家安全文件中第一次确认网络安全的极端重要性。

我国在主动顺应互联网发展大趋势下，经历20余年持续快速发展，实现了国内互联网产业从无到有、从小到大的健康发展，取得了令世界瞩目的成果。2017年，我国网民规模达7.72亿，连续10年位居世界第一；技术创新能力大幅提升，信息技术发明专利授权数达16.7万件，我国创新指数在全球排名上升到第22位，是唯一进入前25名的中等收入国家，跻身全球创新领导者行列；[①] 在即时通信、电子商务、移动支付、共享经济等网络应

① 摘自国家互联网信息办公室发布的《数字中国建设发展报告（2017年）》。

用领域形成本土创新优势；一批立足本土创新、具有国际影响力的大型互联网企业迅速崛起，我国成为仅次于美国的互联网大国。更值得一提的是，2017 年我国数字经济规模达到 27.2 万亿元，占 GDP 比重达到 32.9%，总量位居全球第二。[①] 伴随着我国数字经济发展的高歌猛进，网络空间安全日益成为我国国家安全战略乃至国际合作的重要内容，继 2016 年 12 月发布并实施《国家网络空间安全战略》之后，中国外交部和国家互联网信息办公室于 2017 年 3 月共同发布《网络空间国际合作战略》，这是中国首次就网络问题发布国际战略，是指导中国参与网络空间国际交流与合作的战略性文件。[②]

全球数字经济大发展背景下，网络空间承载着技术创新突破、数字经济发展、国际竞争角逐等多重多维职能，网络空间安全的内涵和外延比以往任何时候都要丰富，内外因素比以往任何时候都要复杂，种种威胁和挑战的联动、交织、共振、转化效应比以往任何时候都要突出。

二　2017年全球网络空间安全总体态势

2017 年以来，各类网络安全事件不断涌现，网络攻击特征变化导致全球网络安全威胁更趋严重，维护网络空间和平稳定的国际治理呼声日益高涨。然而，各国政府参与网络空间治理程度日益加深，大国现实政治与网络空间映射关系不断深化，各方围绕各类治理议题的竞合对抗博弈更趋复杂。与此同时，在数字经济全球化浪潮驱动下，人工智能、区块链、物联网等新兴技术快速兴起，围绕新兴技术领域的国际治理大幕正在开启。

（一）全球网络攻击呈现全新特征，基础设施面临严峻威胁

2017 年，针对公共卫生、电信网络、交通设施等重点民生领域的全球

① 摘自国家互联网信息办公室发布的《数字中国建设发展报告（2017 年）》。

② 《网络空间国际合作战略》，新华网，http://www.xinhuanet.com/2017-03/01/c_1120552256.htm，2017 年 3 月 1 日。

性网络安全事件频发，5 月 WannaCry 勒索软件席卷全球，6 月 FireBall、暗云等病毒持续来袭，7 月黑客针对英国关键信息基础设施开展攻击，8 月仙女座大规模模块化僵尸网络频现，10 月坏兔子勒索软件感染欧洲多国基础设施，11 月美国最大的 DNS 供应商 Dyn 系统遭遇大规模攻击。相较以往，当前全球范围的网络攻击日益呈现武器化、融合化、智能化的新特征。最典型的事件是 WannaCry 勒索病毒的爆发，全球 150 多个国家和地区的 30 多万台电脑、至少 28000 余个机构被感染。其中，美国、中国东部和欧洲西部等信息化程度高的国家和地区成为病毒感染的重灾区，受污染领域涉及公共卫生、电信、能源、交通以及政府部门等各类关键信息基础设施。WannaCry 勒索病毒所利用的“永恒之蓝”漏洞不仅印证了美国网络武器库的存在，及其巨大的波及范围和潜在破坏力，也侧面反映了网络攻击背后无法忽视的国家行为，网络安全问题的政治化、军事化日益将全球网络空间推入更加危险的境地。同时，WannaCry 勒索病毒融合微软操作系统漏洞、木马和蠕虫等攻击方式，并利用暗网技术获得隐蔽通信渠道，通过设置对未注册域名的访问作为后台控制加密和感染传播“总开关”，最终以比特币等加密货币完成对用户的勒索支付，这些融合化、智能化的网络攻击手段不仅起到规避反病毒技术检测、实现快速传播的作用，也有效逃避了对犯罪活动的追溯，达到隐藏攻击者身份的目的。

（二）网络安全国际规则推进艰难，治理平台博弈日趋复杂

随着网络空间国际治理逐步走入深水区，主要国家围绕网络空间利益的争夺日趋激烈，国际规则制定进程举步维艰。在 2016～2017 年联合国信息安全政府专家组的最后一次会议上，25 个国家官方代表因自卫权、反措施等相关国际法在网络空间适用方面的明显分歧，导致谈判最终破裂，未能就国家主体的网络空间行为规范达成具有共识的成果性文件，这标志着在联合国治理框架下，网络空间治理进程从原则性规范转向具体条款适用的新阶段，由于直接关系到各国在网络空间的核心安全利益，在缺乏有效共识的情况下，达成一致可接受的成果越发艰难。相比于联合国框架下网络空间治理