B 工业和信息化蓝皮书

BLUE BOOK OF INDUSTRY AND INFORMATIZATION

世界网络安全发展报告

(2016~2017)

主编 / 尹丽波

国家工业信息安全发展研究中心

ANNUAL REPORT ON WORLD CYBER SECURITY

(2016-2017)

2017版

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

工业和信息化蓝皮书
BLUE BOOK OF
INDUSTRY AND INFORMATIZATION

世界网络安全发展报告（2016~2017）

ANNUAL REPORT ON WORLD CYBER SECURITY (2016-2017)

主　编／尹丽波
国家工业信息安全发展研究中心

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

图书在版编目(CIP)数据

世界网络安全发展报告.2016-2017/尹丽波主编
. --北京：社会科学文献出版社，2017.6
（工业和信息化蓝皮书）
ISBN 978-7-5201-0381-7

Ⅰ.①世… Ⅱ.①尹… Ⅲ.①计算机网络-网络安全
-研究报告-世界-2016-2017 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字（2017）第036760号

工业和信息化蓝皮书
世界网络安全发展报告（2016~2017）

主　　编/尹丽波

出 版 人/谢寿光
项目统筹/吴　敏
责任编辑/宋　静

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　59367018
印　　装/北京季蜂印刷有限公司

规　　格/开 本：787mm×1092mm　1/16
印 张：21.75　字 数：362千字
版　　次/2017年6月第1版　2017年6月第1次印刷
书　　号/ISBN 978-7-5201-0381-7
定　　价/89.00元

皮书序列号/PSN B-2015-452-5/6

本书如有印装质量问题，请与读者服务中心（010-59367028）联系

权威·前沿·原创

皮书系列为
“十二五”“十三五”国家重点图书出版规划项目

工业和信息化蓝皮书
编　委　会

《世界网络安全发展报告（2016～2017）》
课 题 组

课题编写 国家工业信息安全发展研究中心
网络与信息安全研究部

顾　　问 何德全　崔书昆　胡红升　沈　逸

组　　长 何小龙

副 组 长 刘　迎　张　格　张　恒

成　　员 肖俊芳　于　盟　李　俊　张慧敏　孙立立
刘京娟　杨帅锋　张　妍　刘　冬　程薇宸
吴艳艳　王　墨　江　浩　唐　旺　胡　彬
刘文胜　杨佳宁　张哲宇　孙　军　黄　丹
刘小飞　董良遇　唐旖浓　李耀兵　李　敏
王晓磊　程　宇　张　莹　郭　娴　赵　冉
伍　扬　张　伟

主编简介

尹丽波 国家工业信息安全发展研究中心（工业和信息化部电子第一研究所）主任，高级工程师。国家工业信息安全产业发展联盟理事长、中国两化融合咨询服务联盟副理事长、国家网络安全检查专家委员会秘书长。长期从事网络信息安全和信息化领域的理论与技术研究，先后主持工业转型升级专项、国家发改委信息安全专项、国家242信息安全计划等几十项重要研究课题，作为第一完成人获部级奖励1项。

国家工业信息安全发展研究中心

国家工业信息安全发展研究中心（工业和信息化部电子第一研究所），前身为工业和信息化部电子科学技术情报研究所，成立于1959年，是我国第一批成立的专业科技情报研究机构之一。

围绕工业和信息化部等上级主管部门的重点工作和行业发展需求，国家工业信息安全发展研究中心重点开展国内外信息化、信息安全、信息技术、物联网、软件服务、工业经济政策、知识产权等领域的情报跟踪、分析研究与开发利用，为政府部门及特定用户编制战略规划、制定政策法规、进行宏观调控及相关决策提供软科学研究与支撑服务，形成了情报研究与决策咨询、知识产权研究与咨询、政府服务与管理支撑、信息资源与技术服务、媒体传播与信息服务五大业务体系。同时，国家工业信息安全发展研究中心还是中国语音产业联盟、中国两化融合服务联盟、国家工业信息安全产业发展联盟的发起单位和依托单位。

国家工业信息安全发展研究中心将立足制造强国和网络强国的战略需求，以“支撑政府、服务行业”为宗旨，以保障工业领域信息安全、推进信息化和工业化深度融合为方向，致力于成为工业信息安全和两化融合领域具有国际先进水平的国内一流研究机构，成为国家战略决策的高端智库和服务行业发展的权威机构。

