B 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(2015)

主编/惠志斌　唐涛

上海社会科学院信息研究所

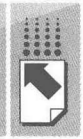
ANNUAL REPORT ON DEVELOPMENT OF CYBERSPACE SECURITY IN CHINA (2015)

2015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（2015）

ANNUAL REPORT ON DEVELOPMENT OF CYBERSPACE SECURITY IN CHINA (2015)

主　　编 / 惠志斌　唐　涛
上海社会科学院信息研究所

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. 2015/惠志斌，唐涛主编. —北京：社会科学文献出版社，2015. 4
（网络空间安全蓝皮书）
ISBN 978 - 7 - 5097 - 7362 - 8

Ⅰ. ①中… Ⅱ. ①惠… ②唐… Ⅲ. ①计算机网络 - 安全技术 - 研究报告 - 中国 - 2015 Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字（2015）第 069843 号

网络空间安全蓝皮书
中国网络空间安全发展报告（2015）

主　　编 / 惠志斌　唐　涛

出 版 人 / 谢寿光
项目统筹 / 郑庆寰
责任编辑 / 郑庆寰　陈　颖

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　59367090
读者服务中心（010）59367028
印　　装 / 北京季蜂印刷有限公司

规　　格 / 开 本：787mm × 1092mm　1/16
印 张：22. 75　字 数：379 千字
版　　次 / 2015 年 4 月第 1 版　2015 年 4 月第 1 次印刷
书　　号 / ISBN 978 - 7 - 5097 - 7362 - 8
定　　价 / 79. 00 元

皮书序列号 / B - 2015 - 437

上海蓝皮书编委会

中国网络空间安全发展报告（2015）
编　委　会

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人，具有高级专业技术职称的25人，下有信息资源管理、信息安全、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、互联网实验室等机构建立合作关系，承接国家社科基金重大项目“大数据与云环境下国家信息安全管理范式及政策路径研究”（2013）、国家社科基金重点项目“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主要领导的批示。

---

* 欲了解网络空间安全发展最新动态，请关注“网安观察”微信公众号。

主编简介

惠志斌 上海社会科学院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空间安全、网络信息科学等，已出版《全球网络空间信息安全战略研究》《信息安全辞典》等专著和编著共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》等专业论文20余篇；现正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“大数据与云环境下国家信息安全管理范式及政策路径研究”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，多篇专报获中央领导批示；参加首届国家网络安全宣传周“网络安全专家30谈”，先后赴瑞士、印度、美国等国参加网络信息安全国际会议。

唐 涛 上海社会科学院信息研究所副研究员，兼任上海社科院《上海新智库专报》责任编辑。2009年毕业于武汉大学信息管理学院，获管理学博士学位。2007~2008年在美国威斯康星大学密尔沃基分校访问学习，2012~2013年在中央宣传部挂职工作。目前主要从事网络舆情、两化融合、信息社会等方面的研究。主持国家社科基金项目“移动互联网环境下网络舆情新特征、新问题与对策研究”、上海市政府发展研究中心项目“城市经济：网络化环境下的城市发展研究”、上海市经济和信息化委员会“上海市两化融合十三五规划前期研究”等课题。出版学术著作《网络舆情治理研究》，在核心期刊发表论文10多篇，多篇专报获中央领导批示。

摘　要

21 世纪人类跨入网络信息时代，网络空间成为继陆、海、空、太空之外人类赖以生存的“第五空间”，网络空间安全议题上升到国家战略层面受到各国高度重视。对我国而言，网络空间安全形势尤为复杂严峻，面临来自国内外的诸多挑战。2014 年 2 月 27 日，中央成立了网络安全和信息化领导小组，习近平总书记担任组长并提出“建设网络强国”的战略目标，我国网络空间安全研究面临前所未有的重大机遇和历史使命。

在此背景下，“网络空间安全蓝皮书”应运而生。本蓝皮书由上海社会科学院信息研究所联合国内相关学术和管理机构策划编撰，旨在从社会科学的视角，以年度报告的形式，跨时空、跨学科、跨行业地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。

