

B. 20

网络空间全球治理现状与 中国战略选择

沈逸*

摘要：网络空间无论潜在的还是现实的风险，都迫切要求对其进行全球治理。本文在界定了网络空间的概念、结构与特征之后，详细分析了网络空间全球治理的基本实践与现状，指出网络空间全球治理正处于转折的十字路口。一方面，以美国为首的发达国家不断巩固并改善自身对全球网络空间事实上的绝对控制；另一方面，对全球网络空间依存程度持续提升的新兴大国和发展中国家无法继续无视或者容忍美国在全球网络空间继续维持并滥用其优势地位，推进全球网络空间变革的呼声正在持续提升之中。作为新兴大国和发展中国家的大国，中国应该充分利用这一窗口时机，积极主动地参与网

* 沈逸，复旦大学副教授，主要从事国际政治、网络空间安全与治理方面的研究。



络空间全球治理，在战略路线、战略理念、战略突破与战略步骤上全面做好战略布局和战略谋划，以便更好地维护中国国家利益，同时也真正担负起大国责任，为世界贡献智慧与力量。

关键词： 网络空间 全球治理 中国战略 中国话语
全球网络空间新秩序

一 背景：网络空间的结构与特征

全球网络空间的发展，不仅让人们充分享受相互连接带来的收益，同时也对国家安全提出了全新的挑战。2013年4月，黑客窃取美联社的官方主账号，发布假消息称白宫发生两次爆炸、奥巴马受伤，导致美国金融市场出现短期急剧波动。2013年6月，美国中央情报局前雇员E. 斯诺登（Edward Snowden）披露美国秘密建设名为“棱镜”的网络监控系统，使如何制约霸权国家在网络空间滥用其能力优势成为各方关注的重点；2014年，美国商务部通信管理局宣布准备放弃对网络名称和地址分配机构直接监管的消息，更是将推进网络空间国际治理机构变革的问题提上了议事日程。正是在此背景下，网络空间国际治理的相关研究日趋具有其迫切性的需求。

“网络空间”是一个随着信息通信技术发展而出现的一个全新空间。从结构上来说，全球网络空间可以看作由众多不同的“层”（Layer）自下而上重叠而成：最基础的是“物理层”，即众多提供关键服务的服务器、路由器、交换机、终端接入设备以及将这些设备连接起来的有形或者无形的线缆；然后是“逻辑”/“代码”层，即运行于“物理层”之上的软件，这些软件构成并限定了最终用户使用网络的方式和限度，除非具备特定的能力，否则最终用户只能在“逻辑”/“代码”层限定的范围或者说给定的权限内接入网络并使用相关的资源；最后则是由具体的互联网用户所创造的“内容”层，即通过“物

理层”以及“逻辑”/“代码”层传播的由具体用户所创造的内容。^①

信息技术的发展使世界进入移动互联网的时代，内容的创造能力与信息搜集能力有了空前的发展，移动互联网发展的重点从计算转向了数据。超乎想象的大数据在网络空间以超越已有的数据抓取、存储、搜索、分析和呈现能力的速度迅速在网络空间累积起来，以海量、多样化、非结构化为特征的大数据时代来临。能够率先在数据存储与挖掘方面占据主导的行为体，在经济上就有机会创造前所未见的巨额财富，在政治上则可以获得前所未有的巨大影响力，进而在包含网络安全在内的整个安全战略领域获得巨大的战略优势。反之，如果未能预见，并做出妥善的应对，则主权国家将会被移动互联网的浪潮所吞没。如表 1 所示，2001 ~ 2010 年，利比亚、突尼斯、埃及、叙利亚手机用户增长了 25 ~ 218 倍，同期美国与中国的手机用户分别增长了 2.17 倍和 5.93 倍。移动互联用户的急剧增长发生在出现过“阿拉伯之春”的国家，显然并非偶然。

表 1 部分国家移动互联用户的增长速率

单位：倍

国 家 \ 年 份	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
利比亚	1	1.4	2.54	10	40	78.56	90	147.58	190.68	218
突尼斯	1.00	1.48	4.93	9.60	14.60	19.02	20.16	22.11	25.19	28.57
埃 及	1.00	1.61	2.08	2.74	4.88	6.44	10.77	14.78	19.81	25.29
叙利亚	1.00	2.00	5.93	11.73	14.75	23.38	31.18	35.28	50.11	59.00
俄罗斯	1.00	2.27	4.66	9.47	15.48	19.44	22.09	25.74	29.74	30.67
中 国	1.00	1.42	1.86	2.31	2.72	3.18	3.78	4.43	5.16	5.93
美 国	1.00	1.10	1.25	1.44	1.59	1.79	1.94	2.03	2.13	2.17

资料来源：国际电联 ITU 数据库（<http://www.itu.int/>）。
 注：利比亚、突尼斯、埃及、叙利亚、俄罗斯、中国、美国手机用户指数，以 2001 年为 100，时间跨度为 2001 ~ 2010 年。

网络空间是一个典型的非领土空间，类似之前曾经出现过的海洋、外层空间以及电磁波频率，不同国家遵循不同的行动准则，并展开激烈竞争。

^① Yochai Benkler, “From Consumers to Users: Shifting the Deeper Structures of Regulation Towards Sustainable Commons and User Access”, 52 Federal Communications Law Journal 561 (2000).



