国家的“浮现”与“正名”

——网络空间主权的层级理论模型释义

杨　帆*

摘　要：网络空间是人为构建的技术空间，网络治理必须充分考虑技术逻辑。为了理解晚近国家在网络空间中作用增强、不断“浮现”的态势，需要结合网络空间生成演进历程及网络通信基本技术过程，构建网络空间的层级理论模型。根据该模型，网络空间相关议题可被拆解到意义层、内容层、应用层、协议层、硬件层和网络层等六个不同层级进行具体研判。在层级模型的检视下，“全球网络公域”的主张在除协议层之外的其它层级均无法有效成立；基于各国在意义层通常难以调和的抵牾、以及在以网络层为代表的其它层级所能实现的治理能力，网络空间主权有生成的必要性和实现的可行性。囿于其底层技术逻辑的先决性限定，网络空间不太可能完全“再主权化”，而“网络空间版主权原则”也将以其独特方式塑造法律秩序。

关键词：网络空间　层级理论模型　全球网络公域　网络空间主权

网络及其丰富应用已经与日常生活的方方面面深度交织，以至于人们通常很难意识到，互联网雏形首次在实验室诞生以来只不过短短 50 余年的历史，而如果从网络放开限制、被大规模民用和商用开始起算的话，这个历史跨度还要再缩减一半。①

网络技术的急速勃兴与更迭势必引发剧烈社会变迁，进而造成一个尚未结束的思想混乱、观点碰撞的过渡期。其中一个被广泛辩论的核心问题是：国家在网络治理中应扮演何种角色、发挥何种功用。对此，具有不同利益诉求的各类网络行为体依凭着各异的理由，均试图树立和维护那种他们认为“本应如此”、但实际上只是最有利于其自身的立场主张，例如：技术精英和网络朋克们希望网络空间是“独立领地”和“法外净土”，不应受到以国家为象征的世俗公权力的侵入；② 大型互

---

* 法学博士，厦门大学法学院国际法教研室助理教授。本文系 2017 年度教育部哲学社会科学研究重大课题攻关项目“大数据时代个人信息保护边界与策略研究”（17JZD031）的阶段性研究成果，并受到“中央高校基本科研业务费专项资金”（0130 - ZK1074）的资助。

① 参见杨吉：《互联网：一部概念史》，清华大学出版社 2016 年版，第 60—63 页。

② 历史曾经为诸如约翰·巴洛（John Barlow）之类的互联网朋克以及诸如乔恩·波思泰尔（Jon Postel）之类的技术精英提供了论辩和布道的舞台，他们热切地期望网络空间能够成为“独立领地”和“法外净土”，与传统的现实社会断绝一切治理意义上的关联。《网络空间独立宣言》不仅描绘了对这种乌托邦世界的幻想，甚至还表达了对于网络自治实现路径的乐观预期。See John Barlow, *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation, Davos Switzerland, February 8 1996.

联网企业希望网络空间是没有边境的公共领域，是真正的世界级自由市场，以便它们的网络产品和服务能够无远弗届、无孔不入、无利不盈;① 网络技术先发国家希望网络空间是拒绝继受主权观念的虚拟位面，并极力主张“全球网络公域”的观念，以便其能够最大限度发挥网络技术优势而免于受到其它国家的指摘和阻挠;② 网络技术后发国家则倾向于主张网络空间是现实世界的延伸，作为世界秩序基石的主权国家体系也应当在网络空间中得到某种程度的投射。③

诸多关于网络空间的国际法研究也部分反映了这些矛盾主张。例如，苏珊·布伦纳（Susan Brenner）即认为，网络时代的各种“威胁”形式已经脱离了传统时代的“地域性”特征，基于主权格局的治理范式无法延用。④ 而杰克·戈德史密斯（Jack Goldsmith）与蒂姆·吴（Tim Wu）在其合著中指出，尽管在互联网发展早期人们认为“领土政府在消融”,⑤ 但是随着国家实体在网络空间逐渐谋求并成功确立其主导地位，网络空间呈现出越来越明显的“威斯特伐利亚化”特征。⑥

晚近，作为网络空间国际治理规则化的代表，《塔林手册 2.0》第一章关于“主权”的规定明确了“国家主权原则适用于网络空间”。⑦ 尽管如此，关于网络空间法律秩序的既有讨论基本都忽视了网络空间的底层技术逻辑，而这种缺失又将在一定程度上影响有关论点和主张的说服力。⑧ 本文即尝试构建一座从技术逻辑到法律秩序的理解桥梁——因为一个对网络空间法律秩序有解释力的理论模型，必须能够契合网络空间行为的基本技术过程。