序

新一轮科技革命和产业变革正在兴起，制造业与互联网融合发展，使其数字化、网络化、智能化特征越来越明显。云计算、大数据、物联网等新一代信息技术席卷全球，典型应用层出不穷，人工智能、量子计算、光通信、3D 打印等前沿技术正取得重大突破。以智能制造、信息经济为主要特征的信息化社会将引领我国迈入转型发展新时代。

由国家工业信息安全发展研究中心编写的“工业和信息化蓝皮书”已连续出版三年，在业界形成了一定的影响力。2016～2017 系列蓝皮书在深入研究和综合分析的基础上，密切跟踪全球工业、网络安全、人工智能、智慧城市和信息化领域的最新动态，主题覆盖宽广、内容丰富翔实、数据图表完备，前瞻探索颇具深度。

值此系列图书付梓出版之际，谨以此序表示祝贺，并期望本系列蓝皮书能对我国制造强国和网络强国建设有所助益。

工业和信息化部党组成员、副部长

2017 年 5 月 23 日

摘　要

当今时代，基于信息网络的技术创新、变革突破、融合应用空前活跃，网络已经渗透到政治、经济、文化、社会、军事等各个领域，网络空间已成为继陆地、海洋、天空、太空之外的“第五空间”，信息资源与关键信息基础设施已成为国家发展最重要的“战略资产”和“核心要素”，网络安全在国家安全诸要素中的地位日益凸显。以美国为首的发达国家对网络安全的重视达到前所未有的程度，纷纷将网络安全上升到国家安全与发展的战略高度，并加强了争夺网络空间优势地位、抢占国家综合实力制高点的部署和行动。

随着我国经济发展和社会信息化进程加快，网络信息技术在国家政治、经济、文化等领域的应用日益广泛，保障网络安全已经成为关系国家经济发展、社会稳定乃至国家安全的重要战略任务。习近平总书记指出：网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国……没有网络安全就没有国家安全，没有信息化就没有现代化。中央网络安全和信息化领导小组的成立，进一步强化了网络安全工作的顶层设计和总体协调。党的十八大，十八届三中、四中、五中、六中全会都把网络安全作为重要议题，强调完善网络安全法律法规，加强网络安全问题治理，确保国家网络安全。建设网络强国战略目标的提出，发展“互联网＋”、大数据、智能制造等行动计划的出台，国家网络空间安全战略的发布，为未来我国网络安全保障与建设指明了方向。《中华人民共和国网络安全法》的出台，使网络安全各项工作开展和推进正式步入有法可依、有据可循新阶段。

立足新时期、面对新形势，为更好地反映国内外网络安全发展态势和特点，及时把握世界各国在网络安全战略、政策、技术、产业发展等方面的最新动向与进展情况，为政府部门和军方、行业、有关企事业单位以及相关科研机构提供决策信息参考，国家工业信息安全发展研究中心网络与信息安全研究部

在对2016年世界网络安全领域持续跟踪的基础上推出了《世界网络安全发展报告（2016～2017）》。报告详细阐述了世界主要国家和地区的信息安全政策与措施，密切跟踪国内外网络安全领域技术动向与产业发展状况，全面、深入分析了世界网络安全领域发展态势与特征。

2009年以来，国家工业信息安全发展研究中心每年编写世界网络安全发展年度报告。《世界网络安全发展报告（2016～2017）》以2016年世界网络安全领域的新情况、新动态和新进展为着眼点，通过对网络安全战略法规、网络安全政策制度、工控信息安全、政府网络安全、网络安全技术及网络安全产业等内容的系统梳理与分析，总结提炼了2016年世界网络安全发展态势与特征，并对未来世界网络安全发展趋势进行了预测和展望。