一种是“先占者主权”原则。这一原则建立在国家中心主义基础上，强调以实际控制能力为主要表现形式的硬实力，认为国家在此类非领土空间中的行动自由与国家的实力直接相关，有多强的实力就可以获得相应的使用份额。坚持此项原则的国家，往往看重“行动自由”，认为应该尽可能少地运用规则或者其他非实力因素去限制国家的行动，或者为国家的行动设定某种边界。

另一种是“人类共同财产”原则。对于技术等硬实力处于相对弱势的国家，尤其是那些在第二次世界大战后才逐渐进入国际舞台的发展中国家，往往试图借助多边主义以及国际机制保护自身合法权益。奉行此原则的国家认为，必须让所有国家，包括那些暂时不具备实际技术能力开发利用特定资源的国家，保留一定的资源份额，以便使其享受到作为人类共同财产的稀缺资源所能带来的福利和收益。

相比于海洋、外空以及电磁波频率这些非领土空间，网络空间非领土空间的属性更加特殊，“先占者主权”和“人类共同财产”两种原则之间的竞争及其可能产生的后果影响更加深远。

从属性上看，网络空间用户和资源分布的不对称性更加显著。国际电信联盟与其他相关机构的统计数据显示，全球网络空间的用户结构经历了从发达国家向发展中国家扩散的进程。截至 2013 年底，全球网络用户的总数已经突破 25 亿，在全球人口中所占比例将近 40%（见图 1），而且从 2006 年开始，来自发展中国家的网民在全球网络人口中所占比重逐渐接近并超过 50%，成为全球网民中的多数。

但是这种多数不能掩盖发展中国家整体网络渗透率偏低的现实：在总量提升的同时，各地区之间的差异比较显著。同样根据来自国际电信联盟的数据，欧美地区整体上网比例已经突破 60%，而非洲则不足 10%。

在与数据相关的关键设施方面，发达国家与发展中国家也存在着显而易见的差距。以支撑全球网络空间的关键基础设施之一——海底光缆系统为例。自 1988 年 12 月开始，第一条跨洋海底光缆（TAT-8）进入商业服务，到 2008 年，欧美公司垄断了全球光缆市场，其铺设的海底光缆普遍发端于欧美发达国家，或者以欧美发达国家为中枢桥接点。虽然从 2008 年开始，相关公司将投资方向转向了基础设施薄弱的非洲等地区，但欧美公司垄断海底光缆的事实没有改变。2008 ~ 2012 年，总价 100 亿美元的新的海底光缆系统投入使用，其中

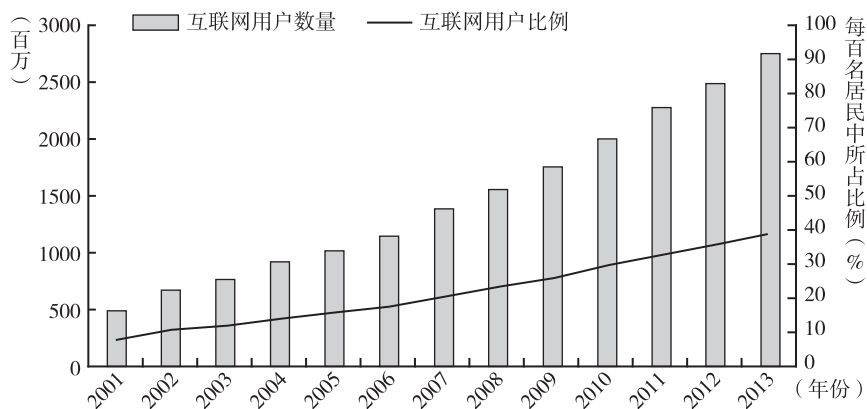


图1 2001~2013年全球互联网用户数量及比例

资料来源：国际电信联盟，<http://www.itu.int/en/ITU-D/Statistics/Pages/slat/default.aspx>，登录时间：2014年1月6日。

70%集中在撒哈拉以南非洲地区。从投资者的构成来看，欧美大型运营商以及大财团投资所占比重进一步提高，达到投资总额的80%，当地非电信部门的私人投资占14%，当地政府和开发银行仅为5%。

服务器是支撑全球网络空间的枢纽，但观察世界服务器厂商所占的市场份额，可以发现，惠普、国际商用机器公司（IBM）、戴尔、甲骨文、富士5家公司占据了2012年全球市场份额的84.7%，处于压倒性的优势地位。而全球网络空间关键性的资源——国际顶级地理域名主服务器及其管理者中，包括1台主根服务器和12台辅根服务器，分别归属4家美国公司、3个美国政府相关机构、2所美国大学、1家美国非营利的私营机构、1家欧洲公司、1个欧洲私营机构和1个日本机构管辖。

用户多数分布在发展中国家，优质的资源、服务以及关键技术多分布在发达国家，不对称性十分显著。因此，要弥合发达国家奉行的“先占者主权”原则和发展中国家呼吁的“人类共同财产”原则的鸿沟，其中的难度可想而知。

从效用看，有助于提升使用者福祉的公共性与带来额外收益的私有属性之间的张力十分显著。网络空间的用户，更加强调的是将网络作为提升使用者福祉的公益产品，看重的是网络产品以及网络空间行为的实际效用；网络空间资



源的所有者，在市场经济背景下，优先考虑的是获取更多的利润回报；在主权国家为主体构成的国际体系中，掌握优势网络资源且信奉先占者主权原则的主权国家更加关注的是如何用网络空间来增强自身的实力。对于这些国家（通常是发达国家）来说，“先占者主权”天然与自我中心的理性人假设相匹配，遵循这一原则近似某种必然的选择；相反，如果转而奉行“人类共同财产”原则，则可能是“非理性”的。

但是，网络空间的特殊性在于：必须同时保持一定的覆盖范围，也就是说，网络空间必须具有某种公共性，而不能成为少数乃至单一国家政府掌控之下的私有网络；同时，如果所有国家都奉行同样程度的先占者主权原则，网络空间可能在某种程度上陷入霍布斯所说的无政府状态，即一切人反对一切人的战争。这种无政府状态下的网络空间，难以成为提升用户福祉的来源。

二 实践：从互联网治理到全球网络空间治理

信息技术的持续进步，网络用户的大量增加，日益深刻地改变着人类日常的行为模式。但是，信息技术的高速发展并不意味着人们就此进入一个天堂般完美无缺的世界，在带来便利的同时，整个人类社会同样面临着巨大而广泛的挑战和考验：信息技术本身存在各种先天的缺陷，同时不同的个体对于信息技术的掌握程度存在显著的差异，随着信息技术深入渗透到社会的各个层面，在带来巨大收益的同时，也诱惑着部分个体或组织借助其掌握的技术优势去获取更大的回报，而整个社会也因此面临巨大的风险。