作为“网络空间安全蓝皮书”的首部年度研究报告，《中国网络空间安全发展报告（2015）》以 2013 ~ 2014 年为研究背景（重要事件回溯至 2011 年），以习近平总书记关于建设网络强国的指导思想进行框架设计和内容组织，全书汇集国内二十余位专家学者的最新研究成果，分为序言、总报告、风险态势篇、政策法规篇、文化传播篇、产业技术篇、人才教育篇、国际合作篇、大事记等九个部分。其中序言从学理层面探讨了网络空间安全相关概念内涵和理论源流；总报告《挑战与变革：中国网络空间安全发展研究》全面分析了我国网络空间安全的总体现状以及发展对策；各专题篇由一篇综合性研究子报告，以及二三篇聚焦该专题领域细分问题的论文构成，涉及网络空间漏洞管理、网络安全审查制度、网络颜色革命、网络恐怖主义、数据主权、物联网安全等方面；大事记对 2011 ~ 2014 年国内外重大安全事件进行了回顾。

本报告认为，我国网络空间安全发展总体形势为：中国网络空间安全顶层设计取得重大突破，“棱镜门”事件全面拉响我国网络空间安全警报，新技术

新应用发展使我国网络空间系统性风险加剧，我国网络信息产业正被逐步纳入安全可控发展轨道，国家不断加大力度整治网络乱象维护网络清朗空间，网络个人信息安全事件频发成为重大社会问题，中国逐步登上全球网络空间治理的舞台，全国掀起网络空间安全人才教育的热潮。新时期我国网络空间安全需要在政策法律、文化传播、产业技术、人才教育、国际合作等多个方面综合施策，包括：秉持治理理念构建网络空间安全制度体系，以媒体融合为契机加快网络文化繁荣发展，以科技创新为核心驱动网络信息产业跨越发展，举全社会之力打造多层次网络安全人才队伍，抓住战略机遇积极推动全球网络空间新秩序的形成。

Abstract

In the 21st century, human beings has stepped into the age of the Internet. Cyberspace becomes the "fifth domain" which is of great importance to human life, alongside land, sea, air and space. Cyberspace security has been raised up to the national strategic level, and has absorbed great attention from every country. China is being challenged to confront the extremely complex and severe cybersecurity threats from home and abroad. In February 27, 2014, China established the Central Cybersecurity and Informatization Leading Group, President Xi Jinping headed this group and proposed the strategic goal of "building our country into a cyber power". Chinese cbersecurity research is facing an unprecedented great opportunity and historical mission.

In this context, *Blue Book of Cyberspace Security* is published at this historical moment. The series of books are compiled by the Institute of Information of Shanghai Academy of Social Sciences in association with relating domestic academic and management agencies. From the perspective of social sciences, in the form of the annual report, these books aim to observe the current situation and trends of cyberspace security at home and abroad across time and space, interdisciplinary, and cross-industry, present a relatively comprehensive stereoscopic picture of cyberspace security to the readers, and provide a decision-making support for promoting the construction of cyber power.

Annual Report on Development of Cyberspace Security in China (2015) is the first report of the *Blue books of Cyberspace Security*. With the big events in 2013 and 2014 serving as its research background (some important events date back to 2011), it is framed and organized on the basis of President Xi Jinping's guiding ideology of the construction of cyber power. This book incorporates the latest researches from more than 20 experts and scholars in China. It divides into nine sections, including preface, general report, risks & Situation, policies & laws, cultural communication, industry & technologies, talents & education, international governance and Chronicle

of Events. The preface theoretically discussed the origins of three concepts; the general report, *Research on the Development of Chinese Cyberspace Security: Challenges and Changes*, comprehensively analyzes the overall situation of cyberspace security in China and offers the countermeasures for cyberspace development. Each thematic section is composed of one comprehensive sub-study report, and two or three thesis focuing on segment problems, such as cybersecurity vulnerability management, cybersecurity censorship, Color Revolution in the Age of Internet, cyber terrorism, data sovereignty, IoT security. Chronicle of Events reviews the major domestic and abroadsecurity events from 2011 to 2014.

According to this report, currently, the overall cyberspace security development situation in China are: China's cyberspace security top level design has made great breakthroughs; NSA's "Prism" event of United States extensively raises the alarm of our cyberspace security; development of new technologies and applications increases the systematical risks of our cyberspace; China's information and communication industry is being gradually incorporated into the controlled security development track; the efforts of regulation on internet chaos and maintenance on the clearness of cyberspace have been intensified continuously; personal data leakage incidents frequently occur, becoming a major social issue; China has gradually appeared on the stage of global cyberspace governance; the whole country has spurred the fervor for cyberspace security's talents education. In this new era, China's cyberspace security needs to take integrated measures from multiple aspects of policy and law, cultural communication, industry and technology, talents and education, international cooperation, etc. These measures include upholding the idea of governance to build a cyberspace security system, taking the media convergence as an opportunity to accelerate the prosperity and development of cyberculture, taking the technology and innovation as the core to drive the development of information and communication industry, giving the power of the whole society to create a multi-layered cybersecurity workforce, and seizing the strategic opportunity to actively promote the formation of a new global cyberspace order.

