ISSN 1006-9550
CN 11-1343/F

国家社科基金资助期刊

世界经济与政治

WORLD ECONOMICS AND POLITICS

伊斯兰的国际体系观
刘中民

中国实现体系内全面崛起的四步走战略
张　春

小行为体与国际制度
魏　玲

国际关系中的大数据变革及其挑战
蔡翠红

中国社会科学院
世界经济与政治研究所　主办

2014 5
总第405期

SHIJIE JINGJI YU ZHENGZHI

1979 年创刊

2014 年 5 月 14 日出版

国际组织

全球治理

后斯诺登时代的全球网络空间治理*

沈　逸

【内容提要】　全球网络空间中，不同行为体之间占有的资源与拥有的能力处于不对称状态，因为这种不对称，数据主权的重要性日趋凸显。基于数据主权的能力竞争，已经成为当下国家间能力竞争的最前沿。这种竞争旨在实现保障国家网络安全和塑造全球网络空间行动准则这两个主要目标，这两者之间的关系，整体来看，是并行不悖的，尤其是对大国而言。推动这种竞争的主要驱动力来自体系层面，即全球生产力的深刻调整与变迁。因为如此，这种竞争的出现、发展和加剧都是无法避免的。只有从这一视角出发，各个行为体尤其是中国等新兴大国才能准确把握后斯诺登时代全球网络空间治理的核心任务，并形成与之匹配的整体性战略，探索并确立符合时代发展方向和需求的网络空间治理新秩序。在此过程中，包含网络空间关键基础设施、支撑技术与标准、核心资源等实际分配与有效使用等领域的全球网络空间治理体系的调整，将成为各国关注的核心领域，也将成为网络空间新秩序的主要组成部分。

【关键词】　数据主权；全球网络空间；网络安全；全球治理；信息战略

【作者简介】　沈逸，复旦大学国际关系与公共事务学院副教授，复旦大学金砖国家研究中心副主任。（上海　邮编：200433）

【中图分类号】　D815　G203　【文献标识码】　A　【文章编号】　1006-9550(2014)05-0144-12

* 感谢《世界经济与政治》杂志的匿名评审专家提出的建设性修改意见，文中错漏之处由笔者负责。

自 2010 年开始至今的四年多时间里，与互联网以及全球网络空间相关的议题迅速崛起，并逐渐从相对边缘的区域次第渗入到国际舞台的核心区域：2010 年维基揭秘网站与美国国防部、国务院展开了信息公开与国家安全的博弈，谷歌公司则试图挑战中国对互联网的主权管理；2011 年西亚北非局势发生动荡，奥巴马政府出台《网络空间国际战略》；2012 年到 2013 年有被渲染为美国国家安全的“中国网络间谍攻击”系列新闻和中情局前雇员爱德华·斯诺登（Edward Snowden）披露的“棱镜门”事件；2014 年美国修改国家安全局存储数据的构想浮出水面，突然宣布“放弃”对互联网名称与数字地址分配机构（ICANN）的“管理”，更是直接将网络空间与不同行为体之间的关系推上了风口浪尖。

如何正确认识和理解上述事件的含义，特别是从国际关系的视角理解上述变动对国家安全、国家间关系以及与各类行为体（包括国家与非国家行为体）密切相关的全球网络空间治理体系所带来的影响，显然有重要的理论价值与实践意义。在此发展变动的关键时刻，理解“数据主权（data sovereignty）”这个重要概念的含义，并以此构建分析、认识、理解问题的框架的起点，显然是非常重要的。

一 变动环境下的数据主权

自 20 世纪 60-70 年代至今，信息技术革命造就了一个几乎有效覆盖全球各地的网络空间，不同类型的行为体接入其中并从事日趋频繁、形式多样的信息生产、交换、传输、存储和处理等相关的活动。[①] 在 20 世纪 90 年代，互联网刚刚启动实质性的商业化进程没多久，有关网络技术发展与管辖能力、管辖权的微妙关系就引发了人们的关注。[②] 进入 21 世纪之后，随着“云计算”这一运用的兴起，“数据主权”的概念也逐渐引起了研究者的关注。“数据主权”概念的兴起，是以云计算为代表的互联网最新应用刺激的结果，也是自互联网诞生之日起就内嵌其中的技术特征与客观特点使然，其最主要的表现形式就是数据所有者、使用者、存储者在地理位置上的分离以及由此带来的权利/权力识别和有效行使的问题。[③]

---

① Yochai Benkler, “From Consumers to Users: Shifting the Deeper Structures of Regulation towards Sustainable Commons and User Access,” *Fed. Comm. LJ*, Vol. 52, No. 3, 1999, p. 561.