为了规避网络空间的安全风险，使其成为提升人类福祉的共同来源，网络空间迫切需要国际治理。在 2003 年召开的全球信息社会峰会（World Summit on the Information Society）突尼斯会议上，首次就互联网是否要治理以及如何治理等问题展开了激烈讨论，这一讨论的结果推动了联合国秘书长设置互联网治理工作组（Working Group on Internet Governance），授权此工作组研究并提出网络治理的定义。2004 ~ 2005 年，此工作组召开了四次会议，最终于 2005 年 6 月，互联网治理工作小组提交了工作报告，此报告界定了互联网治理的工作定义：互联网治理就是政府、私营公司和社会，根据各自的角色、共享的原则、规范、规则、决策过程以及程序，来塑造互联网的演化和使用。与此同

时，这份报告首次明确提出了互联网治理的对象：网络治理的对象远远不止网络地址和域名管理，还包括更加重要的内容，包括关键网络资源，互联网安全，确保使用互联网促进发展等。

根据这份报告内容与互联网以及网络空间的密切程度，可以看出互联网治理的同心圆结构，如图 1 所示。

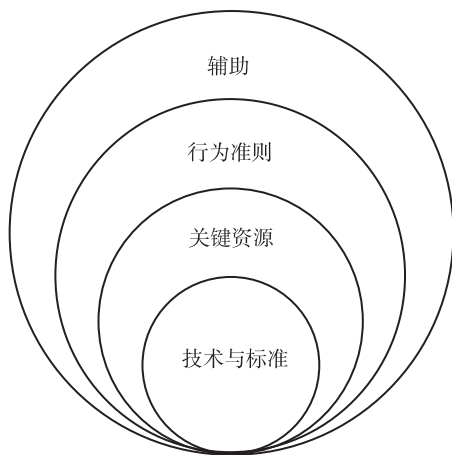


图 1 互联网治理的同心圆结构

其中，最核心位置的是互联网赖以存在和发展的关键技术与标准的掌控，掌握了技术与标准，则网络未来发展的方向与路径就在很大程度上被决定了；同时，掌握了最新技术与标准的行为体，也会因此获得远远超过其他行为体的话语权和战略优势。其次就是互联网关键资源的管理，包括域名系统和互联网地址的管理；根服务器系统的管理，特别是对根服务文件的管理；技术标准的管理；平行互联的管理；电信基础设施的管理；技术创新的管理。再然后，核心位置之外处于治理中心地位的是对使用互联网方式和网络空间里不同类型行为的管理，包括治理互联网的垃圾邮件，保障网络安全，以及网络犯罪的治理。截至 2014 年底，围绕这些问题的全球治理，也就是不同类型治理主体之间的关系协调问题并没有得到有效解决。最后，中心地位之外的是与互联网发展不直接相关的支撑或者辅助性机制安排，比如最典型的是工作组所列举的知识产权保护。



在 2005 年网络治理工作组提交的报告中,对互联网治理当时的状况做了简要的评价,相关内容如表 2 所示。

表 2 互联网治理的对象及现状

名称	现状	简述
根区文件和系统管理	事实上单独处于美国政府控制之下	因为历史因素,美国政府是唯一一个在现有的多边利益相关方里有权、有能力更改根区文件和系统的主权行为体,对根区有操作权的行体与美国政府之外的主权行为体之间缺乏正式的法律管辖关系
互联费用	不公平分布的费用	越是距离骨干网遥远的互联网服务供应商,越是需要支付昂贵的网络接入费用,对此接入费用问题,缺乏有效的解决方案
互联网稳定性、安全性和网络犯罪	缺乏有效的机制和工具	缺乏有效的机制保障网络的稳定性和安全性,缺乏有效的机制来解决跨国犯罪问题
垃圾邮件	无一致认识	对垃圾邮件的定义缺乏共识,无一致的全球协定作为各国反垃圾邮件立法的基础
参与全球政策的发展	现有的多边利益相关方模式存在显著缺陷,阻碍了弱势方实质性地参与全球治理体系	缺乏透明度、公开性和可参与的进程,政府间组织和国际组织的参与受到限制,对发展中国家、个人、社会组织和中小企业来说,进入门槛过高,全球网络空间治理的会议举办集中在发达国家,缺乏全球网络空间治理的有效参与机制
能力建设	国家层面资源分配不均	发展中国家的网络能力建设缺乏足够的资源支持
域名分配	有关顶级域名的建设需要新机制	有关通用顶级域名 (generic Top-level Domain Name, 缩写为 gTLDs) 的政策和(管理)流程需要进一步的完善
IP 地址分配	IP 地址分配的政策引发关注	对 IP 地址分配政策感到担心。因为历史原因,IPv4 地址分配存在不均衡;这一不均衡的现实已经在互联网地区注册机构的报告中得到了反映;在向 IPv6 地址转移的过程中,一些国家感到有关地址分配政策应该有必要保障平衡,即确保各地区都能均衡地获取这一资源
知识产权保护	如何适用于网络空间	如何有效地将知识产权保护原则适用于网络空间,存在不同的观点,需要在权利的拥有者和权利的使用者之间,达成某种均衡
数据保护和隐私权	不存在或者缺乏一致性	无论是国别的法律体系,还是全球标准体系,都缺乏适用于网络空间的隐私和数据权利保护。由此导致的结果是,即使法律承认用户拥有相关的权利,但用户也没有什么有效的手段来保障和实现自己的权利。比如,在某些用于查询 WHOIS 的数据库里,显然缺乏对个人信息的保护



续表

名称	现状	简述
消费者权益	缺乏全球标准	在电子商务等环节,缺乏全球标准来保障互联网上的消费者权益
语言问题	进展不显著	在推进互联网多语种运用上缺乏国际协调;在多语言顶级域名、多语言电子邮件地址和多语言关键词查询、多语言本地(网络)内容等领域没有解决技术标准问题

资料来源: Chateau de Bossey, “Report of the Working Group on Internet Governance”, June 2005, <http://www.wgig.org/docs/WGIGREPORT.pdf>, 最近访问时间: 2014 年 12 月 13 日。

从治理主体的角度来说, 网络的国际治理, 除了主权国家的政府之外, 还涉及一系列的政府间国际组织、国际非政府组织、非营利性的私营公司等。综合已有的资料, 在国际层面参与网络治理的最主要行为体及其基本性质、职责和功能, 如表 3 所示。

