

网络空间治理的力量博弈、 理念演变与中国战略*

鲁传颖

【内容提要】 全球网络空间治理进程不仅涉及信息发达国家与信息发展中国家在互联网关键资源、网络权力和网络安全等领域的复杂博弈，还包括政府、私营部门和市民社会等行为体之间的相互博弈。“棱镜门事件”在加剧网络空间治理博弈的同时，也推动各方政策立场持续调整，增加了治理合作的可能性。与此同时，网络空间领域的博弈也反映出互联网治理与网络空间治理等相关治理理念的相互冲突与相互融合趋势。目前，中国在全球网络空间治理上的参与仍面临诸多挑战。中国需要以网络空间博弈的发展趋势和治理理念的演进为基础，结合“十三五”规划提出的网络强国战略，以国际机制塑造、人才培养及技术发展等为核心建构长远、完备和全面的参与战略。

【关键词】 互联网治理 网络空间治理 多方博弈 网络强国战略

【作者简介】 鲁传颖，华东师范大学国际关系与地区发展研究院博士研究生，上海国际问题研究院全球治理研究所助理研究员

【中图分类号】 D815

【文献标识码】 A

【文章编号】 1006-1568-(2016)01-0117-18

【DOI 编号】 10.13851/j.cnki.gjzw.201601007

* 本文系国家社科基金青年项目“‘棱镜门’与中国参与国际互联网治理战略研究”（15CGJ001）的阶段性成果。感谢《国际展望》匿名评审专家和编辑部老师提出的建设性修改意见，文中疏漏由笔者负责。

2013年6月,美国国家安全局(NSA)前雇员爱德华·斯诺登披露了该局的“棱镜”监听项目。该事件^①使网络空间治理在国际议程中的优先次序再度提升,但也加剧了各方立场的分化,导致网络空间治理陷入困境,为网络空间治理的建章立制带来极大挑战。另外,国际社会对网络空间及其治理的复杂性缺乏清晰、统一的认知,由此而造成的片面立场和单一政策进一步加剧了治理困境。面对上述复杂情势,约瑟夫·奈(Joseph Nye)试图通过借鉴环境治理领域的机制复合体理论来解释网络空间治理的实践,通过多个不同的治理机制组成的松散耦合复合体来分析网络空间治理。^②这为分析网络空间治理形势提供了一个有益的视角,即网络空间治理是由多个而非单一的治理机制组成,各种机制之间的相互作用对治理产生影响。本文拟从更加宏观的视角来审视网络空间治理发展的进程,并试图探索网络空间博弈背后的理念演变,同时分析政府、私营部门、公民社会等治理行为体在国际、国内两个层面的复杂关系。在此基础上,探讨中国的应对措施和参与网络空间治理的战略。

一、网络空间治理的力量博弈

网络空间治理的进程伴随着各国政府之间的博弈过程。根据各国政府在网络技术、网络能力和网络使用度等方面的情况,可以将其划分为信息发达国家、信息发展中国家和信息不发达国家三类。^③也有国际组织以网络就绪度(Readiness)为指标衡量各国的信息化程度。这种排名基本上与传统的发达、发展中以及不发达国家的三分法相重叠,当然也存在个别发展中国家的信息化水平上升到发达国家行列,或部分发展中国家的信息化水平跌落到不发达国家的水平。因此,按照信息发达国家、发展中国家和不发达国家的三分法来划分在学术上更加精确。网络空间治理的力量博弈主要有三个方面:

^① 该事件一开始被称作“斯诺登事件”,后来逐渐改为“棱镜门事件”。为便于叙述,本文统一称之为“棱镜门事件”。

^② Joseph Nye, “The Regime Complex for Managing Global Cyber Activities,” *Global Commission on Internet Governance Paper Series*, No. 1, 2014, pp. 5-13.

^③ 杨剑:《数字边疆的权利与财富》,上海人民出版社2012年版,第158-159页。

一是信息发达国家与信息发展中国家在网络权归属、网络资源分配方面的博弈；二是非政府行为体与政府之间就互联网关键资源控制、网络安全与自由等问题的博弈；三是作为网络空间中的主导国家，美国政府联合其境内的私营部门、市民社会与其他国家之间在互联网关键资源归属等问题上的博弈（图 1）。