② Michael Marien, “New Communications Technology—A Survey of Impacts and Issues,” *Telecommunications Policy*, Vol. 20, No. 5, 1996, pp. 375-387.

③ Zachary Peterson, Mark Gondree and Robert Beverly, “A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud,” Proceedings of the 8th USENIX conference on networked systems design and implementation, 2011.

有学者指出，对数据主权的理解，其最主要回答的问题是数据的集中存储与分散的用户之间的权力博弈：不同个体能力的差异在没有显著的物理边界可供感知的网络空间中被进一步放大了，分散的用户如果不主张对数据拥有法律和政治意义上的权利/权力，则很难应对具备技术、资源、能力优势的数据存储方（通常来说是公司或者机构）对数据的不当运用。①

也有学者指出，可以通过提供更加有效的技术方案来解决上述分散的用户与集中的组织、机构之间的权力不平等问题。具体来说，这需要发展数据识别和追踪的相关技术，然后将此类技术和能力交给相关的个体，确保其能够有效地追踪并了解网络空间存储数据的使用情况。②

随着全球网络空间的形成，随着越来越多的人开始使用网络，根据国际电信联盟的数据，全球接入互联网的用户大概占全球总人口的30%-40%。有学者指出，网络空间自身的特定属性既为推动网络空间的权属界定和治理提供了便利条件，又提出了前所未见的全新挑战：网络空间最主要的特点是其无显著边界的空间属性。逻辑代码支撑的逻辑空间与线下某些规则确定的物理世界之间形成彼此接近但仍然有实质性距离隔阂的状态。而在这个特殊的空间里建立主权，而且是参考现实世界中的主权，正成为国家间竞争的新领域。③

尽管有学者指出，真正的“网络空间”其实是难以被准确地感知并管理的逻辑空间，但网络空间从没能够真正脱离物理世界而实际存续。对网络空间治理的难点之一就是如何在网络空间中凸显管理权限的存在，这种存在必须尽可能多地被各种行为体感知并认可。这种感知可以是对条文制度的感知，也可以是对网络空间某种间接存在的行为规范的感知。这种感知必然是主观和客观的密切结合，是行为体依据客观框架产生主观判断的结果。④

---

① Primavera De Filippi and Smari McCarthy, “Cloud Computing: Centralization and Data Sovereignty,” *European Journal of Law and Technology*, Vol. 3, No. 2, 2012, http://ejlt.org/article/view/101/234，登录时间：2014年4月10日。

② Marc Mosch, et al., *Automated Federation of Distributed Resources into User-Controlled Cloud Environments*, 2012 IEEE/ACM Fifth International Conference on Utility and Cloud Computing, 2012, pp. 321-326.

③ Kris Barcomb, Dennis Krill, Robert Mills and Michael Saville, “Establishing Cyberspace Sovereignty,” *International Journal of Cyber Warfare and Terrorism*, Vol. 2, No. 3, 2013, pp. 26-30.

④ Patrice Lyons, “Cyberspace and the Law: Your Rights and Duties in the On-Line World: Edward A. Cavazos and Cavino Morin. The MIT Press, Cambridge, Mass. 1994,” *Information Processing & Management*, Vol. 31, No. 6, 1995, p. 910.