表 3 网络空间国际治理主要行为体及其性质、职责与功能

名称	类别	取向	位置	备注
亚太经济合作组织(APEC)	区域性多边国际组织	制度与跨国合作	边缘	主要机制为亚太经合组织电信与信息工作组
东南亚国际组织(ASEAN)	区域性多边国际组织, 军事联盟背景	制度与跨国合作	边缘	依据 2009 ~ 2015 年东盟共同体路线图, 包含打击跨国网络犯罪等行动计划
欧洲理事会(EC)	区域性多边国际组织, 政治联盟背景	制度与跨国合作, 侧重打击网络犯罪方向	外围	强意识形态色彩的政治同盟; 历史悠久; 聚焦网络犯罪与反恐
欧洲联盟(EU)	区域性国际组织, 主权国家构成的一体化组织	能力建设, 制度与跨国合作, 强调全面的网络安全能力	中心外围之间	欧盟主要执行欧洲委员会下设欧洲网络与信息安全局(ENISA), 专职负责网络安全问题; 同时设有欧洲标准化委员会(ECS)、欧洲电工标准化委员会(ECES)、欧洲电信标准机构(ETSI), 共同推动网络和通信技术标准化工作
事件响应和安全团队论坛(FIRST)	主权国家背景的跨国技术工作论坛	能力建设, 问题解决与制度建设	中心	技术取向, 与标准化组织密切合作, 采用“通用脆弱评分系统”(CVSS), 为信息系统的脆弱性进行标准化评定
八国集团(G8)	多边政府间国际组织	能力建设, 制度建设与跨国协调合作	中心	下设高科技犯罪小组, 以及全天候响应的高科技犯罪联络网络



续表

名称	类别	取向	位置	备注
电机及电子学工程师联合会 (IEEE)	专业技术人员构成的国际组织	技术标准建设	中心	主要起作用的是下设的标准委员会,此委员会与美国技术与标准国家委员会相协调,共同起草电力控制系统的网络安全标准
国际电工委员会 (IEC)	政府间国际组织,由各国的国家或私营界的委员会构成	技术标准建设	核心	与国际标准化组织的联合技术委员会,共同起草并发布作为国际标准的技术方案
国际标准化组织 (ISO)	国际非政府组织	技术标准建设	核心	与国际电工委员会协作发布网络安全技术标准
国际电信联盟 (ITU)	联合国下属的政府间国际组织	能力建设,国际发展与跨国协调	中心与外围之间	分为三个部门,包括电信标准化部门 (ITU-T)、无线电通信部门 (ITU-S)、电信发展部门 (ITU-D)
互联网号码与名称分配局 (ICANN)	私有非营利性美国公司	协调管理	核心之核心	协调对全球域名系统的技术管理,根据从美国商务部获得的招标合同,行使 IANA 职能
互联网工程任务组 (IETF)	基于资源的松散跨国网络	核心技术研究、技术标准研究	核心之核心	1986 年由美国政府组建,主要通过电子邮件开展工作。主要在互联网工程指导小组监督下开展工作
互联网治理论坛 (IGF)	跨国论坛	观念与信息交流	中心	根据 2005 年信息社会世界峰会 (突尼斯进程) 授权联合国秘书长创立,主要讨论网络治理相关政策问题的基于多利益相关方模式的论坛;议程设置松散;并不直接形成技术标准或者有约束力的文件,但会上讨论的观念和信息会对其他国际组织产出重要影响
国际刑警组织 (INTERPOL)	政府间合作组织	聚焦打击计算机、网络犯罪	中心	全球打击网络犯罪的最重要的合作网络,构成网络治理的重要组成部分
Meridian 进程	政府间合作机制	聚焦关键基础设施保障的政府间合作机制,并正试图将合作范围扩展到工业控制系统	中心	2005 年在英国举办,之后匈牙利等多国和地区举行,是全球主要的政府间网络关键基础设施保障问题对话机制。美国国土安全部、白宫等在其中发挥重要的作用



续表

名称	类别	取向	位置	备注
北大西洋公约组织 (NATO)	军事同盟、政治同盟	聚焦美国及其核心军事盟友的网络安全, 网络战	中心	《塔林文件》, 以及设置在爱沙尼亚的北约卓越中心聚焦网络战行为规范和网络战具体实践案例研究
美洲国家组织 (OAS)	政治同盟	聚焦反恐、网络安全标准以及打击网络犯罪	中心 - 外围	2004 年通过美洲国家全面网络安全战略, 以美洲国家反恐委员会 (CICTE) 应对来自网络的恐怖威胁; 以美洲国家电信委员会 (CITEL) 检讨并统一美洲国家的网络安全标准; 美洲国家司法部长会议下的网络犯罪政府专家组来应对网络犯罪问题
经济合作与发展组织 (OECD)	基于意识形态的政府间国际组织, 政治联盟	内部成员的网络安全与隐私政策协调	中心与外围之间	基于共识的决策机制

数据来源: United States Government Accountability Office, “Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance”, <http://www.gao.gov/assets/310/308401.pdf>, 最近访问: 2014 年 12 月 13 日。

三 现状：全球网络空间治理的不对称性与相互依赖性

网络空间国际治理体系的基本现状，是美国占据显著优势位置下的不均衡发展。以美国为代表的欧美发达国家连同那些掌握在它们手中的公司与组织，在全球网络空间治理中占据中心位置，其优势体现在关键技术标准、应用、基础设施、核心硬件研发、生产以及商业化能力方面，起到存储、挖掘和使用数据的作用，并有能力将技术优势转化为巨大的商业优势；以大量亚非拉地区的发展中国家为代表，处于全球网络空间治理中的边缘位置。

掌握了信息技术优势的新型跨国公司，以谷歌（Google）、推特（Twitter）、脸谱（Facebook）等为代表，正逐渐具备了正面挑战国家主权的能力，伊朗、埃及、突尼斯等发展中国家在 2009 ~ 2011 年遇到了这种挑战。相关事件发展证明，完全依据传统管制方式的政府可能因为无法适应新的挑战而失去管制的