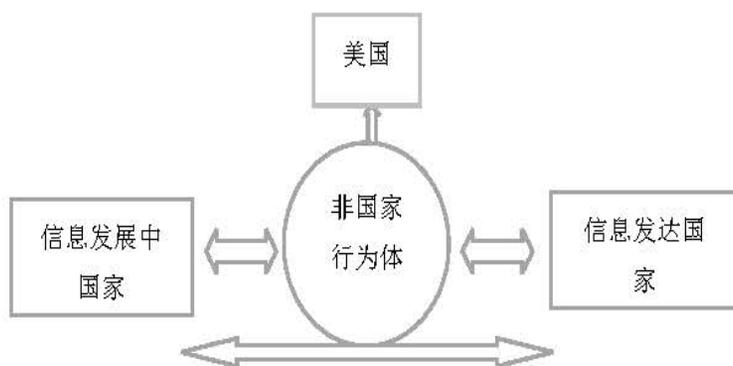


图 1：网络空间博弈的基本态势

资料来源：作者自制。

首先，信息发达国家与信息发展中国家围绕着网络空间的关键基础设施和网络技术之间的博弈。根据网络空间治理领域力量博弈的行为体、议题和特点，可以将其划分为三个阶段。

第一阶段是早期的互联网治理时期，这大致从国际互联网的形初期到联合国召开信息社会世界峰会（World Summit on Information Society, WSIS）为止；该峰会分为 2003 年日内瓦会议和 2005 年突尼斯议程两个阶段。信息社会世界峰会表面上表现为各国政府与私营部门和市民社会之间的斗争，实质上则是美国与其他国家就互联网控制权而展开的博弈。

这一时期是互联网快速发展的阶段，大量新的技术及技术标准被创造出来，美国政府借机大力推动信息技术发展，并制定了一系列国际技术标准、行业和产业规范。而信息发展中国家还处于学习、借鉴阶段，这使美国等发

达国家在该领域处于绝对强势地位。^① 这一阶段的互联网治理主要围绕互联网域名注册与解析及其相应的 13 台根服务器控制权、互联网协议 (IP) 地址分配等关键资源展开争夺。美国几乎控制了互联网标准制定和管理的所有国际组织和核心企业,并拒绝将相关管理职能国际化或交由联合国专门机构管理。^② 因此,在信息社会世界峰会上,尽管面临来自联合国、信息发展中国家甚至欧洲国家的压力,美国依然拒绝交出国际互联网管理权。进入 21 世纪后,以中国为代表的信息发展中国家的网络科技力量不断提升,它们所拥有的域名、用户等互联网资源已经超过了信息发达国家,但在互联网治理中的代表性远远不足,因此对现有互联网治理体现的合法性提出了质疑。

第二阶段是网络空间治理的政治竞争和主权竞争阶段,有人称之为政府在网络空间的“回归”阶段。这一阶段从信息社会世界峰会到 2011 年。2011 年,中国、俄罗斯等国向第 66 届联大提交了“信息安全国际行为准则”,主张联合国在网络空间治理中发挥主导作用。同年,美英等国政府主导的全球网络空间治理大会(Global Cyberspace Conference),又称伦敦进程(London Process)正式召开。

这一阶段网络空间治理博弈的特点是,随着网络技术的不断突破及其对现实社会的颠覆性变革,网络空间已经成为人类社会的“第五战略空间”。围绕网络空间中秩序、权力与财富的分配,信息发达国家与信息发展中国家在下列问题上产生了严重分歧:网络空间属性是“全球公域”还是“主权领域”;治理手段是政府主导的“多边治理”,还是非政府行为体主导的多利益攸关方(Multi-stakeholder)模式;治理文化是西方主导的“一元文化”,还是平等协商的“多元文化”。^③ 这一时期的矛盾焦点还集中体现在信息内容的自由流通领域,希拉里·克林顿就任美国国务卿时,针对互联网自由发表了多次讲话,鼓吹美国的互联网自由战略。在始于 2010 年年底的西亚北非动荡之中,美国政府与社交媒体网站在背后所扮演的角色引起了信息发展

^① 杨剑:《数字边疆的权利与财富》,第 213-221 页。

^② 沈逸:《全球网络空间治理原则之争与中国的战略选择》,载《外交评论》2015 年第 2 期,第 66-70 页。

^③ 鲁传颖:《试析当前网络空间全球治理困境》,载《现代国际关系》2013 年第 9 期,第 44-47 页。

中国家的广泛关注，并加强了对互联网的管理。^①

第三阶段从“棱镜门事件”之后一直到现在，这一阶段的竞争更加聚焦网络空间的安全治理。“棱镜门事件”使美国在网络空间治理领域的道德制高点遭受质疑、领导力下降，迫使其在推动网络空间治理中放低姿态。与此同时，网络空间安全形势进一步恶化，各国面临的安全威胁进一步加大。在经历了“棱镜门事件”初期的激烈对抗之后，信息发达国家与信息发展中国家均意识到维护网络空间的安全需要各国的共同参与，没有任何国家可以单独主导网络空间治理进程。信息发达国家与信息发展中国家在认知层面的差距逐渐缩小，对抗性举措减少，合作的空间开始增长。

其次，“棱镜门事件”引起了政府与私营部门、市民社会之间在网络安全、公民隐私等问题上的激烈博弈。美国国家安全局前雇员爱德华·斯诺登揭露了一个包括“棱镜”、“X 关键分”（X-Keyscore）、“美景”（Fairview）、“核心”（Main core）等近 10 个监控项目在内的监控体系，该监控体系由国家安全局、中央情报局、联邦调查局等多个情报机构参与，几乎覆盖了网络空间的社交网络、邮件、即时通讯、网页、影片、照片等所有信息。^② 国家安全局要求微软、谷歌、脸谱等 9 家主要全球互联网企业向监控项目开放数据库以便开展数据监控。在“棱镜门事件”曝光后，微软、谷歌、脸谱等企业向法院公开起诉联邦政府。^③ 市民社会也纷纷行动起来，反对大规模数据监控。美国市民社会联盟在网上发起“停止监视我们”（Stop Watch Us）的行动，向美国政府施加压力，得到数万网民在网站上的签名、留言及数百个公民团体的响应，他们通过组织游行示威、向国会请愿、发起网络倡议等方式配合该行动。^④

在“棱镜门事件”引发了其他国家对与美国政府合作开展监控项目 ICT

^① “Secretary Clinton’s Remarks on Internet Freedom,” *IIP Digital*, December 8, 2011, <http://iipdigital.usembassy.gov/st/english/texttrans/2011/12/20111209083136su0.3596874.html#axzz2eIWPYNRu>.