论信息安全、网络安全、网络空间安全

王世伟*

信息安全、网络安全、网络空间安全是近年来国内外非传统安全领域出现频度较高的词语，在各国的安全战略和政策文件中，在相应的国家管理机构名称中，在新闻媒体的文字报道中，在理论学术研究的名词术语中，以及在各类相关的活动用语中，这几个概念交叉出现，但逻辑界限并不清晰，需要进行深入研究，以便在信息安全研究与实践的逻辑起点上有理性清晰的认知，在信息安全的基础理论研究中能形成业界内外具有共识的学术规范。本文主要依据近年来全球信息安全领域的文献资料，并结合与之相关的实践活动，对信息安全、网络安全、网络空间安全等概念及其相互关系做初步探讨。

一　“信息安全”的概念与涉及范围

（一）“信息安全”概念的出现和发展

信息安全的实践在世界各国早已出现，但一直到了20世纪40年代，通信保密才进入学术界的视野。20世纪50年代，科技文献中开始出现“信息安全”用词，至20世纪90年代，“信息安全”逐步进入各国和各地区的政策文献，相关的学术研究文献也逐步增加。总部设在美国佛罗里达州的国际信息系统安全认证组织（International Information Systems Security Consortium）将信息安全划分为十大领域，包括物理安全、商务连续和灾害重建计划、安全结构和

* 王世伟，上海社会科学院信息研究所研究员，主要研究方向为网络信息安全管理、智慧城市、大都市图书馆。

模式、应用和系统开发、通信和网络安全、访问控制领域、密码学领域、安全管理实践、操作安全、法律侦察和道德规划。可见，“信息安全”概念所涉的范围很广，在各类物理安全的基础上，包括了“通信和网络安全”的要素。据文献考察，1990 年成立的“德国联邦信息技术安全局”（BSI）（或译为“德国联邦资讯安全局”），是“信息安全”出现在机构名称中较早的例子。1992 年 3 月，欧盟理事会通过了“关于信息系统安全领域的第 92、242、EEC 号决定”，是欧盟较早的信息安全政策，也是“信息安全”一词出现在政策文件中较早的例子。1994 年 2 月，中国国务院出台了第一部关于计算机信息安全的法规《中华人民共和国计算机信息系统安全保护条例》；1996 年 2 月，法国也成立了“法国信息系统安全服务中心”。以上机构名称中均使用了“信息系统安全”。“信息安全”不仅成为机构和政策的用词，也逐渐细化为专指某一领域或某一方面的信息安全问题。

进入 21 世纪，“信息安全”一词出现的范围不断扩大，在各类文献中出现的频次也不断增加。“信息安全”成为各国安全领域聚焦的重点。既有理论的研究，也有国家秘密、商业秘密和个人隐私保护的探讨；既有国家战略的谋划，也有信息安全内容的管理；既有信息安全技术标准的制定，也有国际行为准则的起草。信息安全已成为全球总体安全和综合安全最重要的非传统安全领域之一。

（二）“信息安全”的内涵及其引申出的系列相关概念

所谓信息安全，指保障国家、机构、个人的信息空间、信息载体和信息资源不受来自内外各种形式的危险、威胁、侵害和误导的外在状态和方式及内在主体感受。信息安全从研究和实践而言，可以从诸多维度来观察。以信息安全威胁而言，包括信息主权的博弈、各类信息犯罪、各类信息攻防的技术等。以信息安全政策而言，包括国际和地区组织的政策、国家或城市的政策、某一领域和行业的政策、国际的双边与多边协议等。以信息安全法律而言，包括国际和地区组织的法律、国家或某一城市的法律、某一领域和行业的法律等。以信息安全标准而言，包括国际信息安全标准、国家信息安全标准、信息安全管理标准、信息安全认证标准、信息安全评价标准、信息安全等级标准、某一范围的信息安全标准等。以信息安全机构而言，包括国际或地区组织机构、国家机

构、各国的行业机构、学术研究机构和智库等。以信息安全产业而言，包括信息安全产业基地或产业园、信息安全企业、信息安全产学研创新联盟、信息安全产品、信息安全服务等。以信息安全教育而言，包括信息安全素养教育、信息安全专业教育、信息安全职业认证、信息安全教育实践等。以信息安全研究而言，包括信息安全研究机构、信息安全著作和论文、信息安全会议与论坛、信息安全刊物和网站等。