合法性，乃至最终导致政权更迭。

具备熟练的信息技术运用能力和得到跨国网络支撑的非政府行为体，无论是基地组织这样的恐怖主义团体，还是埃及“四月六日运动”（April 6th Movement）或者塞尔维亚“应用非暴力行动和战略中心”（Center for Applied Non Violent Action and Strategies，简称 CANVAS）这样的非政府组织，都得以通过网络发布信息、交流知识和技能、建构与其他类型的行为体（包括政府、公司和国际非政府组织）的跨国互动，进而在某个特定地理位置或者特定事件上，形成对目标国家的局部优势，进而威胁国家安全、挑战原有的游戏规则，或者影响国际体系既定的互动模式。

从更加深层次的权力关系来看，全球网络空间与信息革命的出现，固然挑战了原有的权力结构，但也为强化原先就占据压倒性优势的行为体，提供了巨大的机会。即使是众多看起来是非政府组织有效挑战国家主权的实践案例，大量事后披露的材料也会最终证明，能够借助信息技术挑战国家主权的非政府组织，几乎无一例外地必须得到来自其他主权国家的支持。

美国在网络空间国际治理中占据显著的优势地位，这种地位主要通过三个方面显著表现出来：首先，美国商务部通信管理局（NTIA，Department of Commerce）掌握法理上对网络空间最重要的关键基础设施——域名系统的管理权（见表4），全球互联网名称和地址分配机构（ICANN）必须从商务部通管局获得合同，才能在其管理下对网络域名实施管理；其次，根据合同，对全球域名服务器根文件的变动或者修改，如增加一个新的顶级域名，必须得到美国商务部通信管理局的批准，而美国做出的让步是承诺对此类权力的使用保持必要的克制，不做带来负面效果的改进；最后，美国商务部通管局可以随时根据需要，对 ICANN 的核心机构——互联网号码分配当局（IANA）的权限进行增减。2012 年美国商务部通管局在延长 ICANN 管理合同期限到 2019 年时，就提出了“凡是试图要增加新的顶级地理域名的申请，必须向 IANA 提交一份文档，以证明此新顶级域名的增加反映了所有利益相关方的共识，并有助于全球公共利益”。此项规定引发了激烈抗议，最终在 2011 年 11 月 11 日，此项规定被改成“提交一份专门的文档，说明此项措施如何增加了机会，让相关的利益相关方获得了更多的机会，并且有助于全球相关公共利益”。与此同时，美国政府仍然保留了相当的特权：所有竞争此项合同的必须是全部归美国所有和

运营的企业，或者是美国的大学或学院；所有主要的运作和系统都必须在美国领土；美国政府保留检查合约内各项系统和系统运作情况的权力。

表 4 网络管理关键基础设施：顶级地理域名服务器的管理者

主机名	IP 地址	管理者	地理位置
a. root-servers. net	198. 41. 0. 4, 2001 : 503 : ba3e ; : 2 ; 30	VeriSign, Inc. 威瑞信公司	美国弗吉尼亚
b. root-servers. net	192. 228. 79. 201	University of Southern California (ISI) 南加州大学	美国加利福尼亚
c. root-servers. net	192. 33. 4. 12	Cogent Communications Cogent 通信公司	美国华盛顿 D. C.
d. root-servers. net	199. 7. 91. 13 , 2001 : 500 ; 2d ; : d	University of Maryland 马里兰大学	美国马里兰
e. root-servers. net	192. 203. 230. 10	NASA (Ames Research Center) 美国航空航天管理局	美国加利福尼亚
f. root-servers. net	192. 5. 5. 241 , 2001 : 500 ; 2f ; : f	Internet Systems Consortium, Inc. 互联网系统协会有限公司	美国加利福尼亚
g. root-servers. net	192. 112. 36. 4	US Department of Defence (NIC) 美国国防部(网络信息中心)	美国弗吉尼亚
h. root-servers. net	128. 63. 2. 53 , 2001 : 500 ; 1 ; : 803f ; 235	US Army (Research Lab) 美国陆军研究实验室	美国马里兰
i. root-servers. net	192. 36. 148. 17 , 2001 : 7fe ; : 53	Netnod Netnod 网络公司(瑞典)	瑞典斯德哥尔摩
j. root-servers. net	192. 58. 128. 30 , 2001 : 503 ; c27 ; : 2 ; 30	VeriSign, Inc. 威瑞信公司	美国弗吉尼亚
k. root-servers. net	193. 0. 14. 129 , 2001 : 7fd ; : l	RIPE NCC 欧洲网络资源协调中心	英国伦敦
l. root-servers. net	199. 7. 83. 42 , 2001 : 500 ; 3 ; : 42	ICANN 互联网域名与名称管理机构	美国弗吉尼亚
m. root-servers. net	202. 12. 27. 33 , 2001 : dc3 ; : 35	WIDE Project 大范围集成分布式环境项目	日本东京

仅就 ICANN 现有的内部决策机制看，也存在比较显著的权力分配不均衡的问题：第一，民主化，或者说国际化程度不足。截至 2014 年底，ICANN 政府意见委员会有 111 个国家或地区的正式成员，但是 ICANN 的决策机构理事



会成员只有 16 个有投票权的名额；而这 16 名代表的产生，只有 1 名是通过相对民主的一般委员会产生，其他 15 人由提名委员会产生。提名委员会，根据章程第 7 条第 2 款，包含 15 名有投票权的委员构成；其中 5 名委员会来自一般委员会，7 名委员来自普遍名称支持机构，3 名委员来自名称委员会等相关支持机构。提名委员会和理事会的整体数量限制，都决定了无法有效保障足够的代表性。第二，现有地理区位的划分亟待调整。无论是互联网用户数量，还是国家数量，现有的五大地理区域划分都已经无法反映互联网发展的现状，最明显的一点就是现有的地理区域划分中，亚洲、大洋洲、太平洋区域是作为一个区域，而北美也是作为一个单独的区域。这种划分，或许在互联网发展早期能够反映网络用户的地理分布，从而具有足够的代表性，但现在显然已经完全脱离了网民分布的实际。^① 第三，整个 ICANN 理事会成员、提名委员会成员中，来自欧美公司的比例过高，技术力量相对落后，但拥有庞大数量的亚非拉地区新兴国家的代表缺乏。以本届理事会为例，非西方的代表 4 人，分别来自智利、阿根廷、南非和中国台湾地区；而美国一国就产生了 4 名代表，加上 2 名加拿大代表，单一北美地区的代表就超过 6 人。不平等性可见一斑。