^② “NSA’s Prism Surveillance Program: How it Works and What it Can Do,” *The Guardian*, June 9, 2013, www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

^③ “Obama Weighing Security and Privacy in Deciding on Spy Program Limits,” *The New York Times*, December 20, 2013.

^④ See “Stop Watching Us” Website, <https://optin.stopwatching.us/>.

企业的不满，各国纷纷采取新的措施保障网络空间安全。例如，中国政府加快了网络空间的法制化进程，并开始讨论网络安全设备自主可控的指导思想、制定了网络安全审查办法，在先后出台的《国家安全法》、《反恐怖主义法》、《网络安全法（草案）》和《刑法修正案（九）》中都大幅增加了涉及网络安全的条款。这些举措引起了美国信息通信技术企业的严重关切，并游说美国政府对华施压，要求中国政府取消相关规定，如《反恐怖主义法》第十八条中规定“电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密技术支持和协助”。^① 尽管从政府角度看，这些举措有助于维护网络安全和国家安全，但在私营部门看来，上述规定的举措不仅将增加技术上的投入，也会大幅度增加成本。只要网络空间治理未实现突破，政府与私营部门、市民社会之间的博弈会继续存在，并在一定程度上将演变为国家间博弈。

最后，美国政府与其境内的私营部门、市民社会之间结盟与其他国家在互联网关键资源归属问题上的博弈。互联网关键资源包括：IP 地址分配、协议参数注册、通用顶级域名（gTLD）系统管理，国家和地区顶级域名（ccTLD）系统的管理及根服务器系统的管理和时区数据库管理等。有学者形象地用掌握网络空间中的“封疆权”来形容互联网名称与数字地址分配机构（Internet Corporation for Assigned Names and Numbers, ICANN）在网络空间治理中的地位。^②

由于历史的原因，这些资源一直由美国国家通信与信息管理局（National Telecommunication and Information Administration, NTIA）下属的互联网数字分配机构（Internet Assigned Numbers Authority, IANA）负责管理，NTIA 通过定期与 ICANN 签订合同，授权其管理 IANA 的职能。因此，可以认为美国政府控制着互联网的关键资源。联合国任命的互联网治理工作组（WGIG）在报告中指出，美国政府单方面控制着如根区文件在内的互联网关键资源。^③

^① 《中华人民共和国反恐怖主义法》，中国人大网，2015年12月28日，http://www.npc.gov.cn/npc/xinwen/2015-12/28/content_1957401.htm。

^② 杨剑：《数字边疆的权利与财富》，第213-221页。

^③ WGIG, *Report of the Working Group on Internet Governance*, Château de Bossey: WGIG, 2005, <http://www.wgig.org/docs/WGIGREPORT.pdf>.

国际社会对这种情况一直不满，WGIG 报告中提出了四种方案以取代既有架构，希望通过政府间组织或全球性机构来接管互联网关键资源。^① 对于 ICANN 来说，虽然一直寻求独立于美国政府之外并与之开展了多次争夺，但它更关注的是如何避免其他政府间组织或机构接管或取代其地位。弥尔顿·穆勒将这种现象描述为“一些网络自由主义者甚而最终转变成了国家主义的秘密支持者，因为只要被挑战的国家是他们的祖国，他们就转而为美国辩护，允许其控制、主导互联网。”^②

因此，在一些情况下，ICANN 选择与美国政府“结盟”共同阻止其他国家或政府间组织影响其治理结构。在 ICANN 的组织架构和决策体制中，各国政府代表所在的政府咨询委员会（Government Advisory Committee, GAC）只有资格提名一名不具有表决权的联络员。信息发展中国家认为，作为一种互联网治理的国际机制，在 ICANN 中来自信息发展中国家的代表性不足，在其未来的管理架构中，应当体现政府的职责和权力，增加政府咨询委员会的权限。但 ICANN 多次表示不会接受这种改变。对于这种情况，无论是在政府咨询委员会中，还是在 ICANN 的全体会议上，美国政府代表与 ICANN 的官方立场高度一致。直到“棱镜门事件”爆发，美国政府才迫于多方面压力宣布重启 ICANN 的国际化进程，这将网络空间治理博弈导向了新的阶段。

二、网络空间治理未来的发展态势

随着网络空间治理进程的推进，各方对网络空间属性的认知逐渐达成共识，并由此使其在治理方法、路径上的分歧缩小。特别是在认知层面，各国对网络空间的认知由基于不同的政治、经济、文化背景，强调各自的独特性转向基于网络空间的客观属性和规律，强调不同观点之间的融合。^③ 网络空

^① Ibid.