全文的逻辑展开如下：国家作为传统管制者，事实上已经“浮现”成为网络空间治理实践的重要主体；通过深入剖析网络空间的场域特性及其治理演化进程，充分结合网络通信的基本技术过程，有望构建网络空间的层级理论模型，并以此对国家在网络空间治理中的介入提供理论支持，为其“正名”；文章最后提出若干有关网络空间主权及其基本法律秩序的推论。

---

① 例如：2016 年《中华人民共和国网络安全法（草案）》公布时，全球 40 多个互联网企业商业团体曾集体致信中国政府，对草案中要求关键信息基础设施重要数据本地化储存的规定提出抗议，认为此规定会损害在华外企利益，可能构成事实上的投资准入壁垒，并呼吁中国政府重新考虑相关“争议条款”。参见《外媒呼吁中国网络安全法重新考虑“争议条款”》，环球国际新闻网，http://oversea.huanqiu.com/article/2016-11/9650005.html，最后访问时间：2018 年 7 月 7 日。

② 例如：2005 年美国国防部发布的《国土防御和民众支持策略》中明确宣称“全球公域由国际水域、天空、外空以及网络空间构成”；2010 年时任国务卿希拉里在其关于网络自由的演讲中也提到“全球互联公域”，see Hillary Rodham Clinton, “Remarks on Internet Freedom”, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (last visited July 7, 2018).

③ 例如：早在 2010 年 6 月，中国国务院新闻办就曾发布《中国互联网状况》白皮书，认为互联网是国家重要基础设施，中华人民共和国境内的互联网属于中国主权管辖范围，中国的互联网主权应受到尊重和维护。其后，2015 年 12 月 16 日，中国国家主席习近平在第二节世界互联网大会上代表中国政府向全世界提出共同构建网络空间命运共同体的主张，并提出了推进全球互联网治理体系的四项原则，作为其中的首要原则，“尊重网络主权”得到重申。2017 年 6 月 1 日，经由全国人大常委会通过的《中华人民共和国网络安全法》正式实施。作为我国第一部统筹网络空间安全的管制性法律，该法继续延用了中国政府在诸多政策文件或会议发言中所一贯主张的“网络空间主权”概念。

④ Susan Brenner, *Cyber Threats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009), pp. 8-10.

⑤ Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006), p. 27.

⑥ See Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006), pp. 183-184.

⑦ 〔美〕迈克尔·施密特主编：《网络行动国际法：塔林手册 2.0 版》，黄志雄等译，社会科学文献出版社 2017 年版，第 57—72 页。

⑧ 这或许是因为学科壁垒使然：擅长于讨论秩序问题的法律学者，往往缺乏深入理解网络技术的必要知识背景。

一 从“法外之地”到国家“浮现”：网络空间的“巴尔干化”

与现阶段网络空间所呈现的“巴尔干化”景象相去甚远，[①] 互联网最初被创造的直接目的是为了应对在想象中因核武器攻击导致的通信瘫痪，其核心目标是实现强固的连接（robust connection）和稳健的信息传输。因此，按照保罗·巴兰（Paul Baran）在1964年提出的设想，网络架构采用了去中心化的分布式设计。[②] 这在技术底层逻辑上就决定了，互联网给人的第一观感通常是一个可以在世界范围内共享的、没有“边界”和“国境”概念的虚拟空间。

但是，由于其封闭、小众的特性，初代互联网的范围实际上仅局限于实验室的有限空间之中，它所连接的网络技术专家们所构成的也只是一个“熟人社会”，因此早期互联网架构师们完全没有关注网络安全问题的必要。在这方面，一个如今看来可能令人无法想象的例证是：在1998年“国际互联网名称和编号分配公司”（简称ICANN）成立之前，互联网上的域名管理权限基本上是由当时南加州大学的乔恩·波思泰尔（Jon Postel）教授个人来行使。[③] 然而，随着互联网的发展，陌生人之间相互连接的机会越来越多，因此可能产生的社会联系也越来越复杂，网络安全的需求就变得越来越突出和不容忽视。如果缺乏公认威权和有效管制，网络空间将极有可能上演霍布斯所描述的“所有人反对所有人的战争”的“自然状态”。[④] 而在传统环境下相对力量处于劣势的行为体，却有机会在网络空间获得不对称的技术能力；这种能力一旦以一种恶性方式反作用于现实世界，势必会加剧“自然状态”中的敌意对立。[⑤]