必须要说明的是，域名管理仅仅只是全球网络空间治理的一小部分内容，用联合国 2005 年网络治理工作组提交报告的话来说，“能力建设”才是真正的关键所在，是网络空间国际治理的主题。在欧美发达国家看来，美国倡导的多边利益相关方面模式，被认为是实现“能力建设”、缩小“数字鸿沟”的最为有效的方式。

从现状看，全球网络空间治理的整体架构呈现显著的不对称相互依赖特征，所有国家和行为体整体上对网络存在显著的依赖性；发达国家凭借技术、制度、战略、政策能力等综合优势，占据显著地位，敏感性强而脆弱性较低；发展中国家对网络空间的依赖则是典型强敏感高脆弱，作为数据主要提供者的发展中国家，没有获得相匹配的收益，在网络空间面临被边缘化的局面。

^① 根据 ICANN 的章程第五款，国际代表性的相关规定，地理区域划分为欧洲、亚洲/大洋洲/太平洋地区、拉美/加勒比地区、非洲以及北美，资料来源：BYLAWS FOR INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, Section 5, 来源：<https://www.icann.org/resources/unthemed-pages/bylaws-2002-12-15-en>，最近访问时间：2014 年 12 月 13 日。

相比已经引发广泛关注的域名分配问题，在对网络空间治理起支配作用的关键技术和标准层面，发达国家的支配地位与发展中国家的弱势地位所带来的问题更加严重。1985 年成立的互联网工程任务组（IETF）就是最典型的代表。IETF 是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定，绝大多数国际互联网技术标准出自该组织的意见征求书。从形式上看，IETF 是一个由为互联网技术发展做出贡献的专家自发参与和管理的国际民间机构。它聚集了与互联网架构演化和互联网稳定运作等业务相关的网络设计者、运营者和研究人员，并向所有对该行业感兴趣的人士开放。IETF 的体系结构分为三类：互联网架构委员会（IAB）、互联网工程指导委员会（IESG），以及在八个领域里面的工作组（Working Group）。

但是，互联网架构委员会的前身是 1986 年美国建立的互联网活动委员会（Internet Activities Board），这个委员会是美国国防部先进研究署（DARPA）管理互联网活动的互联网设置控制委员会（ICCB）的接替者。这些委员会的发展演变与互联网的逐步商业化密切相关，但这种演化的过程始终处于欧美发达国家政府、技术人员以及公司的有效控制之下。

四 出路：中国参与网络空间全球治理的战略选择

当下中国面临复杂的安全态势，在全球网络空间治理中处于相对弱势的不利状态。但是，中国同时也面临难得的机遇，这一方面来自美国迫于国际压力所做出的暂时调整，即美国于 2014 年 3 月宣布的准备放弃对 ICANN 的直接监管，将其移交给一个新的多边利益相关方构成的机构；另一方面来自中国自身所具有的整体资源和能力的巨大发展。基于这一大背景，综合全球网络空间治理体系的现状，大体可以得出如下几个方面的简要结论。

（一）战略态势：挑战重重，但已经面临转折点

全球网络空间仍然主要处于美国控制之下，但这种控制已不是不可动摇和不可挑战的、绝对的、全面的控制。全球网络空间治理结构正处在转折的十字路口，一方面，美国试图运用暂时的退让，凭借美国公司、私营机构和非政府组织的强大技术优势和影响力，以退为进，巩固并改善自身对全球网络空间事



实上的绝对控制；另一方面，对全球网络空间依存程度持续提升的国家，包括新兴国家和发展中国家，都无法继续无视或者容忍美国在全球网络空间继续维持并滥用其优势地位，推进全球网络空间变革的呼声正在持续提升之中。

对中国来说，面对这样一个变局，需要从战略高度形成自己的认识和判断：整体而言，中国面临的主要威胁，不是美国直接运用自身的综合软硬实力，在短期内挑战和冲撞中国的政权或者国家安全，而是美国持续维持其在全球网络空间治理结构中的优势地位，并将这种优势地位转化为在网络运用等科技发展最前沿领域对中国进行全面围堵与遏制。这种“温水煮青蛙”的战略如果成型，则中国长期持续发展的战略动力将被逐渐扼杀，改革开放 30 年以来取得的成果将因为长期战略动力的失去而逐渐被消耗殆尽，进而在中美战略竞争的持久博弈中最终处于失败的境地。换句话说，从持久战的视角出发，在全球网络空间的博弈，是中美双方逐渐进入战略相持阶段的标志，中国必须有长期持久作战的耐心和决心，也因此必须克服短期的恐惧和焦虑，构建自己的国际网络空间治理的大战略。

中国面临的主要挑战是，中国在全球网络空间中仍然是最为典型的发展中国家，表现为中国在全球网络空间各关键领域的全面落后或者是处于相对弱势地位。这种落后和弱势，覆盖完整的产业链和价值链，以及网络空间各个关键应用领域。应对这种全面的挑战，必须形成一个完整的战略体系，从短期、中期、长期出发，形成完整的战略发展路线和愿景，从而有效、系统地应对中国发展所面临的挑战，做出全面的回应。

（二）战略路线：全面替代、部分替代和关键卡位的选择

从技术和应用发展的角度来看，中国推进全球网络空间治理结构变革的底气，最终需要来自技术、标准、基础设施、接入设备、关键应用和核心能力的支撑。在这条道路上，从改革开放至今，整个中国均面临着艰巨的选择。在网络空间治理方面，战略路线就是在全面取代、部分替代以及关键卡位三者之间的权衡与取舍。

全面替代意味着中国拥有自己的 IOE，包括芯片、操作系统、通信协议、核心节点设备、存储装置等，这不仅仅是技术先进性程度上的超越，而且还是市场化运用领域的超越。但是，这种全面替代需要时间，甚至可能是漫长的时