^② [美]弥尔顿·L.穆勒：《网络与国家：互联网治理的全球政治学》，周程等译、王骏等校，上海交通大学出版社 2015 年版，第 4 页。

^③ 王明国：《全球互联网治理的模式变迁、制度逻辑与重构路径》，第 69-70 页。

间的互联、共享属性决定了零和博弈不适用于网络空间，网络空间的安全、发展、自由是政府、私营部门和市民社会所追求的共同目标。同时，安全、发展、自由这三个议题的相互制约关系，使得任何一方都不能忽视其他行为体的利益，而追求自身的绝对利益。正如习近平主席 2015 年 12 月 16 日在第二届世界互联网大会（World Internet Conference, WIC）开幕式的主题演讲中指出：“在信息领域没有双重标准，各国都有权维护自己的信息安全，不能一个国家安全而其他国家不安全，一部分国家安全而另一部分国家不安全，更不能牺牲别国安全谋求自身所谓绝对安全”。^① 这一立场反映了网络空间治理的上述特殊属性。由此，国际社会也逐步意识到，没有任何一方可以主导网络空间治理进程。

首先，美国的网络空间战略调整与 ICANN 国际化进程将推动网络空间治理架构的重大转型。面临重重压力，美国通过部分放弃互联网关键资源的直接控制权，为其网络空间国际战略的调整做准备。^② 2014 年 3 月 14 日，美国商务部下属的 NTIA 宣布将放弃对 ICANN 的控制，并在移交声明中指出，将由 ICANN 管理层组织全球多利益攸关方讨论接收问题，但明确拒绝由联合国或其他政府间组织接管。^③ ICANN 自成立以来一直在寻求自己的独立地位，ICANN 国际化的目标不仅是要摆脱美国政府的制约，同时还要确保在美国政府放权后，不会被其他国家和政府间组织接管。因此，ICANN 既需要与美国政府达成协议以保证自己的独立性，也要与其他国家政府展开博弈，避免其国际化遭到强烈反对。

其次，联合国在网络空间治理中的作用持续提升，将有力地推动网络空间治理架构和规范的建设步伐。通过联合国信息安全政府专家组（GGE）的努力，国际社会在网络空间的行为规范和建立信任措施等方面也取得了重要突破。2013 年 6 月，联合国发表了一份由 15 个国家的代表组成的专家组的

^① 《习近平出席第二届世界互联网大会开幕式并发表主旨演讲》，中央网信办，2015 年 12 月 16 日，http://www.cac.gov.cn/2015-12/16/c_1117480642.htm。

^② 沈逸：《全球网络空间治理原则之争与中国的战略选择》，第 65-66 页。

^③ “NTIA Announces Intent to Transition Key Internet Domain Name Functions,” *The NTIA*, March 14, 2014, <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

报告。报告首次明确了“国家主权和源自主权的国际规范及原则适用于国家进行的通信技术活动，以及国家在其领土内对通信技术基础设施的管辖权。”同时，报告进一步认可了“联合国宪章在网络空间中的适用性”。^①“各国在努力处理通信技术安全问题的同时，必须尊重《世界人权宣言》和其他国际文书所载的人权和基本自由。”^②与 2010 年的专家组报告相比，上述内容分别作为 2013 年报告的第 20 和 21 条款出现，这是一个巨大的进步，表明信息发达国家和信息发展中国家在网络空间治理认知理念的兼容性不断提高。2015 年 7 月，联合国关于从国际安全的角度看信息和电信领域的发展政府专家组公布了第三份关于网络空间国家行为准则的报告。这份报告在保护网络空间关键基础设施、建立信任措施、国际合作等领域达成了原则性共识。信息发展中国家关心的网络主权进一步得到明确，信息发达国家主张的国际法特别是武装冲突法在网络空间中的适用也写入其中。^③

最后，政府与非国家行为体在网络空间治理中的竞争与合作模式将发生重大转变，多层次博弈将成为网络空间治理的“新常态”。在治理方式和路径方面，各国在网络空间治理中的政策立场也更强调从实际出发，特别是在处理政府与其他行为体的关系上。各方都意识到应当根据网络空间治理中的问题来划分政府与其他行为体的职责。对于多利益攸关方治理模式，信息发达国家与信息发展中国家的认知逐步统一，政府与私营部门、市民社会根据各自的职能参与网络空间治理。认知缩小意味着一方对另一方的关切更加了解，信息发达国家与信息发展中国家在网络空间治理中的博弈将更具针对性，表现为竞争与合作同步进行，以竞争促进合作。当然，这与信息发展中国家加大了对网络空间建章立制的投入，在网络空间治理的话语权上的增长有关。巴西、中国先后建立了网络空间多利益攸关方会议（NetMundial）和世界互联网大会机制，探讨网络与国家安全、网络主权等核心问题，信息发

^① *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN General Assembly Document A/68/98, June 24, 2013.

