互联网实验室
ChinaLabs
年度蓝皮书系列

Broadview
www.broadview.com.cn

网络空间安全蓝皮书

2013-2014

主编 / 方兴东 崔光耀
执行主编 / 胡怀亮 李刚 彭琳

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

互联网实验室
ChinaLabs
年度蓝皮书系列

网络空间安全蓝皮书

主编 / 方兴东 崔光耀
执行主编 / 胡怀亮 李刚 彭琳

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

内 容 简 介

在网络空间风云变幻莫测的 2013 年至 2014 年，“安全”成为维护网络空间持续、健康发展的核心议题之一。本书着眼于全球网络空间安全的整体趋势，结合 2013 年至 2014 年国内外重大网络安全热点事件，洞察未来网络安全全球博弈的特点，探索中国的网安战略与实践策略。

本书汇集了政府部门、安全研究咨询机构、高等院校、咨询公司等网络安全领域的顶级专家、学者、行业意见领袖和独立学者的最新评论文章和报告，展示了当前网络安全领域研究的中坚力量及其独特的视角，对读者深入了解网络空间安全与发展的关系，以及体会网络安全态势及其演进趋势，都具有重要的启发意义。

本书适合安全专业领域人员，以及关注网络安全和互联网治理规律特点的普通读者和其他行业相关人士阅读。

图书在版编目（CIP）数据

网络空间安全蓝皮书. 2013～2014 / 方滨兴，崔光耀主编. —北京：电子工业出版社，2015.5
（年度蓝皮书系列）
ISBN 978-7-121-25802-2

Ⅰ. ①网… Ⅱ. ①方… ②崔… Ⅲ. ①互联网络－安全技术－白皮书－中国－2013～2014
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 067690 号

策划编辑：刘　皎
责任编辑：潘　昕
印　　刷：北京季蜂印刷有限公司
装　　订：北京季蜂印刷有限公司
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：720×1000　1/16　印张：17.25　字数：290 千字
版　　次：2015 年 5 月第 1 版
印　　次：2015 年 5 月第 1 次印刷
定　　价：75.00 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。
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。
服务热线：（010）88258888。

本书编写委员会

主编：方兴东、崔光耀

执行主编：胡怀亮、李刚、彭琳

参编机构：互联网实验室、《中国信息安全》杂志

“年度蓝皮书系列”编写委员会

丛书总策划：刘九如

丛书总编：方兴东

丛书主持：赵婕

执行策划：刘伟、孙雪

丛书编辑支持单位：数字论坛、博客中国

丛书编辑合作单位：互联网实验室、浙江传媒学院互联网与社会研究中心、电子工业出版社研究院

序

中国全面接入互联网并成为“世界头号网络大国”的20年，也是信息安全行业成长、发展和蔚然壮大的20年。虽然不像互联网行业那样成绩骄人，但信息安全行业的影响力却持续上扬，涉及范围日益扩大。可以说，信息安全融入了社会生活的方方面面，大到国家安全、经济发展和社会稳定，小到亿万百姓生产生活的各个环节，都深深铭刻了信息安全的印记，不仅为媒体和各社会各界广泛关注，甚至成为大国政治博弈的重要筹码。

这些年来，人们对信息安全的认识不断深化，从早期专注于做强密码以保证信息的安全性、完整性和可靠性的通信保密，到后来通过技术和管理手段防范威胁与风险的网络和信息安全，从终端到网络，从单机防护到系统安全——堵漏洞，筑高墙，严防死守，构建了全生命周期的信息安全保障体系。但是，网络信息技术日新月异的发展速度远远超出了人们的想象，网络应用的频次和范围不断增大，网络空间涵盖的区域也越来越广，由此，一个新的安全域悄然形成，它促使人们从更新颖的角度和更宽阔的视野来把握信息安全的内涵。在这种情况下，纯技术对抗的安全博弈时代渐行渐远，一个综合了国内和国际、政治和军事、个人和社会、技术与管理、攻防与内容、线上与线下、媒体与舆情等各种关系的网络空间大安全时代开启了，其标志之一当属美国《网络空间国际战略》的出台，而近年来国际上兴起的网络空间治理浪潮均与之有着密切的关联。可以看出，通信保密时代在于做强密码，网络信息安全时代主要是应对风险，网络空间安全时代则侧重把控网络。