间。在全面替代之前，如何应对成为需要面临的问题。世界不会因为中国的需要而停下脚步，因此，全面替代可以作为长期战略，基于中国自主知识产权的芯片、操作系统等要大力研发，但这显然只是战略路线中长期的部分，而不是全部。

相对全面替代而言，先要做到部分替代。这里的“部分”是指根据中国自身能力和需求，在力所能及的关键点上，实施有效的替代。这种替代无法改变全局，但能改变局部的力量对比。比如，可以考虑的是推进以华为为代表的国产设备在国内网络传输核心枢纽节点上的替代，也就是至少在国内，在至关重要的网络体系中，将数据传输的核心枢纽掌握在中国自己手中。当然这不仅仅是换上华为设备的问题，还包括了相应的安全机制和安全能力的全面更新。这种替代，因为明确建立在中国已有的技术、标准和产品能力的基础上，所以相对更加快速，而且能够在中短期内看出相应的成效。但同时，这需要中国相关主管部门在管理方式、方法和制度设计上，做出必要的调整。这种调整，不仅要符合中国的国家利益，而且还需要在形式和程序上符合相应的国际游戏规则。一如美国对华为的制约，无论多么牵强，但至少还是努力在法律的框架内进行的。这要求中国不仅提升自身的技术能力，还必须提升自己的治理能力，这种能力，不仅在中短期内有效，而且还会对长期战略博弈产生深刻的影响。

部分替代仍然需要一定的时间，而且无法全面改变力量对比和战略态势，这就需要同时用关键卡位来弥补。关键卡位，卡的是以入侵安全监测为典型代表的关键能力，包括入侵安全监测、攻击防御、0day 漏洞的有效挖掘与修复等。和中国一样，俄罗斯在芯片、操作系统、关键基础设施等领域也全面落后于美国，但是，俄罗斯凭借卡巴斯基强悍的防卫能力，至少可以有效地侦测并阻断美国实际实施的入侵行动。换言之，关键卡位能力意味着阻断对手将胜势转化胜利，阻断对手实际运用自己的战略优势来获取实际的利益。在这个过程中，中国所拥有的庞大的民间安全技术团队，当仁不让地成为主力。相比具有资源优势的国家队，民间团队最宝贵的是布局人才核心战略优势。但这一优势正面临来自跨国公司的挖掘与收购，比如，最新攻破了苹果 64 位操作系统的 Keen 团队已经收到了来自谷歌团队的收购邀约，出价 10 亿美元；再比如，刚刚拿到亚洲企业在全球入侵检测团队首个第一名成绩的安天工作室，其核心技术人员也面临外资公司的强力挖掘。中国政府必须对这些民间企业提供战略级



的投资和支持，为这些企业进入市场，自主获取合理利润，提供最大限度的支持和保障。这是在最短时间内扭转中国在网络空间治理中不利态势的、最有效的手段和方法。当然，这种战略投资的注入，必须注意参考市场化的做法，通过风险投资的机制实施，避免好心办坏事。

总体而言，中国当下需要形成自己的推进全球网络空间治理变革的路线图，将上述三个方面，即关键卡位、部分替代、全面替代，作为中国发展战略应对能力的短期、中期、长期选择。

（三）战略理念：从“删除、封堵”到“开放、引导、鼓励”的转变

中国要在全球网络空间治理中取得突破，中国国内对互联网的管理必须做出重大变革与调整。这种调整，就是在思路上从“删除”和“封堵”改为更加积极的“开放”“引导”以及“鼓励”。必须指出的是，不存在没有管理的互联网，但问题是要找到合适的方法进行管理。有效的管理，应该符合用户的使用习惯，并且为用户所接受。美国的“棱镜”项目曝光之后，并没有引发美国国内网民的强烈反弹，原因在于，这种监控式的网络管理，对用户来说，除非被告知，否则难以察觉。只要解决了有效应用监控所得资料的问题，对多数用户来说，互联网就是没有管理的。这极大地降低了美国政府管理互联网时面对的各种阻力和不满。中国应该从中吸取经验。

中国对互联网管理有自己的需求和特色，但至少需要就管理的规则尤其是具体操作性的规则做出详细的规定，并以法律形式向社会公布。在现行管理体制中，属地化分散的管理权限，自由裁量的空间过大，不仅让用户感觉恶劣，而且还提供了巨大的寻租空间。蓬勃发展的删帖产业，就是这种寻租的集中体现。2014年4月新闻披露1名海南网警接受贿赂，删除天涯论坛上的负面信息和新闻，是当下网络管理内在结构性危机的冰山一角。不尽快变革，则可能让中国失去参与全球网络空间治理的战略机遇期。因此，这个调整，不是一个简单的战术问题，而是一个重大的战略问题，必须慎重对待。

（四）战略突破：构建“全球网络空间新秩序”

除了上述操作性的内容之外，中国参与全球网络空间治理结构的变革，还必须在话语和符号塑造方面发出自己的声音。从短期看，2014~2015年这两

年，是中国参与并影响全球网络空间治理新秩序的机会之窗，中国应该积极行动起来，至少先提出符合中国国家利益的全球网络空间治理新模式，建议可以考虑“创建全球网络空间新秩序”为主要诉求，实现对“数据主权”的有效保障和运用，并团结新兴国家和发展中国家，共同推动网络空间治理秩序的全面变革。

第一，“全球网络空间新秩序”可以被视为“世界信息与传播新秩序”运动的继承和发展，有利于中国在国际舆论环境中争取更加有利的态势。建立“世界信息与传播新秩序”运动是20世纪60~70年代，世界上各个发展中国家共同倡议发起的，旨在改变世界传播格局不平等、不平衡的状态。这一运动因为苏联的解体，以及20世纪80~90年代发达国家与发展中国家悬殊的力量对比而最终没有取得成功。如果中国能够在继承的基础上，倡导并推动建立、完善“全球网络空间新秩序”，有助改善中国的战略处境，在全球舆论空间占据道德高地，获取话语主动权，抵消来自美国倡导的“互联网自由”理念的战略压力。中美围绕网络空间展开的话语博弈，很大程度上是一场抢占全球舆论场道德高地的博弈。简单否认美方指责，只会加剧中国的战略被动，中国必须提出既符合自身国家利益，又符合世界发展潮流的核心理念，才能在同等高度上回应美国压力，这同时也是中国成为负责任大国的重要标志之一。