^② *Ibid.*

^③ *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN General Assembly Document A/70/174, July 22, 2015.

展中国的声音将越来越多、越来越大。

三、网络空间治理的理念演变

在信息发达国家与信息发展中国家，政府、私营部门和市民社会等围绕网络空间治理的博弈从冲突转向融合的背后，反映了网络空间治理理念的持续演变。尽管围绕网络空间治理的博弈主要是为了争夺网络空间的权力与财富，但行为体对治理的主体、客体和方法的不同认知对治理的冲突与融合产生了重要影响。微软首席研究及战略官克雷格·蒙迪（Craig Mundie）在第七届中美互联网论坛上就曾指出，“中美双方在网络空间的误解很大程度上是由于对‘互联网治理’和‘网络空间治理’两个概念的混淆所导致”。^① 同样，网络空间治理博弈和冲突也反映了上述两种治理概念之间的冲突。

互联网治理被认为属于一种由非政府行为体主导的多利益攸关方治理模式，但网络空间治理也需要政府和政府间组织的参与和协调。互联网治理项目（Internet Governance Project, IGP）将互联网治理定义为“所有者、运营商、开发者和用户共同参与的一个由互联网协议所联接起来的与网络相关的决策，包括确立政策、规则和技术标准的争端解决机制，制定资源分配和全球互联网中人类行为的标准。”^② 上述定义包括三个方面，即技术标准和协议的接受和认可，域名和 IP 地址等互联网资源的分配，人类的互联网行为产生的垃圾邮件、网络犯罪、版权和商标争议、消费者保护问题、公共部门和私人的安全问题等相关的规定、规则和政策等。劳拉·迪娜尼斯（Laura DeNardis）提出要按照互联网传输的 TCP/IP 协议的层级，并根据不同层级的不同功能构建互联网模式，依据功能、任务和行为体分别讨论互联网资源控制、标准设定、网络接入、网络安全治理、信息流动、知识产权保护等六个层面的互联网治理内容。^③

^① 克雷格·蒙迪于 2014 年 12 月 4 日在华盛顿召开的“第七届中美互联网论坛”上发言。

^② Mathiason J., “A Framework Convention: An Institutional Option for Internet Governance,” Internet Governance Project, December 20, 2004, <http://internetgovernance.org/pdf/igp-fc.pdf>.

^③ Laura DeNardis and Mark Raymond, “Thinking Clearly about Multistakeholder Internet Governance,” Paper Presented at Eighth Annual GigaNet Symposium, November 14, 2013, pp. 1-2,

网络空间治理从原先互联网治理所强调的专业性、技术性领域转向更广泛的政治、安全和经济范畴，政府和政府间组织在网络空间治理中的重要性也日益凸显。网络空间是一个更广泛的领域，它不仅包括互联网，还包括网络中传输的数据，网络的用户以及现实社会与虚拟社会的交互等。相对应的网络空间治理则是一个更加宽泛的概念，它是“包括网络空间基础设施、标准、法律、社会文化、经济、发展等多方面内容的一个范畴”。^① 它所包含的治理议题更加多元，面临的挑战也在不断增加。如“棱镜门事件”引发的对大规模数据监控的关注、政府在网络空间开展的网络行动导致的高持续性威胁（APT）、全球范围内的数字鸿沟（Digital Divide）与数据贫困（Data Poverty）、网络恐怖主义、网络商业窃密等越来越多的治理议题已经超越了传统的互联网治理理念的范畴。

网络空间治理博弈中涉及的“全球公域”与“网络主权”、“网络自治”与“国家主导”等冲突反映出人们未能客观、正确地理解“互联网治理”与“网络空间治理”之间不同的治理主体、客体和方法，试图用单一的治理方法去解决其中的多元议题。以 ICANN 为代表的互联网治理主体所推崇的自下而上、公开透明的治理模式，对于国家在应对网络战、大规模数据监控、窃密等高可持续性威胁、网络恐怖主义等问题而言，缺乏有效性和针对性。与此同时，以国家为中心、自上而下的网络空间治理理念也无法有效应对当前国际互联网治理的现实问题，不能取代互联网国际组织在该领域的主导地位。

随着网络空间治理进程的推进，上述两种治理理念和方法在碰撞中也开始不断融合。约瑟夫·奈认为，网络空间是由多个治理机制组成，其中互联网治理聚焦于技术层面，是网络空间治理的一个子集。应当根据不同的治理议题，构建不同的治理机制，让不同的行为体来发挥主导作用。^② 治理观念的融合还表现在各方对多利益攸关方治理模式共识的增加。ICANN 采用的是一种自下而上、基于共识基础的决策过程，并主张限制政府作用的治理模

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377.

^① Panayotis A. Yannakogeorgos, “Internet Governance and National Security,” *International Strategic Studies Quarterly*, Vol. 6, No. 3, 2012, p. 103.

^② Joseph Nye, “The Regime Complex for Managing Global Cyber Activities,” pp. 5-13.