国际社会网络空间安全的冷暖变化自然会直接或间接地反映到国内信息安全领域。

2003年在我国信息安全保障发展史上具有特殊的地位。这一年春天，美国出

台了《网络空间安全国家战略》。同年 7 月，我国信息安全保障的纲领性文件《关于加强信息安全保障工作的意见》（27 号文件）颁布，明确了信息安全保障工作的总体方针、目标和基本原则，是此后很长时间内国内信息安全保障的指针，虽然它与信息化强国美国较早地把信息安全确定为国家战略并制定了详细的措施相比还有差距，但从国家层面的认识程度和基本举措上看，还是基本保持了同步。在接下来的中共十六届四中全会上，又首次把信息安全与政治安全、经济安全、文化安全并列提出，在《2006-2020 年国家信息化发展战略》中也明确了信息安全保障工作的长远目标，但实质性的推进力度并不可观。当此之时，大洋彼岸的美国经过几届政府的努力，在信息安全领域动作频仍，但我们经过 10 年时间，还停留在 27 号文件的框架下，与发达国家的差距也越来越大。对这一点，中共十八届三中全会决定的说明中给出了深刻的总结："从实践看，面对互联网技术和应用飞速发展，现行管理体制存在明显弊端，主要是多头管理、职能交叉、权责不一、效率不高。同时，随着互联网媒体属性越来越强，网上媒体管理和产业管理远远跟不上形势发展变化。"

2014 年，中国信息安全迎来了久违的热潮。新一届中央领导审时度势、果断决策，成立了高规格的中央网络安全和信息化领导小组，统一领导协调国家网络安全和信息化的各项工作，把信息安全问题提高到战略全局的高度来统筹领导、总体布局、全盘把握，科学分析了安全与发展的辩证关系，明确提出了"没有网络安全就没有国家安全，没有信息化就没有现代化"的论断，明确了网络安全与信息化工作要着重致力于"网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进"的工作重点和建设网络强国的前进方向，从组织落实、顶层设计、战略制定、法规完善、科学管理、强化自有技术、开展国际合作等方面大步向前推进。由于抓住了矛盾的症结所在，因此，局面迅速打开，长期以来在与西方发达国家的网络博弈中所处的被动局面也出现转机，这是世人都看得到的事实。

在这个过程中，偶然曝光的斯诺登事件无疑起到了推波助澜的作用，它不仅帮助我们更加深刻地认识了网络空间安全较量的严峻形势，也在很大程度上改变了我们的安全观念。不过，与其说是斯诺登事件促成了我们政策上的革命，不如说是信息化发展的内在原因所形成的必然推动，斯诺登事件不过是提供了一个催

化的契机而已。

正如习近平总书记所指出的："网络安全和信息化对一个国家很多领域都是牵一发而动全身。"如今，云计算、物联网、移动互联网、大数据、智慧城市等信息技术革命的浪潮来势正猛，在错综复杂的环境下科学认识和把握信息安全的内在规律和发展趋势，努力实现网络强国的宏伟目标，绝不是一件轻松的事情，需要长期磨砺，长期积累，也需要各方面的专家学者深入研究思考，科学研判，指点网络江山，运筹决策智慧，以"建久安之势、成长治之业"。