大数据时代的来临加速了上述立法过程以及在网络空间树立主权的各种复杂行动。[①] 相比此前互联网经历过的那些发展，当下发生的最新变化就是网络空间的数据已经、正在而且还将持续转变成为一种战略资源，这一资源的分布与石油等自然资源存在显著差异，其使用方式和可能的获益也远比传统的资源要可观。[②]

数据的资源化发展又提升了网络空间治理的竞争。目前比较一致的共识是全球网络空间基本处于事实上的无政府状态。这种无政府状态是指至少在形式上不存在单一的对网络能够实施强制性管理的主体，不同的行为体都努力通过自己的实践来拓展自身在网络空间中的行动空间，以获得更多的行动资源，掌握并运用制定规则的权力，为自身的利益制定适用于一定范围的网络空间的行动准则。这种竞争在很大程度上构成了影响未来国际体系不同行为体彼此关系与地位的新型竞争的核心与关键所在。[③]

要更好地认识并理解这种网络空间正在出现并高速发展的新型竞争，就必须深刻认识当前全球网络空间的现状与主要特征。

二 全球网络空间呈现不对称性

20 世纪 90 年代至今，全球网络空间取得了快速发展，但这种快速发展造就的是其资源与能力的不对称分配：现实世界中的发展中国家并没有因为网络技术的发展实现在国际体系中位置或者是自身实际发展水平的跨越式流动，反而在网络空间中被进一步边缘化，进而还可能因为这种边缘化而固化其在现实世界中的位置。现实世界中的发达国家，尤其是产业能力和技术优势显著的发达国家，在网络空间中同样处于核心位置，并因为在技术研发与创新等诸多方面的显著优势，进一步拉开在现实世界中与发展中国家的差距。具体来说，这种资源与能力的不对称表现在如下两个方面：

第一，虽然网络用户群体的总量发生了显著变化，但不同类别国家之间的整体分布存在显著的差异。整体来看，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。根据国际电信联盟等相关机构的统计数据，全球网络用户的总数已经突破了 25 亿，在全球人口中所占比例将近 40%（参见图 1），而且从 2006 年开始，来

① Kris Barcomb, Dennis Krill, Robert Mills and Michael Saville, "Establishing Cyberspace Sovereignty," pp. 321-326.

② Brad Brown, Michael Chui and James Manyika, "Are You Ready for the Era of 'Big Data'," *McKinsey Quarterly*, Vol. 4, 2011, pp. 24-35.

③ Johan Eriksson and Giampiero Giacomello, "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State," *International Studies Review*, Vol. 11, No. 1, 2009, pp. 205-230.

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。

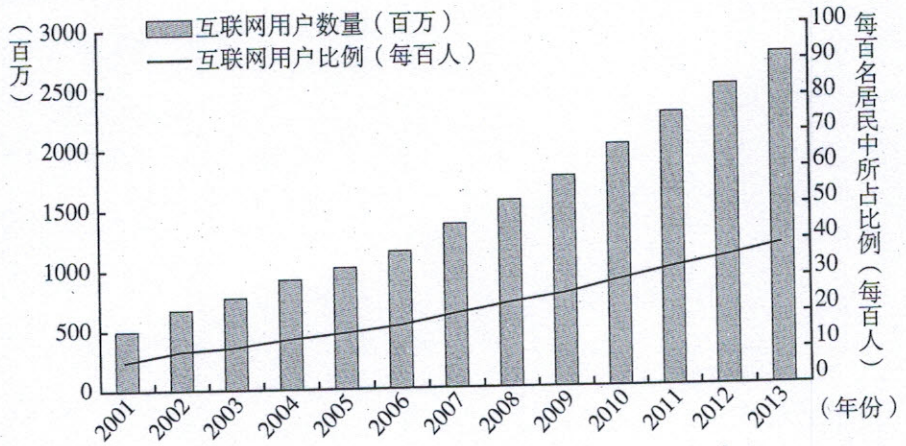

图1　全球互联网用户数量及比例(2001-2013年)