式。^① 很多信息发展中国家最初对多利益攸关方治理模式持反对态度，强调应当采用政府主导的多边治理模式。随着治理进程的深入，信息发展中国家逐步接受多利益攸关方治理模式，只要政府的作用得到合理体现，这种观点也在私营部门和市民社会代表中获得越来越多的共识。政府、私营部门和市民社会根据各自的功能与责任来参与决策过程，不刻意将其他行为体排除在外，也不刻意追求个别行为体的领导权，体现出更加客观和平衡的网络空间治理理念。

四、中国的战略应对

中国政府提出了网络空间全球治理的两大目标，即共同构建和平、安全、开放、合作的网络空间和建立多边、民主、透明的国际互联网治理体系，同时还将网络强国战略作为重要战略目标纳入“十三五”规划建议中。前者主张对外参与国际网络空间治理进程，以此来建立有利的国际治理体系；后者主张发展网络技术力量，培育网络产业，增强国家网络实力。两者之间的相互支持和相互促进需要有一个能够统筹内外、应对复杂网络空间形势的国际战略。尽管中国政府并未公布具体的网络空间国际战略文件，但通过分析现有的相关政策，仍可以发现中国的网络空间国际战略还处于摸索阶段。因此，有必要对照网络空间力量博弈的特点和网络强国战略来分析和探讨中国的网络空间国际战略。

（一）中国网络空间国际政策实践

自 1994 年接入国际互联网起，中国就制定了各种形式的网络国际政策融入国际网络空间体系。这一方面是扩大开放的需要，希望通过国际合作学习、引进国外先进的技术标准；另一方面是信息技术的驱动，融入全球化必须全方位参与国际体系。^② 此外，随着中国在国际事务中的影响力越来越

^① Miles Kahler, ed., *Networked Politics: Agency, Structure and Power*, Ithaca, New York: Cornell University Press, 2009, p. 34.

^② 杨洁勉：《新时期中国外交思想、战略和实践的探索创新》，载《国际问题研究》2015 年第 1 期，第 18 页。

大以及对网络的依存度上升,主动参与网络空间治理也是维护国家利益的重要路径和方式。中国的网络政策在很大程度上受到国际网络空间治理形势的影响,并在与国际网络空间治理制度的互动中得到发展和提升,呈现出多领域、多层次和多主体的特点。

第一,中国政府网络国际政策覆盖了国际技术标准合作、信息通信技术产业合作、全球互联网治理、打击网络犯罪、网络经济、数字鸿沟等多个领域,与全球网络治理的发展趋势总体上保持一致。首先,从早期的技术、产业和互联网标准的合作逐步拓展至更加广泛的网络相关政策合作,很多政策领域实际上已经超出了互联网本身的范畴,与国际经济、政治、安全相结合。其次,“棱镜门事件”之后,随着网络空间安全治理成为治理中的主要议题,中国网络政策的关注点也相应聚焦于网络安全治理,及建立在此基础上的国家安全、政治安全、经济安全和社会安全。中国不仅在国际上大力反对大规模网络监控,提倡维护国家网络主权,而且在国内政策上也更加注重与网络安全相关的立法工作,在实践中维护国家安全和主权。

第二,中国的网络空间国际政策覆盖了双边、地区、多边和国际等多个层级。从双边层面来看,中国与韩国、英国、澳大利亚等国家建立了政府间对话合作机制,这些合作不仅覆盖网络安全、数字经济和发展等内容,还成为双边外交关系的重要内容和支撑。此外,中美、中俄之间在网络安全领域开展了不同程度的建立信任措施(Confidence Building Measures, CBMs)。^①在地区层面,中国与东盟、上合组织、欧盟、阿盟等地区组织和国家之间建立了多种形式的网络对话合作机制。2009 年中国政府分别与东盟和上合组织成员国签订了《中国—东盟电信监管理事会关于网络安全问题的合作框架》和《上合组织成员国保障国际信息安全政府间合作协定》。^②中国还积极参与东盟地区论坛网络安全工作组的工作,并于 2013 年 9 月在北京召开了东盟地区论坛“加强网络安全措施研讨会——法律和文化视角”。会议倡

^① “FACT SHEET: President Xi Jinping’s State Visit to the United States,” White House, September 25, 2015, <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

^② 中华人民共和国国务院新闻办公室:《中国互联网状况》,人民出版社 2010 年版,第 1-16 页。

议互联网的发展需要法律规则的引领，也需要促进和尊重文化多样性，各方应在网络安全领域加强交流、增进互信、推进合作，共同构建和平、安全、开放、合作的网络空间。^① 最后，中国还积极参与多边和国际层面的网络空间治理机制，无论是联合国框架下的信息安全政府专家组、国际电信联盟、信息社会世界峰会、互联网治理论坛，还是联合国框架之外的伦敦进程、网络空间多利益攸关方会议等机制，中国都是主要参与者；此外，中国还通过召开世界互联网大会来开展网络空间的主场外交。中国还与俄罗斯、乌兹别克斯坦等上合组织成员国共同向联合国大会提交了两个版本的“信息安全国际行为准则”。^② 中国也是全球互联网治理联盟的主要参与方，国家互联网信息办公室（网信办）主任鲁炜和阿里巴巴集团董事局主席马云当选为该联盟的委员。