我们期待这样的大智慧、大成果。

崔光耀

目　录

第一部分　总体形势篇 …… 1

第一章　2013 年网络空间安全发展研究报告 …… 2

第二章　2013 年我国信息安全基本状况 …… 34

第三章　2013 年全球信息安全形势大盘点 …… 39

第四章　2013 年全球各国信息安全建设情况 …… 55

第二部分　热点观察篇 …… 73

第五章　中央网络安全和信息化领导小组的由来及其影响 …… 74

第六章　源自未雨绸缪，贵在风雨同舟——解读中央网络安全和信息化领导小组成立 …… 83

第七章　“棱镜”系统折射中国网络安全面临严峻挑战 …… 93

第八章　斯诺登效应前因解读——与 Cyber 空间相关的博弈思考 …… 97

第九章　微软 Windows XP 事件拷问中国网络安全战略 …… 111

第十章　“空间网络”挑战网络空间安全 …… 127

第十一章　移动互联网时代的国家网络安全疆界变迁 …… 131

第三部分　战略观察篇 …… 141

第十二章　警钟长鸣 奋力前行——加紧构筑国家网络空间防御体系 …… 142

第十三章　高度关注信息安全十大系统性风险 …… 146

第十四章　信息安全是当今国家安全面临的最大挑战 …… 150

第十五章　美国国家网络安全战略的演进及其实践 …… 153

第十六章　关于构建我国网络安全法律制度的若干思考 …… 176

第十七章　试论网络安全立法与国家网络安全战略 …… 180

第四部分　网络治理篇 ……189

第十八章　浅析信息安全管理的网络思维 …… 190

第十九章　以实力保安全 vs.以治理谋安全 …… 195

第二十章　大战略基石——美国信息安全产业格局解析 …… 207

第二十一章　大数据时代个人信息安全保护 …… 219

第二十二章　“数据”呼唤“法”的全面呵护——从小米、携程、SSL 事件谈起 …… 223

第二十三章　2013 年主要民生舆情热点及特征分析 …… 226

第五部分　未来展望篇 ……237

第二十四章　中央网信小组带来无限期待 …… 238

第二十五章　网络安全与中美新型大国关系 …… 246

第二十六章　2014——中国网络空间战略元年 …… 253

附录 A　2013 年国内外信息安全热点事件 ……257

致谢 ……265

打造 21 世纪的走向未来丛书 ……266

第一部分

总体形势篇

第一章

2013年网络空间安全发展研究报告[①]

方兴东[②]　胡怀亮[③]　张　静[④]

（一）网络安全历史性的年份：2013-2014年

2013年，美国监控互联网丑闻持续发酵，中国是最大的受影响国之一。

2014年，是美国互联网45年，中国互联网20年——这是一个特殊的年份，也是一个历史拐点！

在人类网络空间安全的历史上，2013-2014年将占据特别重要的位置。2013年发生了震惊全球的斯诺登事件，这是全球互联网有史以来最重大的事件，其影响程度之深远将大大超越我们当下的估计。2014年，中央网络安全和信息化领导

---

① 本文原载于《新媒体蓝皮书——中国新媒体发展报告No.5（2014）》，社会科学文献出版社，2014年6月。

② 方兴东，中国互联网协会研究中心常务副主任，浙江传媒学院互联网与社会研究中心主任，互联网实验室和博客中国创始人兼董事长，中国“数字论坛”发起成员。清华大学传播学博士，浙江大学全球创业研究中心博士后。中国计算机学会第十届理事会理事，中国计算机学会企业工作委员会委员，中国计算机学会企业与职业发展工作委员会委员。出版著作《互联网创业地图——互联网如何改变中国的创业机制与财富走向》、《21世纪的书》、《IT史记》、《博客》、《起来——挑战微软霸权》等20部。10多年来为互联网、创业精神、挑战微软、Web 2.0、义乌等摇旗呐喊，被称为“网络旗手”、“博客教父”。