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

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%（参见图2）。

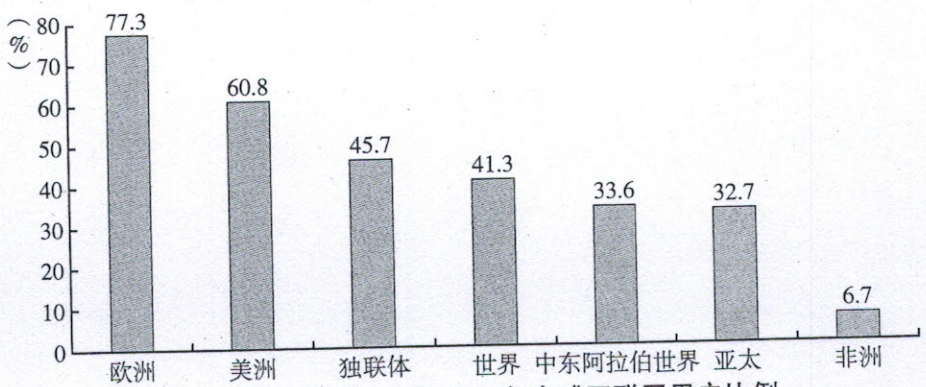

图2　根据地区划分的2013年全球互联网用户比例

资料来源：国际电信联盟通讯数据库，http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2012/stat_page_all_charts.xls，登录时间：2014年3月15日。

如图2所显示的，中东、亚太、非洲等地区与世界网络发展水平存在差距，其中非洲的差距特别显著。这种突出的差距主要是由非洲国家的发展程度所决定的：较低的

发展程度导致非洲国家普遍无法为民众提供足够的基础设施和接入设备，以满足民众使用互联网的需求。

第二，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。从那时开始一直到 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。有统计数据显示，2008-2012 年，总价 100 亿美元的新的海底光缆系统投入服务，平均每年 20 亿美元（或 53000 公里），其中的 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%。①

服务器是支撑全球网络空间的枢纽，通过观察世界服务器厂商所占的市场份额（参见表 1），我们可以发现，主要来自美国、日本的惠普、国际商用机器公司（IBM）、戴尔、甲骨文、富士五家公司占据了 2012 年全球市场份额的 84.7%，处于压倒性的优势地位。

表 1　全球前五位服务器系统制造商市场份额（2012 年第二季度）

厂商	2012 年第二季度市场份额
惠普（HP）	29.6%
国际商用机器公司（IBM）	29.2%
戴尔（DEll）	16.0%
甲骨文（Oracle）	6.0%
富士（Fujitsu）	3.9%
其他	3.9%

资料来源：IDC 全球服务器市场季度追踪，http://www.zdnet.com/server-sales-slow-but-dell-shows-growth-hp-ibm-tied-for-no-1-7000003427/，登录时间：2014 年 3 月 15 日。

通过观察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的基本信息（参见表 2），我们可以发现，13 台主根服务器分别归属 3 家美国公司、3

① *Submarine Telecoms Industry Report*, Submarine Telecoms Forum, Inc., 2013, http://www.terabitconsulting.com/downloads/2013-submarine-cable-market-industry-report.pdf，登录时间：2014 年 3 月 15 日。

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。

表 2　国际顶级地理域名主服务器基本信息及其管理者

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	威瑞信（VeriSign，Inc.）	美国（弗吉尼亚）
b. root-servers. net	192. 228. 79. 201	南加州大学（University of Southern California）	美国（加利福尼亚）
c. root-servers. net	192. 33. 4. 12	科进通信公司（Cogent Communications）	美国（华盛顿哥伦比亚特区）
d. root-servers. net	199. 7. 91. 13，2001：500：2d：：d	马里兰大学（University of Maryland）	美国（马里兰）
e. root-servers. net	192. 203. 230. 10	美国航空航天管理局（NASA's Ames Research Center）	美国（加利福尼亚）
f. root-servers. net	192. 5. 5. 241，2001：500：2f：：f	互联网系统协会有限公司（Internet Systems Consortium，Inc.）	美国（加利福尼亚）
g. root-servers. net	192. 112. 36. 4	美国国防部网络信息中心（NIC，DoD）	美国（弗吉尼亚）
h. root-servers. net	128. 63. 2. 53，2001：500：1：：803f：235	美国陆军研究实验室（Research Lab，US Army）	美国（马里兰）
i. root-servers. net	192. 36. 148. 17，2001：7fe：：53	瑞典互联网交换中心（Netnod）	瑞典（斯德哥尔摩）
j. root-servers. net	192. 58. 128. 30，2001：503：c27：：2：30	威瑞信（VeriSign，Inc.）	美国（弗吉尼亚）
k. root-servers. net	193. 0. 14. 129，2001：7fd：：1	欧洲网络资源协调中心（RIPE NCC）	英国（伦敦）
l. root-servers. net	199. 7. 83. 42，2001：500：3：：42	互联网域名与名称管理机构（ICANN）	美国（弗吉尼亚）
m. root-servers. net	202. 12. 27. 33，2001：dc3：：35	日本宽带项目（WIDE Project）	日本（东京）