正是这种深层需要和客观事实、而不是浪漫想象和主观立场，决定了国家必然会寻求其在网络空间治理中的权威地位。事实上，晚近各国都争相发布自己的网络空间安全战略并积极进行网络管制立法，即意为确立其在网络空间中的管辖“地盘”和法理依据。这也造就了网络空间“巴尔干化”的现实状态。[⑥] 一些国家通过硬件层面运行的国家级网络防火墙，不仅划分出信息

---

① “网络巴尔干化”一词首先见于Alstyne & Brynjolfsson在1997年发表的论文中。See Marshall Alstyne & Erik Brynjolfsson, “Electronic Communities: Global Village or Cyberbalkans”, http://web.mit.edu/marshall/www/papers/CyberBalkans.pdf (last visited July 7, 2018).

在英文语境中，网络空间的巴尔干化通常表述为cyber-balkanization或者internet balkanization，人们还用splinter（分裂）和internet（因特网）专门创造了一个合成词来描述这种现象，即splinternet（分裂网）。此合成词由卡托（Cato）研究所技术研究主任、自由主义智库专家克莱德·韦恩·克鲁斯（Clyde Wayne Crews）在2001年4月2号的《福布斯》杂志中首先提出，但他是从一种积极的意义上使用这个术语，用来指称一种为了降低网络空间“交易成本”而进行的明晰产权的思路。See Aparna Kumar, “Libertarian, or Just Bizarro?”, https://www.wired.com/2001/04/libertarian-or-just-bizarro/ (last visited July 7, 2018).

② 参见杨吉：《互联网：一部概念史》，清华大学出版社2016年版，第2—5页。

③ See Kristen Eichensehr, “The Cyber-Law of Nations”, (2015) 103 *The Georgetown Law Journal* 317, p. 349.

④ 参见〔英〕霍布斯：《利维坦》，黎思复、黎廷弼译，商务印书馆1985年版，第134—138页。

⑤ 黑客即是这方面的一个典例。

⑥ 例如包括：美国在2008年小布什当政时期通过的《综合性国家网络安全倡议》（Comprehensive National Cybersecurity Initiative）、以及2016年2月奥巴马当政时期发布的《网络安全国家行动计划》（Cybersecurity National Action Plan）；中国国家互联网信息办公室于2016年12月27日发布的《国家网络空间安全战略》；英国政府于2016年发布的《国家网络安全战略2016—2021》（National Cyber Security Strategy 2016－2021）；澳大利亚政府于2016年4月发布的《澳大利亚网络安全战略》（Australia's Cyber Security Strategy）；新加坡于2016年发布的《新加坡网络安全战略》（Singapore's Cybersecurity Strategy）。关于2017年全球网络安全立法的简明梳理，可以参见黄道丽：《全球网络安全立法态势与趋势展望》，载《信息安全与通信保密》2018年第3期，第54—60页。

空间的边界，而且还能过通过代码进行有效的信息进出口控制；更多的国家则通过各种措施力图对网上的政治内容进行过滤、审查其中的仇恨性语言和种族极端主义内容。而或许最有说服力的情形是：尽管在很多国家的网络安全战略规划中没有明确用到“网络空间主权”这个词，但是这些战略文件不约而同的核心主张都是维护本国的网络安全，组建防御性力量，甚至构建具备打击能力的威慑性力量或报复性力量。显然，网络空间的这种“军事化”倾向本身就是一种划分界限、区分“敌我”的举措。

值得一提的是，这种网络空间的“巴尔干化”现象也得到了计算机建模预测的理论支持。澳大利亚国立大学国家安全研究院罗杰·布拉德伯里（Roger Bradbury）教授团队对网络空间环境下的行为体演化进行了计算机建模并且发现，在环境刺激（通常是安全威胁）和对此刺激做出反应的综合作用之下，网络空间中的行为体会自发集结、重组，而在这些重组后的簇拥状结构的中心，则是那些有能力提供安全保障的行为体（例如国家）。①