③ 胡怀亮，互联网实验室研究员，从事互联网、IT方向咨询研究超过3年。中国计算机学会会员，通信硕士。目前主要研究方向为网络空间战略、网络安全、网络治理。

④ 张静，1982年出生，女，硕士，互联网实验室副总裁。作为项目组主要成员参与了社科基金一般项目“微信传播的特点与功能研究（13BXW042）”，浙江省政府重点科技创新团队项目“网络媒体技术科技创新团队（2011R50019）”，在核心学术期刊上发表学术论文5篇。重点关注互联网产业前沿、网络安全、网络传播等领域的研究。

小组成立，这堪称中国互联网有史以来最重大的事件，其影响将是全局性和长期性的。这两大事件，让我们在勾勒 2013-2014 年全球和中国的网络空间安全态势与格局时，有了定海神针。

第一，这两大事件将直接影响国际和国内网络空间的格局，网络空间的治理体系，各国的网络政策和安全战略，产业竞争与发展，以及社会全民性的安全意识。2013 年是全球互联网发展过程中具有里程碑意义的一年，全球对网络安全的关注上升到史无前例的高度。全球互联网发展突飞猛进，同时使网络安全形势愈加严峻。从全球范围内，上至政府，下至普通民众，人们对给生产生活带来巨大影响的互联网，已经不仅从技术、经济的角度，而且从政治、社会和文化等角度，有更深刻的认识和理解。正因如此，网络空间安全形势关系到国家政治、经济、社会、文化、军事等多方面的安全，正如中央网络安全和信息化领导小组的第一次会议上明确指出的："网络安全和信息化对一个国家很多领域都是牵一发而动全身的。"

第二，在美国不断政治化的努力下，网络空间安全问题首先是政治问题，其次是社会问题，最后才是技术问题，由此，全球网络空间中美两强博弈的基本格局初步形成。网络安全研究工作早期叫信息安全研究，信息安全侧重于软件系统与业务流程安全及信息内容安全等领域。然而，在一些国家发生借助网络手段实施的"颜色革命"，2012 年中国的华为、中兴等企业遭到美国国会的调查，以及 2013 年斯诺登事件之后，网络安全问题已经延伸到国家政治安全、文化安全等领域，各国对网络安全问题的看法已经超越技术问题层面，上升到社会问题、政治问题层面。

2013 年下半年及 2014 年年初，又有 3 个重大事件发生。一是美国微软公司在 2014 年 4 月停止对 Windows XP 系统用户的技术支持与服务[①]，这导致中国的政府集中采购用户和大量普通用户的信息安全、网络安全受到极大威胁。二是中国成立了由党、政、军一把手担任组长的中央网络安全和信息化领导小组[②]，统筹管理国家网络安全领域的工作，显示了中央最高层对网络安全的认识达到前所未有的

① 《微软宣布 50 天后 XP 停止服务 360 宣布继续保护 XP》，新华网，2014 年 2 月 17 日，http://news.xinhuanet.com/fortune/2014-02/17/c_126147099.htm。

② 《习近平：把我国从网络大国建设成为网络强国》，新华网，2014 年 2 月 27 日，http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm。

水平，也必将对未来我国的网络安全形势带来不可估量的重大意义。三是美国政府宣布将有条件移交根服务器管理权，将其置于一个新的国际性组织的管辖之下，而非美国政府的商业合同管理之下[①]。

接下来，本文通过梳理2013-2014年度重大网络空间安全事件，分析网络安全形势的变化特征与演变趋势，把握网络安全态势的走向，同时从公共政策的角度给出应对当前网络安全形势的建议对策，并为建设网络强国做一些有意义的探讨。

（二）全球互联网——2013年开启“后美国时代”

1. 曼迪昂特报告鼓吹“中国黑客威胁论”