资料来源：http：//www. iana. org/domains/root/servers，登录时间：2014 年 3 月 15 日。

从某种角度来说，在当今的全球网络空间中，发展中国家主要提供使用者，发达国家主要提供基础设施与关键应用，这一新的“中心-外围”架构已经初见端倪。这种具

有显著不对称性的架构,加剧了发达国家与发展中国家之间甚至发达国家之间本来已经存在的能力差异。这种能力是当下国家间竞争的新焦点,主要包含保障国家网络安全以及塑造全球网络空间行为准则两个方面。2013 年引发全球轰动的“棱镜门”事件,就是非美国本意地展现出这种能力的典型案例,人们由此看到的是未来大国网络空间博弈的冰山一角。

三 美国网络安全战略进攻性凸显

直到2013 年之前,关于美国国家网络安全战略的特性始终存在某种争议。但“棱镜门”事件的出现,使人们充分看到了美国国家网络安全战略的显著特征,即进攻性。

2013 年 6 月 6 日,《美国华盛顿邮报》刊载了题为《美国情报机构的机密项目从九家美国互联网公司进行数据挖掘》的文章,披露美国国家安全局从 2007 年开始执行代号为“棱镜(PRISM)”的信号情报搜集行动。该行动的信号情报活动代号(SIGINT Activity Designator,SIGAD)是 US-984XN。在 2012 年美国总统阅读的每日情报简报中,有 1447 项的引用来源指向了 US-984XN,因此,媒体报道中将“棱镜”称为美国国家安全局最重要的情报来源。在美国情报界,“棱镜”是政府内部使用的非机密活动代号,US-984XN 是情报界正式使用的机密代号。根据规定,信号情报活动意味着拥有相对独立的信号情报搜集站点(比如一个固定的基地)的情报活动。

“棱镜”项目具体开始实施的时间是 2007 年。布什政府通过并签署《保护美国法》以及 2008 年修订了《对外情报监听法》之后,“棱镜”项目开始投入使用,并一直处于美国对外情报法庭的管理之下。“棱镜”项目的基本思路是通过对网络数据的大范围监控,来搜集各种相关情报。

综合已经被公开的相关资料可以发现,“棱镜”系统的本质就是一个超大规模的数据系统,包含了近乎覆盖全网的数据流搜集、存储、分类以及检索功能,具备存储 ZB(万亿 GB)级别数据的能力,并且能够对音频、视频等非结构性的海量数据进行实时快速的分类查询。这是美国国家战略能力在网络安全领域的系统体现,而非一个单一的项目或者是个案。这种能力表现为有效保障国家网络安全的协调-整合能力。最突出的表现就是美国政府与公司之间微妙复杂的长期关系。这种关系并不是从“棱镜”项目才开始存在的,其历史可以被追溯到 1947 年至 1973 年互联网正式诞生之前的“三叶草行动(Project Shamrock)”。美国国家安全局与西联汇款、美国电报公司、国际电报公司等三家企业合作,在将近 30 年的时间里对所有打入和打出美国的国际电

报进行了实时监听,这种监听在20世纪60年代达到顶峰。①

“棱镜”系统的正常运作至少涉及九家巨型互联网公司(谷歌、微软、雅虎三家占据其中90%以上数据来源)、四个美国情报机构(联邦调查局、中央情报局、国家安全局、国家情报总监)以及十套子系统(“打印光环”、“交通贼”、“剪刀”、“协议开发”、“余波”、“码头”、“主路”、“针鲸”、“运输工具”以及“核子”)。