目　录

V 政府网络安全篇

VI 网络安全技术篇

VII 网络安全产业篇

VIII 附录

皮书数据库阅读使用指南

总 报 告

General Report

B.1
世界网络安全特征与趋势

刘京娟 杨帅锋 肖俊芳*

摘 要: 2016年，网络空间博弈持续发酵，关键信息基础设施的安全防护不容乐观，少数国家多管齐下提升网络军备实力，全球网络安全形势仍然十分严峻。维护国家网络空间安全已成为国际共识，世界各国重视加强顶层设计，积极开展双边、多边合作。未来，中美在网络安全领域的关系将步入新阶段，严厉打击网络犯罪的需求将愈发迫切，新技术、新应用的安全问题将日益凸显。

关键词: 网络安全 网络空间 风险 合作

* 刘京娟，硕士，国家工业信息安全发展研究中心工程师，研究方向为网络安全政策法规、大数据网络安全、关键信息基础设施保护；杨帅锋，硕士，国家工业信息安全发展研究中心助理工程师，研究方向为工业信息安全、网络安全战略规划；肖俊芳，博士，国家工业信息安全发展研究中心高级工程师，研究方向为网络安全战略规划与情报分析。

一　世界网络安全总体态势与特征

（一）网络空间博弈持续发酵

2016 年，国家、政府与企业间在网络空间的博弈加剧，其中，国家、地区间的博弈焦点主要围绕国际话语权争夺、国家经济利益维护以及网络攻击和窃密行为；企业与政府博弈则更多地聚焦于加密技术与监控的对抗。与此同时，随着网络空间的战略地位逐渐上升，现实世界的物理冲突蔓延至网络空间，少数国家间甚至爆发网络冲突。

1. 大国围绕国际话语权展开角逐

近年来，美国持续通过垄断核心技术资源、制定推出国际标准规则、加大网络意识形态渗透、加强网络军备建设等手段把持并强化其网络霸主地位，掌控着网络空间的话语权。尽管“棱镜门”事件对美国在国际上的声誉造成了严重不良影响，甚至对美国互联网控制权产生冲击，然而美国并未放弃对网络主导权的把控。2016 年，美国依然延续其一贯作风，在谋求网络主导权的路上越行越远。一方面，美国丝毫不掩饰其意欲制定国际网络规则的野心和行动。2016 年 3 月，据公开发表的《美国国务院国际网络空间政策战略》，美国已经制定并且正在推进有关国际网络稳定性的战略框架，这一战略框架已经获得专注于国际安全环境下信息和通信领域发展的联合国信息安全政府专家组（UNGGE）的支持。此外，2016 年，美国官员多次在公开场合标榜其他国家应该效仿和应用美国制定的网络安全标准和立法，世界需要遵守美国的网络规范。2016 年 10 月 19 日，美国白宫发言人欧内斯特表示，推动建立网络空间国际规则应该是下一任美国总统面临的国家安全重要“优先事项”。另一方面，尽管美国已于 2016 年 10 月 1 日将互联网数字分配机构（IANA）职能管理权移交给互联网名称与数字地址分配机构（ICANN），但是美国为这一移交设定了有利于其自身的前提条件，那就是不交给联合国、国际电信联盟或其他政府间机构，而是交给“全球互联网多利益攸关社群”（包括学界、民间组织、行业组织、政府等），而美国依然将通过比其他国家强大得多的企业、硬件和软件技术、人才等优势继续保持其对全球互联网管理的至高影响力。事实上，这

一移交在美国国内也曾遭遇重重阻碍，其移交过程甚至“一波三折”。

面对美国这一行径，包括中国在内的新兴国家坚持网络空间国际规则的制定要在联合国框架下进行，主张各国在网络空间应遵守以《联合国宪章》为基础的国际法和公认的国际关系基本准则，推动建立网络空间新秩序。早在2011年，中国和俄罗斯等国即向联合国大会提交了《信息安全国际行为准则（草案）》，之后综合国际社会意见和形势发展，上海合作组织成员国对该准则草案进行修改更新，并于2015年1月向联合国大会提交了新版“信息安全国际行为准则”，作为联合国大会正式文件散发，中俄等国积极在联合国层面推动该准则的落实。2016年6月25日，中俄两国元首发表《中俄协作推进信息网络空间发展联合声明》，声明提到“支持各国维护自身安全和发展的合理诉求，倡导构建和平、安全、开放、合作的信息网络空间新秩序，探索在联合国框架内制定普遍接受的负责人行为国际准则”，并提出“主张各国均有权平等参与互联网治理”，“倡议建立多边、民主、透明的互联网治理体系，支持联合国在建立互联网国际治理机制方面发挥重要作用”，中俄基于此声明达成7点共识。