第三，随着网络空间治理所覆盖的内容越来越广泛，中国网络空间国际政策参与的主体也从传统的外交部、工信部进一步扩展到公安部、商务部、财政部以及新成立的网信办，外交部专门设立了“网络事务办公室”来应对网络空间的外交事务。其中，外交部主要负责双边、地区、多边和国际层面的网络外交工作，它还是中国对接联合国框架下网络治理机制的主要力量，特别是来自外交部军控司的官员全程参与四届联合国信息安全专家组的工作。网信办作为中央网络安全与信息化领导小组的常设机构，是中国为了统筹应对网络安全与信息化新设立的重要机构。网信办作为统筹、协调中国网络事务的机构在网络国际政策中的角色越来越重要，不仅开展了多层级的国际网络安全与数字经济合作，还建立了世界互联网大会治理机制。此外，公安部在打击网络安全犯罪、网络反恐，商务部在信息通信技术市场准入，财政部在网络基础设施对外援助等领域的工作都将是今后实施网络空间国际战略的坚实基础。

^① 《东盟地区论坛网络安全研讨会在京举行》，人民网，2013年9月12日，<http://media.people.com.cn/n/2013/0912/c40606-22893628.html>。

^② *International Code of Conduct for Information Security, Annex to the Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General*, UN General Assembly Document A/66/359/, September 14, 2011.

由此可见，中国已经形成了一个较为全面、深入的网络空间国际战略架构，包括多元的参与主体、宽领域的议题覆盖和多层级的参与路径，这为网络空间治理的国际战略构建奠定了良好基础。伴随着中国从网络大国向网络强国的发展，中国将会建立一个全面、完善的网络空间国际战略。

（二）网络空间国际战略面临的挑战

网络空间治理的力量博弈变化给中国的网络空间国际战略带来了多重挑战：一是信息发达国家将继续主导网络空间治理博弈的方向，这对中国的网络空间国际战略构成挑战；二是由于缺乏高级互联网治理人才，导致中国在互联网国际组织中的代表性严重不足；三是网络空间治理博弈转向强调能力建设（Capacity Building）、最佳实践（Best Practice）等方向，将给中国带来竞争压力。这些问题和挑战对中国网络空间国际战略将产生较大冲击，若处理不当，会对网络强国战略的实施造成负面影响。

第一，信息发达国家继续主导网络空间治理博弈方向对中国国际战略构成的挑战。网络空间全球治理是通过各种形式的治理机制发挥作用，机制的构建取决于各行为体之间的谈判，谈判的筹码不仅取决于各行为体的权力大小，还与各方在网络空间全球治理中的议程设置能力息息相关。^①按照约瑟夫·奈的定义，前者可称之为“硬权力”，后者是“软权力”。^②信息发达国家在这两个领域的优势明显，特别是在通过选择性或者优先设置议程左右网络空间治理的机制构建。比如在网络安全治理中，美国依靠其议程设置能力阻止国际社会将大规模数据监控列为治理议程，同时将其重点关切的网络经济窃密设置为优先议程。此外，信息发达国家在设置网络人权议程时，将重点置于自由领域，而民主（一国一票）、平等（大小国家拥有同等话语权）等同样重要的议题则被排除在议程之外。不仅如此，对于各国在“棱镜门事件”后要求加强行使网络主权的趋势，美国则提出“数据本地化”（Data Localization）这一议程以规避在全球治理机制中讨论网络主权。与信息发达

^① [美] 奥兰·扬：《世界事务中的治理》，陈玉刚、薄燕译，上海世纪出版集团 2007 年版，第 36 页。

^② [美] 约瑟夫·奈：《理解国际冲突：理论与历史》，张小明译，上海世纪出版集团 2009 年版，第 78 页。

国家相比，信息发展中国家在议程设置能力上还存在较大差距，缺乏主动设置议程的能力。近年来，随着中国、巴西、印度等国先后建立了各种网络空间治理机制，新兴大国在网络空间全球治理中的议程设置能力不断增强。但总体而言，中国与信息发达国家在治理能力方面的差距依旧存在，并将影响中国通过国际机制维护自身国家利益，以及表达自身关切。

第二，由于缺乏高级网络空间治理人才，导致中国在互联网国际组织中的代表性严重不足。网络空间治理博弈的趋势表明，ICANN、IETF 等国际组织对互联网关键资源的控制权不会受到政府和政府间组织的挑战。随着美国政府放弃对 ICANN 的控制权，后者将具有更大的独立性。网络空间建立在互联网基础之上，网络空间治理的基础也是互联网治理。因此，中国的网络空间国际战略必须要在互联网治理领域实现突破，同时提升在互联网国际组织中的影响力和代表性。对包括中国在内的广大信息发展中国家而言，必须增加在 ICANN 等国际组织中的代表性，让更多来自中国和其他发展中国家的声音出现在 ICANN 中。