谷歌、微软、雅虎等网络公司是“数据提供者”,它们的数据直接提交到美国联邦调查局数据拦截技术单位(The FBI Data Intercept Technology Unit),该单位位于弗吉尼亚州的匡蒂科(Quantico),此地同时也是美国海军陆战队网络部队基地的所在地。

综合协调不同类型的行为体,共同保障美国国家网络安全的政府战略能力,至此表露无遗。由此可以将“棱镜”系统看做是美国奉行的进攻性网络安全战略最为集中、也是最具代表性的体现。凭借自身压倒性的技术与实力优势,美国建立了全球范围内最大、最全面、最复杂的网络空间监控系统,而强大的自身能力自然而然地就投射到了国际网络空间,塑造了美国谋求并尝试在全球网络空间确立压倒性霸权优势的内在战略冲动,这种冲动在冷战结束之后始终存在。②面对这种网络空间战略,简单的批评和否认难以得出可行的战略选择,因为这种战略赖以成长的土壤是其他所有国家尤其是亟须从网络技术及其应用的发展中获得收益的新兴大国,无法脱离其中而存在的全球网络空间。试图通过切割乃至倒退到没有全球网络空间的时代去保障单一行为体自身的安全利益同样是不可取的,因为这将在其他领域对国家安全造成更加严重的不便与伤害。只有直接面对这种挑战才有可能探索到一种真正能够有效实施的后斯诺登时代的全球网络空间治理之路。

在当下的世界,“棱镜”系统的披露引发了全球对网络空间治理的关注,而这种关注有可能催生出一套新的网络空间治理生态系统。③ 通过有效保障数据主权,确立有别于美国的霸权战略,同时又符合网络空间发展客观需求的网络空间治理新模式,可能是唯一有效的解决方案。

---

① Dougald McMillan, *Report on Inquiry into CIA-Related Electronic Surveillance Activities*, Department of Justice, June 30, 1976, pp.26-28, pp.32-36, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/surv09a.pdf,登录时间:2014年4月5日。

② Barry Posen and Andrew L. Ross. “Competing Visions for US Grand Strategy,” *International Security*, Vol.21, No.3, 1996/1997, pp.5-53.

③ Joe Waz and Phil Weiser, “Internet Governance: The Role of Multistakeholder Organizations,” *Journal on Telecommunication & High Technology Law*, Vol.10, No.2, 2013, pp.331-344.

四 以数据主权重塑网络空间治理

2014 年 3 月，在“棱镜”系统曝光之后明显感受到巨大压力的美国政府，宣布将放弃对互联网名称与数字地址分配机构的监管，并承诺将尽快把管理权移交给一个遵循“多边利益相关方(multi-stakeholder)”组建的私营机构。① 这一表态很快引发了各方的热烈回应和讨论，因为这是自 2005 年联合国全球网络工作组出台报告指出“国际域名系统”根区文件和系统“事实上处于美国政府单边控制之下”②以来，全球除美国之外的行为体获得的最佳的塑造网络空间治理生态系统的战略之窗。在此过程中，考虑到美国强调的“多边利益相关方”模式短期内无法被实质性地改变，那么如何在“多边利益相关方”的既定框架内找到能够让那些技术上处于相对弱势的行为体有效维护自身“数据主权”的实践模式，会成为各方博弈的关键所在。

所谓“多边利益相关方”，是美国在 20 世纪 90 年代推进互联网商业化进程中采取的一种运作模式。它将公司、个人、非政府组织以及主权国家都纳入其中，最高决策权归属于由少数专业人士组成的指导委员会，相关的公司、个人、非政府组织在下属的比较松散的区域或者专业问题委员会开展工作，政策制定采取所谓“自下而上”的模式，由下级支撑委员会向指导委员会提出建议和草案，然后指导委员会决定是否通过。其他主权国家的代表则被纳入政府建议委员会，只具有对和公共政策以及国际法等相关的活动或者事项的建议权，而没有决策权，其建议也不具有强制力。③ 一般研究认为，这种模式对掌握有压倒性技术优势的一方，也就是美国最为有利。因为这种开放模式最有助于美国在网络空间的扩张，有研究者直接将其比喻为在网络空间实施的“门户开放”政策。④