2013年，炒作“中国黑客威胁论”的声音仍不时出现，其中影响最大的是2月的曼迪昂特（Mandiant）报告。

2013年2月19日，多家西方媒体引述美国网络安全公司曼迪昂特拟于美国时间周二发表的一份60页的报告，称近年美国遭受的网络黑客攻击多与中国军方有关。《纽约时报》2月19日援引报告摘要称，该公司历时6年，追踪141家遭受攻击的企业的数字线索，证实实施攻击的黑客组织隶属“总部设于上海浦东一栋12层建筑内的中国人民解放军61398部队”。中国官方表示，仅凭IP地址的通联关系就得出攻击源来自中国的结论，难以让人信服。中国外交部和国防部在回应这个报告时都使用了3个字——不专业。2013年3月，美国国家安全局（NSA）局长、网络部队司令部司令基思·亚历山大向国会坦承正在建设网络战部队，包括13支进攻性部队和27支防御性部队。

2. 斯诺登事件让全球反思互联网安全

2013年6月6日，英国《卫报》与美国《华盛顿邮报》几乎同时报道了美国情报部门的“棱镜门”等系统监控项目，引起了全球各界的巨大震动和广泛关切。美国中情局（CIA）前职员爱德华·斯诺顿披露给媒体两份绝密资料。一份资料称美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必

① 《沈逸：说美国放弃互联网管理权，还太早》，环球网，2014年3月17日，http://opinion.huanqiu.com/opinion_world/2014-03/4907511.html。

须每天上交数百万用户的通话记录。另一份资料更加惊人——美国国家安全局和联邦调查局通过进入微软、谷歌、苹果等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录等秘密资料。此后，斯诺登现身香港，声称自己良心感悟，无法允许美国政府利用“棱镜”项目侵犯全球民众的隐私及互联网自由。他表示，美国政府早在数年前就入侵中国的一些个人和机构的计算机网络，其中包括政府官员、商界人士甚至学校。斯诺登后来前往俄罗斯申请避难，获得了俄罗斯政府的批准。

斯诺登事件堪称网络时代第一场震惊全球的大洗礼，开启了全球网络战的新纪元！这个事件的后续影响，如同核冲击波，将异常深远。下面简单分析一下该事件对 6 个层面的影响。

第一，对美国形象的冲击。斯诺登事件最直接的影响就是使美国走下“神坛”。作为互联网的发源地和互联网发展的主要驱动力，美国几十年来一直掌控着互联网的绝对主导权，一直占据着互联网精神的道义高地，把控着互联网问题的话语权，也一直标榜是最安全可靠的守卫者和互联网精神的守护者，担当着网络空间事实上的“世界警察”。本次事件一棒子将一直神圣化的美国打回了原形。事实再次表明，任何垄断力量，如果缺乏有效的制衡与监督，都可能被滥用。美国以安全名义构建全球 360 度监控体系，无限制地延伸自己的监控边界，“棱镜”项目耗资 20 亿美元，可存储全球的通信数据，大大超越了合理的范畴，这无疑是极大的滥用。因此，人们对于美国管理互联网的信任一夜间坍塌，其中就包括美国最紧密的盟友。

第二，对美国互联网控制权的实质冲击。美国是全球互联网事实上的独家管理者。由于历史原因、制度因素及创新能力和国家实力等因素，全球互联网的管理权一直以 NGO 的名义游离在联合国、国际电联等国际组织之外，实际上依然掌控在美国政府手中，形成了美国独一无二的互联网控制权。斯诺登事件之后，各国对网络安全的重视程度必将急剧加大，一向力挺美国的欧洲盟友也将不再放心。在这种情况下，美国将不得不让渡更多的权力给更具代表性的国际组织，全球互联网的制度与规则制定将更加全球化——虽然步伐不可能很快。

第三，对全球网民的影响。“棱镜门”及后续不断披露的信息显示，美国不但严密监视着本国人民，更不辞“辛劳”地监视着美国之外的全球网民。作为一个

网民，安全感顿失！这是一次网民隐私意识的全球大启蒙。网络世界再也不是纯粹和美好的童话世界，而是充满了风险和危险，网络隐私边界问题的重要性将进一步凸显。斯诺登事件最坏的影响大概就是：在“斯诺登效应”下，很可能不会减少世界各国政府对网民的监控，反而会大大增加——既然以自由、民主著称的美国都如此肆无忌惮，还有哪个国家不争先恐后？这大概是斯诺登本人和大家最不愿意看到的结果。本次事件进一步生动地告诉我们每一个人：网络有风险，上网需谨慎！