第二，“全球网络空间新秩序”可以构成支撑中国网络空间战略的核心概念。中国的发展离不开信息技术产业，中国的发展也无法照搬与复制西方国家的老路，因此倡导建立“全球网络空间新秩序”，可以成为中国构建自身网络空间战略的核心概念，将“治理”而非“竞争性博弈”作为应对网络空间挑战、保障中国网络安全的主要手段。从实际效果来看，倡导并推动建立、完善“全球网络空间新秩序”，有助于中国凝聚对现有旧秩序不满的国际力量，也让西方国家难以直接否认。

第三，倡导建立全球网络空间新的信息与传播秩序为中国外交战略提供了新的工具、平台与载体。中国在进入崛起阶段之后，反复声明要建立一个新型大国，要倡导大国与大国之间的新型关系，但目前缺乏一个整体性的具有道德正义性的平台。倡导建立全球网络空间信息与传播新秩序，将中国重视的基本行为准则，包括尊重主权、平等互利、多元包容等纳入其中，不仅体现中国的



国家利益，而且能够用中国智慧为世界做出贡献。“全球网络空间新秩序”将涵盖全球网络空间关键资源共享新秩序、全球网络空间安全新秩序以及全球网络空间信息传播新秩序三个层面，从软硬件资源、行为规范与治理模式三个维度，规划一个理想化的、让多数国家特别是那些在技术、软硬件资源暂时处于劣势的行为体都可以从中受益的全球网络空间。

第四，“全球网络空间新秩序”的基本目标是安全、平等、开放、协商、有序。“全球网络空间新秩序”的核心是走强调合作的道路，“以治理求安全”的理念，通过保障全球网络空间在良性秩序下运行，来保障中国在全球网络空间的安全及利益。其中，（1）“安全”是指，国家应免于受到来自网络空间的冲击与挑战，国际社会支持和鼓励国家通过对关键基础设施、关键数据以及关键服务的有效监管保障自身安全。任何在中国开展业务的企业，都必须将与中国相关的网络基础设施、数据、服务保存在中国境内的数据中心，未经明确授权，不得将其交给外国政府处置。（2）“平等”是指，不同类型的行为体，无论国家大小与技术能力强弱，都处于平等位置，都有均等的从网络空间发展中受益的权利。（3）“开放”是指，全球网络空间向所有合法用户开放，国家不以自身私利垄断性地使用网络技术以及资源。掌握先进技术、应用和资源的行为体，应该主动协助弱势行为体缩小差距，协助弱势行为体培育和发展自身的相关产业或能力。（4）“协商”是指，在新秩序中，存在矛盾与冲突的行为体通过谈判与磋商的方式，而非使用或威胁使用武力，来解决彼此之间的分歧；掌握技术优势的跨国公司应该尊重发展中国家的权益，避免滥用自身技术优势或者是其他大国的支持来谋求有利于自身的争端解决。（5）“有序”是指，新秩序追求在全球网络空间中建立有利于信息有序流动的行为准则。这种有序的信息流动，以信息流动是否能够促进人类生活的实际改善为主要衡量标准。^①

追求实现上述目标的“全球网络空间新秩序”，应成为中国的国家战略，以此摆脱不利局面，跳出“跟着美国走”的怪圈，完善一套全新的全球网络空间游戏规则。

^① 沈逸：《从“棱镜门”看全球网络空间新秩序的建构》，《学习月刊》2013年第8期，第38页。

（五）战略步骤：建立“全球网络空间新秩序”需要顶层设计、综合协同、政策创新、产业配套

1. 顶层设计

因为美国“棱镜”项目的曝光，美国追求网络霸权的战略遭遇批判。我们应该把握契机，从顶层设计入手，推进建立“全球网络空间新秩序”的工作。政府应吸纳国内相关高校和科研机构资源和专家，开展中国网络空间关键基础设施与关键基础数据调研，充分了解发展现状以及具体的困难与挑战；依据上述调研结果，着手制定《中国网络空间国际战略》，从战略全局把握中国国家利益与全球网络空间新秩序之间的辩证关系，推出明确阐述中国主张的战略文件。

2. 综合协同

参考美国经验，在中国外交部、国防部、工信部、公安部等相关机构，设立网络空间事务协调会议，依据国家战略，协调各自工作，共同推进网络空间新秩序的建设；鼓励中国国内学术机构，围绕全球网络空间新秩序开展跨国研究，从理论上丰富和完善全球网络空间新秩序的内涵，并提供相应的建议。网络安全和信息化工作小组的成立，可以看作已经迈出了最为关键的一步，接下来，就是如何落实与完善的问题了。

3. 政策创新

在国内，推动产业政策创新，鼓励中国企业发展网络空间关键设备、技术、应用，推动咨询政策创新，鼓励中国高校、研究机构实现创新协同，围绕网络空间新秩序，建立官产学研一体的咨询智库或是创新平台，推动具有中国自主知识产权的网络空间技术标准以及测评体系的发展；在国际社会，以建立全球网络空间新秩序为目标，依靠中俄战略联盟，整合金砖国家平台，首先在金砖国家内部形成初步的政策意向，以金砖国家名义向世界阐明对全球网络空间新秩序的认识，然后依托金砖国家平台，将全球网络空间新秩序提交联合国框架下的联合国教科文组织、国际电信联盟等机构展开讨论，通过联合国向全球发出建立、健全和完善网络空间全球新秩序的倡议，并最终推动各国共同签署相应的文件。



4. 产业配套

推进全球网络空间治理结构变革的核心与关键，是中国自身技术能力的实质性提升。这种提升，需要产业发展政策的配套，因为最终承担这一使命的是中国的企业。这里的企业既包括国企也包括民企。中国需要构建包括大型央企和民营企业在内的网络产业航母战斗群，以此增强中国提出自身网络治理方案的底气。