需要指出的是，虽然美国政府在涉及全球网络空间治理时基本不使用数据主权这种与主权相关的概念来描述其政策，这是因为美国自身的技术能力足以自保，不存在

---

① NTIA, “NTIA Announces Intent to Transition Key Internet Domain Name Functions,” http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions, 登录时间：2014 年 4 月 15 日。

② Chateau de Bossey, *Report of the Working Group on Internet Governance*, Secretariat of the Working Group on Internet Governance, 2005, http://www.wgig.org/docs/WGIGREPORT.pdf, 登录时间：2014 年 4 月 15 日。

③ Lennard Kruger, *Internet Governance and the Domain Name System: Issues for Congress*, Congressional Research Service, Library of Congress, 2013, http://www.fas.org/sgp/crs/misc/R42351.pdf, 登录时间：2014 年 4 月 23 日。

④ Ryan Kiggins, “Open for Expansion: US Policy and the Purpose for the Internet in the Post-Cold War Era,” *International Studies Perspectives*, Vol.14, No.3, 2013, pp.1-20.

显而易见的对美国数据主权的实质性威胁。事实上，根据2011年颁布的《网络空间国际战略》，当美国的数据主权遭遇威胁时，比如，当关键基础设施遭到网络袭击时，美国的构想是可以使用包括精确制导武器在内的一切手段进行反击。美国只是不希望其他国家运用数据主权这种观念武器来构建阻挡美国网络霸权扩张的壁垒，而不是真的不关注数据主权。美国看好“多边利益相关方”这个概念，关键也在于它认定在此概念下，即使美国政府“放弃”了对互联网名称与数字地址分配机构的“监管”，仍然有可以弥补的方式：美国公司可以凭借自己的优势确保自己在任何新组建的“多边利益相关方”机构中占据压倒性优势，而美国公司总是要遵守美国法律管辖的。这是一种更加间接和隐蔽的方式，以更低的成本有效地实现美国国家网络安全战略。

对于美国之外的其他国家来说，在后斯诺登时代的全球网络空间治理问题上，可选择的战略不多：

第一种是无条件的追随，也就是选择无条件地认可美国的霸权战略，认可美国对自身技术优势的滥用并对美国政府的意图保持无条件的信任。也就是坚信美国政府会如其所宣称的那样，仅仅从国家安全、反恐的角度来使用自己的技术能力，而不会将其用于商业领域展开不对称的竞争。这种战略选择或许是美国的决策者们所喜闻乐见的，但早在2001年，欧盟议会组建的调查小组就指出，美国早就有滥用这种能力的先例，其可信度相当成问题。①

第二种是强硬的对抗，为自身的安全设定一个绝对标准，为此不惜支付巨大的代价，包括在网络空间重现冷战那种阵营对抗，在必要时架设一整套与现有全球网络空间平行的网络（包含基础设施管线在内且与现有网络严格意义上物理隔绝）。在斯诺登以任何人都无法否认和主观阐释的方式披露“棱镜”项目存在之后，这种设想也有浮出水面的态势。不过考虑到其巨大的经济代价和与当今世界整体经济、社会活动方式截然相反的内在思维逻辑，就足以将这种设想排除出其他国家可供选择的菜单之外了。

第三种是从“治理谋求安全”的思路出发，依托“人类共同遗产”原则，通过新兴大国之间的战略协调，凝聚和团结具有相同处境的国家（比如技术能力相对弱小，对网络空间存在高度依赖，但又担忧来自美国滥用自身霸权优势的发展中国家），在此过程中找到强化合作的战略契机。

---

① *Report on the Existence of a Global System for the Interception of Private and Commercial Communications*, European Parliament, Temporary Committee on the ECHELON Interception System, July 11, 2001, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN，登录时间：2014年4月23日。