第三，网络空间治理博弈转向强调能力建设、最佳实践等方向，这将给中国带来严峻的竞争压力。网络空间治理博弈理念的融合使得国际社会对网络空间治理的焦点转向了能力建设、最佳实践等可操作和可落实的领域，包括向信息发展中国家和信息不发达国家提供网络基础设施；提供与网络空间治理相关的技术、法律、政策等人才的培训；提供网络空间治理中遇到的解决各种具体问题的最佳实践。这对于中国参与网络空间治理的国际战略提出了更高的要求，信息发达国家在上述领域的资源优势、人才优势短期内难以撼动，这不仅需要中国政府投入更多资源，也需要中国的互联网企业、行业协会、法律专家的共同和积极参与。

（三）中国参与网络空间治理的战略思路

确立中国网络空间国际战略的基本路径与中国整体对外战略强调的融入国际体系，并推动改革国际体系的宏观目标相一致。^① 为应对复杂的网络空间治理博弈，中国一方面要加强能力建设，并注重将能力转化为参与网络

^① 杨洁勉：《新兴大国群体在国际体系转型中的战略选择》，载《世界经济与政治》2008年第6期，第6页。

空间全球治理的影响力；另一方面在网络安全与开放之间寻求平衡，通过参与国际网络空间建章立制来维护自己的合法权益，避免过度安全化带来的负面影响；并加强网络强国战略与网络空间国际战略之间的战略互动，形成相互支持的网络空间战略体系。

第一，结合网络空间治理的新近和未来发展态势，强化对国际机制的塑造能力。在网络空间全球治理层面，围绕治理平台的斗争日趋激烈。包括互联网论坛、国际电信联盟、伦敦进程、巴西网络空间多利益攸关方会议以及中国的世界互联网大会在内，各个平台都有其主导力量，参与的行为体所关注的议题和发挥的影响力均不相同。中国应结合世界互联网论坛以及参与的其他网络空间治理机制，在网络安全、网络犯罪、能力建设、网络经济、网络文化、数字鸿沟等议题中，探索如何提升自身向国际社会提供能力建设方案、最佳实践和解决方案等公共产品的能力。

第二，着重培养参与网络空间治理的国际化人才。国际互联网治理组织多为非政府组织，其采用的多利益攸关方治理模式通常要求从互联网社群中选拔高级管理人才，根据选拔对象对互联网技术、治理所作出的贡献来担任相应的高级管理职务，而非传统政府间组织的一国一票或按照人口、经济比例来分配名额。以 ICANN 为例，其现有的管理架构是由董事会和 3 个支持组织、3 个咨询委员会及 2 个技术咨询机构组成。董事会由 16 名具有表决权的成员和 5 名不具有表决权的联络员组成，除 ICANN 总裁之外，其余 15 个名额分别来自支持组织、一般会员咨询委员会、区域一般会员组织和提名委员会。要想当选为有投票权的委员，必须要通过自下而上的提名和选举。因此，中国应当理顺体制和机制，积极向 ICANN 等国际非政府组织输送人才，鼓励互联网企业、行业组织和学术机构积极参与 ICANN、IETF、互联网架构委员会（Internet Architecture Board, IAB）等机构的人才选拔，以此来提升在互联网国际组织中的代表性和发言权，并提高中国对互联网治理的影响力。

第三，加强网络强国战略与网络空间国际战略之间的战略互动。中国在“十三五”规划建议中正式提出网络强国战略，并从技术创新、网络文化、

网络基础设施、网络安全和信息化建设、国际合作五个方面着手，推进网络强国建设。^① 网络强国战略中多次提到了对外开放、积极参与国际互联网治理，甚至将国际合作作为单独一章。由此可见，网络空间国际战略与网络强国战略之间相互融合、相互支撑。两者的有效互动，关系到中国对网络空间的开放、安全与发展关系的处理。从双层博弈的角度来看，任何一个国家的战略都面临外部形势和内部利益集团的双重约束，过度强调开放或者安全都不利于整体国家安全和利益。强化网络强国战略与网络空间国际战略之间的互动，有助于提高决策者对于网络空间的安全与开放，网络空间的安全、发展、与开放之间关系的认知，打破双重约束，制定更加符合客观规律的政策。

从技术层面来说，网络强国战略可以更好地为中国参与全球网络空间治理提供支撑。当前网络空间治理的主要竞争已经从认知、理念层面的博弈，转向提供解决方案、最佳实践、能力建设等具体的议题合作领域。缺乏有效的支撑，网络空间国际战略难以持续，并赢得国际社会的认可。与此同时，网络空间国际战略也有助于为网络强国战略营造有利的外部环境、提供外部先进的经验和教训，向国内的 ICT 企业提供广阔的国际市场。最后，还可借鉴对外援助领域的经验，通过 ICT 领域的对外援助缓解甚至消除网络空间治理中的数字鸿沟问题，一方面可以为网络空间治理贡献中国力量，另一方面也有助于中国 ICT 企业的国际化战略。

[收稿日期：2015-12-04]

[修回日期：2015-12-24]

[责任编辑：樊文光]

^① 《网络强国战略》，新华网，2015年11月12日，http://news.xinhuanet.com/politics/2015-11/12/c_128421072.htm。