第四，对全球网络空间安全问题的影响。斯诺登事件不但是对网民安全意识的一次启蒙，更是对全球网络空间安全意识的启蒙，是一次全球性的安全大警示，很可能由此在全球范围内掀起网络安全的军备竞赛，加大预算投入。因为，随着网络时代的全面到来，各国社会、经济、文化、生活等层面都越来越依赖互联网，网络安全逐渐成为国家安全最突出的挑战，各国首先需要“强身健体”，需要在自身安全防御方面快速“补课”。同时，有实力的国家面对美国霸权也不会放弃保留一定的进攻能力。这种军备竞赛估计将成为未来长期的主旋律。

第五，对美国高科技产业和企业的影响。从 Facebook 和微软披露的信息看，2012 年下半年，美国政府就向这两家公司分别提出 10000 多次和 7000 次索取用户资料的要求，平均每天 50 次之多。频度之高，令人咂舌，也令人不寒而栗。美国高科技企业是美国掌控全球互联网的重要环节。一直以纯粹的市场形象昭示自己的美国企业，在美国国家安全的进攻型战略思想下，难逃干系。斯诺登披露，美国国安局全球范围内的网络攻击行动超过 6.1 万项，针对中国内地及香港地区的此类行动数以百计，主要攻击网络中枢，这样可以接触以 10 万计的计算机的通信数据，而不必入侵每一台计算机。这些措施主要通过思科路由器完成。骨干网思科路由器，数亿台使用 Windows 操作系统、英特尔 CPU 的计算机，数亿台使用 Android 操作系统的手机，以及 iPhone、IBM 大型机等，覆盖全产业链和整个生态。如果它们不得不受命于美国政府，那么，其他国家如何能对这些企业及其产品放心？今后又怎能不加强戒备和安全措施？今后谁还敢对美国的跨国公司继续保持高度的信任？

最后，也可能是最富有意味的影响，就是对未来网络空间中美博弈的影响。斯诺登藏身香港，绝对不是偶然，而是堪称天才式的智慧选择。其现实影响、内

在意义与长远影响，都堪称神来之笔。中美围绕网络安全问题的争端已经持续很久，之前一直是中国处于非常被动的局面，也就是说，第一回合美国在舆论战上得了不少分数。而斯诺登事件使中国在第二回合的较量中迅速扭转了形势，一下子扳回了不少分数。但是，这两个回合，都仅仅是序幕而已，双方的博弈将是长期持久的。毕竟，这是两种模式、两种价值观、两种道路的竞争与较量。只要未来能够取长补短，形成良性竞争，那就是互联网发展的最大福音。

斯诺登事件的深远影响如何评价都不为过，更多潜在的影响还将继续发酵。这一事件将大大改变全球互联网的格局和进程，尤其是互联网规则的制定与博弈。当然，我们也必须清醒地认识到，作为全球互联网的中心，10 年之内，美国在互联网领域的绝对主导权——无论是技术、产业、文化，还是国家实力——依然无人可以抗衡，无法真正动摇。斯诺登事件使中美在网络安全领域的实力真实地呈现在整个世界面前。