这种战略契机的主要目标是以数据主权为核心，建立一套具有诱惑力的开放的网络空间治理生态系统，在动态开放、对等安全、有序发展的基础上追求全球网络空间治理质量的提升。在此过程中，仍然需要回答一系列艰巨的问题：

首先，如何在美国政府“放手”之后，有效制约并监管那些实质性掌控关键基础设施/资源的私营公司，比如美国的威瑞信。美国政府希望这类公司填补美国政府“放弃”管理带来的真空，而如果是通过强化主权管理的方式进行制衡，也就是试图用联合国这种政府间国际组织去监管，美国政府会毫不犹豫地停止放权过程并重新强化管理。这意味着其他国家必须寻找到具有足够能力的非国家行为体，包括公司或者是私营机构，尽快尝试去争夺填补美国留下的管理真空，用创新而非传统的方式来维护、保障和实现各国的数据主权。

其次，如何在更加广泛的全球网络空间治理体系中，将数据主权作为一项原则纳入其中并有效地加以体现？数据主权不是要以主权原则来阻滞数据、信息的高速流动，而是要借助强调主权之间的平等性，为那些暂时在技术能力上处于弱势的行为体保留其应得的从网络空间发展中获益的权利和可能，确保网络技术的均衡发展，全球网络空间的拓展以及最终确立的网络空间的治理秩序，能够让不同技术能力的个体享有同等收益的机会和可能。

最后，如何在除了互联网名称与数字地址分配机构之外的其他机构，比如互联网工程师任务组（IETF）等更加关键地掌握了全球网络空间关键技术与技术标准的组织中，也推动能够反映数据主权原则的改革、建设相应的治理新秩序？互联网工程师任务组目前成员超过 1000 人，但核心的提名委员会（NomCom）只有 15 名成员构成，其中包括 10 名有投票权成员以及 5 名非投票权成员，这 15 人中 90% 来自欧美国家的工程师或者技术管理人员，发展中国家的技术人员只有成为欧美公司的高层主管才能进入这个高端的技术俱乐部。就中国来说，加入 IETF 的中国工程师已经超过 30%，但被接纳的技术提案只有总量的 1%，治理结构与现状之间的脱节与不匹配显而易见。

随着时间的流逝、白宫的危机公关以及强调政治正确的西方主流媒体的自我审查，斯诺登与“棱镜门”事件带来的直接冲击必然呈现梯度下降的趋势，无视或者仅仅从“双重标准”的视角展开批判，本质上都于事无补。真正需要的是以此为契机提出基于数据主权保障的网络空间治理机制的新主张，从目前的发展态势看，这个窗口不会敞开太长时间，中国必须迎头赶上，为建设信息强国而努力奋斗。

（截稿：2014 年 4 月　实习编辑：冷鸿基）

世界经济与政治

2014年第5期

（1979年创刊·月刊）

第三届中国出版政府奖期刊提名奖

中文核心期刊（国际政治类）

中国人文社会科学核心期刊

RCCSE中国权威学术期刊

中文社会科学引文索引来源期刊

中国期刊全文数据库来源期刊

CNKI（2013）中国最具国际影响力学术期刊

刊号：ISSN 1006-9550 / CN 11-1343/F

邮发代号：82-871

定价：30.00元（国内）

25.00美元（国外）

国内外公开发行

World Economics and Politics

No.5 (2014) (Monthly, Began in 1979)

Compiler: Editorial Department of the Journal of World Economics and Politics (5 Jianguomennei Dajie, Beijing)

Postal Code: 100732

Telephone: 85195784

E-mail: sjzbjb@cass.org.cn

http://www.iwep.org.cn/

Editor-in-Chief: Zhang Yuyan

Publisher:World Economics Journal Publication Office

Printer: Beijing Jifeng Printing Co. Ltd

Distributor: Beijing Press Distribution Bureau

Subscriptions:

Domestic: Post Office

Overseas: China International Book Trading Corporation (Box 399, Beijing 100044, China)

Subscription Price: $ 25.00 (overseas)

￥30.00 (domestic)

ISSN 1006-9550

05

9 771006 955144