信息安全作为一个大的概念，也引申出一系列相关的概念，如信息主权、信息疆域、信息战等。所谓信息主权，是指一个国家对本国的信息传播系统和传播数据内容进行自主管理的权利，是信息时代国家主权的重要组成部分。由此也形成了信息疆域的概念，即同国家安全有关的信息空间及物理载体。在世界上，一些信息强国利用技术、语言、文化以及经济等方面的优势，控制、限制乃至压制他国信息内容的多样性、信息传播的自主性及信息管理的安全性。2014 年 7 月，习近平总书记在巴西出席金砖国家领导人第六次会晤和在巴西国会发表演讲时强调："互联网技术再发展也不能侵犯他国的信息主权。更不能牺牲别国安全谋求自身所谓绝对安全"，"国际社会要本着相互尊重和相互信任的原则，通过积极有效的国际合作，共同构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的国际互联网治理体系。"这里所提出的"信息主权"的概念，已经与建设民主平等的网络安全和构建全球互联网治理体系的创新思想联系在一起了。"信息战"的概念则折射出信息安全与网络安全概念的前后相续和相互交织。信息战的研究始于 20 世纪 90 年代初。1990 年沈伟光的《信息战》一书问世，较早地提出了信息战的新概念，被誉为"信息战之父"。1994 年，温·施瓦图出版了《信息战：电子高速公路上的混乱》一书，提出了"电子珍珠港事件"随时可能发生的警告，这一新思想启发了网络大规模杀伤性武器等新概念的提出。2000 年 4 月，俄罗斯总统普京签署了《新军事学说》，同年 6 月，俄罗斯发布了《国家信息安全学说》的国家政策文件，专门讨论军事领域的信息战问题，认为以侵略为目的的信息操作已成为世界形势不稳定的主要原因之一。以上列举的信息安全相关概念，都或多或少反映了信息安全与网络安全、网络空间安全概念具有紧密的联系。

二 “信息安全”与“网络安全”、“网络空间安全”的联系与区别

随着全球社会信息化的深入发展和持续推进，相比物理的现实社会，网络空间中的数字社会在各个领域所占的比重越来越大，有的已经超过了半数。数量的增长带来了质量的变化，以数字化、网络化、智能化、互联化、泛在化为特征的网络社会为信息安全带来了新技术、新环境和新形态，原来传统的信息安全主要体现在现实物理社会的情况发生了变化，信息安全已更多地体现在网络安全领域，反映在跨越时空的网络系统和网络空间之中，反映在全球化的互联互通之中。

（一）互联网的发展使信息安全向网络安全和网络空间安全聚焦

20 世纪 60 年代，当互联网发端之际，美国国防部高级研究计划署便将位于不同研究机构和大学的四台主要计算机连接起来，形成互联。20 世纪 70 年代，这样的互联进一步扩展至英国和挪威，逐步形成了互联网。20 年后的 1994 年 4 月，中国北京中关村的教育与科研示范网通过美国公司接入互联网国际专线，中国确立了全功能互联网国家的地位。随着互联网在全世界的普及与应用，信息安全便更多地聚焦于网络数字世界。网络带来的诸多安全问题成为信息安全发展的新趋势和新特点，已很难直接用“信息安全”一词来准确表述网络安全和网络空间安全的新进展，且无法深刻揭示网络安全和网络空间安全的新特征。虽然“信息安全”仍经常使用，但“网络安全”和“网络空间安全”开始与“信息安全”并举，甚或直接用“国际联网安全”“互联网安全”“网络安全”“网络空间安全”等词语。从 20 世纪 90 年代以来信息安全开始向网络安全聚焦，有一个逐步发展和逐步强化的过程。在 20 世纪 90 年代广泛使用的“信息安全”一词，在进入 21 世纪的十多年中，已逐步与“网络安全”和“网络空间安全”并用，而网络安全与网络空间安全使用的频度不断增强，这在发达国家的文献中尤为突出，中国对网络安全和网络空间安全的认知相对滞后。尽管信息安全至今仍然是人们常用的概念，但随着 2002 年世界经合组织通过了关于信息系统和网络安全的指南文件，特别是 2003 年美国