3．网络空间中美两强博弈拉开序幕

网络空间中美两强格局是互联网在美国发展 45 年和在中国发展 20 年最直观的产出。尽管美国在互联网基础资源和技术实力、产业实力上拥有不可比拟的优势，但当前中国网民的数量已经远远超过美国，并成为网民数量第一大国。据世界银行统计数据显示：2012 年，全球网民数量为 25.1 亿；中国网民规模超过全球网民的 20%，达到 5.7 亿；美国为 2.5 亿，在全球网民中仅占 2.5%。此外，中国的网民数量不仅在绝对值上远超美国，增长速度也让美国无法企及。中国网民规模在 2000 年仅有 2000 多万，经过 12 年的发展迅速增长到 2012 年的 5 亿多，增长了 25 倍。美国网民在 2000 年已达 1.2 亿，但是经过 12 年的发展，网民规模仅增长了 2 倍多，与中国 25 倍之多的增长速度相比可见一斑（如图 1-1 所示）。可以说，美国掌握的是互联网势能，而中国拥有的更多是动能。长期来看，未来中美在网络空间下的两强博弈格局将持续存在。

在全球背景下看中国的网络安全现状，既不像 2013 年上半年美国政府主导的舆论战那样，貌似中国已经有足够的实力可以采取积极主动的进攻战略，也不像业界人士哀叹的那样毫不设防，一无是处，无所适从。冷静审视中美实力差距，分析发展趋势，未来 5 至 10 年，中国完全可以立足现实，规划积极有效的网络空

间安全防御型战略，逐渐扭转战略上的被动局面，掌握主动权和主导权。

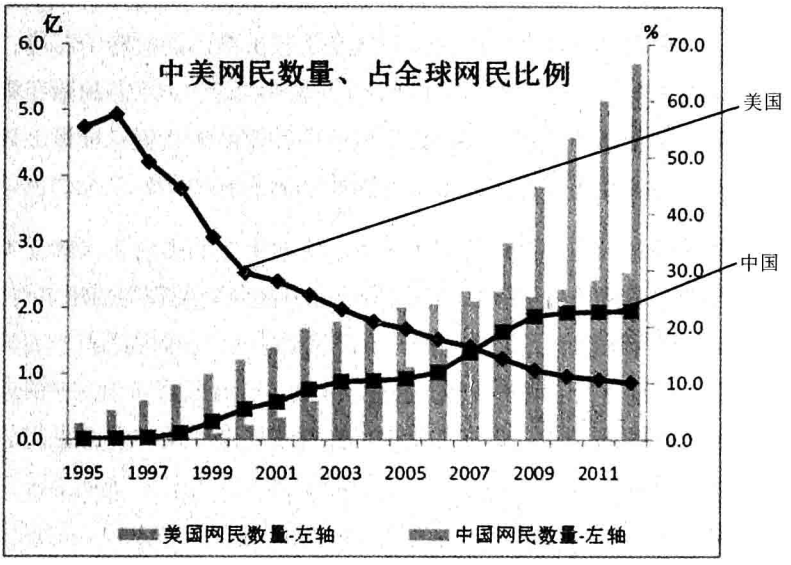

图 1-1　中美网民情况对比

网络空间安全已经成为中美外交的核心要素，也将成为未来国家经济、政治、军事的核心，甚至是最大的引爆点。美国充分利用了网络安全问题的复杂性及规则的模糊性，占据了舆论的主导权和主动权。与现实世界的“三个世界”划分类似，互联网上也可以划分为“三个世界”。现实世界是以经济发展程度来划分的，而网络世界略有不同，是以网络上的主导权来划分的，分为网络殖民国家、网络主权国家和网络霸权国家。从互联网基础设施、互联网产业竞争力和网络战实力 3 个角度上看：全球只有美国一马当先，是唯一具备网络霸权的国家；中国、俄罗斯、印度、日本、澳大利亚、韩国，以及英国、德国等欧洲国家，可以掌握自己网络的主导权，形成了一批网络主权国家；而相当一部分国家，受制于经济实力和发展状况，不具备足够的互联网力量和竞争力，只能成为互联网上受制于人的网络殖民国家。

随着网络空间的重要性不断上升，社会、经济、生活等活动的重心逐步转移到互联网上，各国家开始重视网络空间战略。全球网络空间战略可以分为两种：一种是进攻型战略，另一种是防御性战略。战略源自基础和实力，网络空间战略