2. 多个国家和地区在网络空间频频“交锋”

2016年，美国、俄罗斯、韩国、朝鲜、土耳其、泰国、缅甸、印度、巴基斯坦等多个国家和地区在网络空间领域存在“摩擦”。

一是多个国家指责他国对其实施网络攻击和窃密等行为。美国多次指责中国、俄罗斯对其实施网络攻击和窃密活动，表示中俄正利用隐秘网络行动窃取其机密。此外，韩国和朝鲜相互指责抨击：韩国政府指控朝鲜加强了对其政府的网络攻击，并对其国防承包商发起网络攻击；朝鲜则称韩国的网络攻击指控纯属捏造。美国除了指责中国、俄罗斯外，还指控伊朗对其银行和纽约大坝进行网络攻击，并对伊朗黑客提起诉讼。

二是国家间、地区间冲突蔓延至网络空间，少数国家甚至爆发网络冲突。全球范围内，土俄、泰缅、韩朝、印巴等多个国家间、地区间的物理冲突也在网络空间得到体现。土耳其工业科学与技术部部长承认，土俄关系紧张致黑客攻击增强。泰国曼谷的多个警局网站遭受黑客攻击，泰警方怀疑网络攻击事件与龟岛判决有关。此外，韩国在朝鲜核爆试验后提高军队网络防御能力，并针对朝鲜网络攻击加强安全防范措施。印度与巴基斯坦的紧张局势也蔓延至网络

空间。两岸关系问题引发社交媒体网络大战。这些都是现实世界冲突蔓延至网络空间的真实案例。除了物理冲突蔓延至网络空间外，少数国家间甚至爆发网络冲突。继2015年底乌克兰电网遭受俄罗斯黑客攻击后，2016年1月，乌政府称俄罗斯针对其最大机场发动网络攻击，使其感染黑色能量（Black Energy）病毒。2016年10月，英国军方承认其对控制伊拉克摩苏尔的“伊斯兰国”武装分子发动网络战争，支援伊拉克部队重夺重镇摩苏尔的战役。

3. 企业与政府在网络空间领域存在激烈博弈

这方面，2016年最为典型的例子是著名科技公司苹果与美国联邦调查局（FBI）在关于加密与隐私监控方面开展的持久拉锯战。这一“隐私大战”或将在历史上留下浓墨重彩的一笔。在这场旷日持久的“斗争”中，美国FBI认为，出于打击恐怖主义需要，要求苹果公司提供“适当的技术协助”，为这部手机“开后门”，从而取出手机中的数据，苹果公司则认为政府要求对苹果手机“开后门”的做法会威胁到用户的安全，不能容忍和接受，双方就这一分歧过招数回合，FBI通过联邦法官的法庭指令，要求苹果为联邦调查局开发“政府系统”。苹果CEO库克则发表公开信谴责FBI行为，随后也以判决违反美国宪法第一修正案和第五修正案为由提出异议，并要求法庭重新考虑和解除此前颁布的强制令。这场战火还烧到了整个科技圈，Facebook、谷歌、亚马逊、Twitter、WhatsApp、微软等都表态支持苹果；FBI则得到了奥巴马、特朗普等政界人士的支持。虽然，最后FBI通过第三方破解公司破解了苹果手机，为这场“战争”暂时画上了一个句号，但是政府监管层面和公司保护用户隐私之间的博弈远没有结束。

企业维护商业利益与国家维护网络安全以保障国家安全之间存在摩擦与纷争，企业希望国家尽可能少地为了国家安全牺牲商业利益，而国家则将维护国家安全放在至高无上的地位，矛盾的主要焦点是国家安全和商业利益。在美国，商业利益集团使用个人隐私作为盾牌，来抵制国家权力的扩张；在中国，这些商业利益集团则通过利用自由贸易和国际规则，来抵制国家主权的管辖。

（二）部分国家和地区网络安全顶层设计增强

2016年，美国、欧盟、印度、澳大利亚等多个国家和地区通过加强立法、制定与更新战略计划等手段加强其网络安全顶层设计。