发布了网络空间战略的国家文件，“网络安全”和“网络空间安全”开始成为较之“信息安全”更为社会和业界所聚焦和关注的概念，在理论研究和实践中也使用得更加频繁。

（二）信息安全、网络安全、网络空间安全三者的异同

从上文所列举的国内外诸多政策和标准文献中，我们可以发现，信息安全、网络安全、网络空间安全三者往往交替使用或并行使用。如2003年12月在日内瓦召开的联合国“信息社会世界峰会”首次就信息社会问题进行了讨论，会议讨论通过的《日内瓦原则宣言》第五条原则“树立使用信息通信技术的信心并提高安全性”中，使用了“网络信息安全”的概念；会议通过的另一份文件《日内瓦行动计划》的十条措施中，多处并行使用了“信息安全”与“网络安全”两个概念。在中国，2012年6月，国务院发布《关于大力推进信息化发展和切实保障信息安全的若干意见》，文件中多次出现了“网络与信息安全”的用词，如“夯实网络与信息安全基础”“提升网络与信息安全监管能力”“提升网络与信息安全”等。说明信息安全在受到网络安全和网络空间安全影响的过程中，这三个词有一个混用的模糊期，使人们对这三个词语概念的理解和在实践的应用中产生一定程度的或然性，使学术规范受到了影响，也在实践应用中产生了不确定性。

同时，网络安全与网络空间安全这两个概念在实际使用中区分也并不严格。如2011年11月英国发布的《国家网络安全战略：在数字世界中保护和促进英国的发展》，文件名称中讲的是网络安全，但在文件的内容阐述中，专门讨论了网络空间如何驱动经济增长和变化中的威胁等问题；2014年11月在中国浙江乌镇举行首届世界互联网大会，主办方在会议文件中对“网络安全”板块的讨论则用“网络空间安全”的主题来表述，使人们对网络安全与网络空间安全的概念界限难以区分。

那么信息安全、网络安全和网络空间安全这三个概念究竟应当如何理解并区分呢？

1. 信息安全、网络安全与网络空间安全三者的相同点

（1）三者均类属于非传统安全。较之军事、政治和外交的传统安全而言，信息安全、网络安全、网络空间安全都类属于非传统安全，是进入20世纪末

特别是21世纪初以来人类所面临的日益突出的共同安全问题。2004年9月，中国共产党第十六届中央委员会第四次全体会议通过的《中共中央关于加强党的执政能力建设的决定》，明确指出要“确保国家的政治安全、经济安全、文化安全和信息安全”以及“确保国防安全”。2006年10月中国共产党第十六届中央委员会第六次全体会议通过的《中共中央关于构建社会主义和谐社会若干重大问题的决定》中再次强调了四大安全领域，即“确保国家政治安全、经济安全、文化安全、信息安全”。2012年11月中国共产党第十八次全国代表大会的报告中，先后提到了信息安全、太空安全、网络空间安全。2014年2月在中央网络安全和信息化领导小组第一次会议上进一步提出了网络安全的新要求。近年来中国与世界各国和各地区组织签订的双边和多边的各类协议和发表的共同声明中，信息安全、网络安全和网络空间安全成为相互协商和共同治理的重要内容。

（2）三者都聚焦于信息安全。信息安全可以理解为保障国家、机构、个人的信息空间、信息载体和信息资源不受来自内外各种形式的危险、威胁、侵害和误导的外在状态和方式及内在主体感受（指受威胁和误导等的状态，如网络空间战的对抗状态和方式、黑客攻击的状态和方式、传媒虚假信息带来的误导的状态和方式等）。网络安全、网络空间安全的核心也是信息安全，只是出发点和侧重点有所差别。

（3）三者可以互相使用，但有侧重点。信息安全使用范围最广，可以指线下和线上的信息安全，即既可以指称传统的信息系统安全和计算机安全等类型的信息安全，也可以指称网络安全和网络空间安全，但无法完全替代网络安全与网络空间安全的内涵；网络安全可以指称信息安全或网络空间安全，但侧重点是线上安全和网络社会安全；网络空间安全可以指称信息安全或网络安全，但侧重点是与陆、海、空、太空等并行的空间概念，并一开始就具有军事的性质；网络安全与网络空间安全与信息安全相比较，前两者反映的信息安全更立体、更宽域、更多层次，也更多样，更体现网络和空间的特征，并与其他安全领域有更多的渗透与融合。

2. 信息安全、网络安全与网络空间安全三者的不同点

（1）对应的英文名称反映了三者的视角不同。信息安全对应的英文是Information Security，网络安全对应的英文是Network Security或Cyber Security，