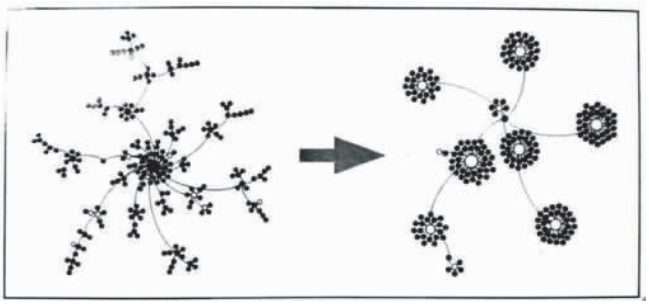

图 1　网络空间“巴尔干化”的计算机建模演示②

说明：本图例通过 10 个类国家节点和 200 个非国家节点对网络进行简单模拟。根据各节点的“偏好连接”，这个网络首先形成一个无尺度网络（图中左边所示网状结构）。随着类国家节点对网络系统中的威胁进行回应和过滤，各节点的连接会被增强或重塑。通过大约 15000 次迭代，该网络演化成为稳定的巴尔干化网络（图中右边所示网状结构）。图中的空心圆圈用于模拟类国家节点，实心圆圈用于模拟非国家节点，节点半径大小同附着于它身上的节点数量成正比。

但是，作为一种实证观察，网络空间中国家“浮现”的现实态势并不具备过多的思辨意义。如何理解这种现实态势、并构建自洽的逻辑模型对国家在网络空间中的“浮现”提供“正名”，才是真正的理论挑战。为此，本文将首先针对已被魅化为宏大叙事的“网络空间”概念进行追本溯源，进而尝试构建契合网络通信基本技术过程的理论模型作为开展后续讨论的框架。

二　网络空间的生成演进及其层级理论模型

（一）从平面网络到虚拟社会：网络的维度崛起

得益于硬件按照“摩尔定律”维持增速、软件按照“安迪——比尔定律”不断提升、以及

① See Rodger Bradbury *et al.*, *Strategy and Statecraft in Cyberspace: Research Program Guide*, National Security College, Australian National University, February 2016, pp. 3 – 4.

② Rodger Bradbury *et al.*, *Strategy and Statecraft in Cyberspace: Research Program Guide*, National Security College, Australian National University, February 2016, p. 4.

资本和人才的疯狂投入,[①] 互联网在其基础设施、终端设备、连接形式、操作系统和软件应用等各个方面均获得了全方位的迅猛发展，人类社会快速完成了从“PC 互联网”到“移动互联网”的过渡,[②] 并正处于向“万物互联网”的整体转型进程当中。[③]

持续升级的互联网类型，不仅仅只是意味着“更多的设备连上了互联网”，在这个过程中积累的量变已经引发了质变。[④] 随着网络的覆盖面越来越广，接入点越来越多，传输速度越来越快，交互的信息越来越丰富，交互的频率越来越密集，互联网实际上已经从以“联（接）”为主的初级平面形态，转型成为以“互（动）”为主的当代立体形态,[⑤] 互联网的节点自组织化倾向和平台去中心化特征也愈发突出。在这个趋势下，作为信息中枢曾经一度风靡的门户网站几近消亡，扁平的网络使得终端节点可以自由通过搜索入口筛选并对接海量信息，自行发起组建各种规模的社交网络进行沟通或协作，在平台上自主浏览商品信息和商业机会并在线决策交易。在这个基础上，以终端用户为核心的搜索、社交和电商的互联网应用以惊人速度迭代进化，用户得以在网上完成丰富而复杂的频繁互动，促进其“线下真实存在”与“线上虚拟存在”深度绑定。

正是因为对于这些社会行为和社会关系的容纳，平面网络的第三维度逐渐得以崛起和确立，使得互联网真正成为名符其实的“网络空间”，虚拟社会和现实社会开始并驾齐驱但又相互交织，逐渐融汇构成一种“立体社会”，进而使各种社会关系也得以被包容其中。

---

① “摩尔定律”由英特尔创始人之一戈登·摩尔提出，其内容为：当价格不变时，集成电路上可容纳的元器件的数目，约每隔 18—24 个月便会增加一倍，性能也将提升一倍。“安迪——比尔定理”是对 IT 产业中软件和硬件升级换代关系的一种非正式概括，用于表达“硬件的性能提升将很快被软件消耗”，其原话是“Andy gives，Bill takes away.”（安迪提供什么，比尔就拿走什么）。其中，安迪指英特尔前 CEO 安迪·格鲁夫，比尔指微软前任 CEO 比尔·盖茨。

② 以中国为例，根据中国互联网络信息中心（CNNIC）的统计，截至 2017 年 12 月，手机网民占 97.5%，移动互联网成为人们学习、工作、生活的新空间。参见 CNNIC：《第 41 次中国互联网络发展状况统计报告》，http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201803/P020180305409870339136.pdf，最后访问时间：2018 年 7 月 7 日，第 22 页。

③ 物联网的蓬勃发展可以从 2017 年 9 月 10 日至 13 日在中国无锡召开的“第七届世界物联网博览会”得到一定程度的印证；会上阿里巴巴集团创始人马云还做了题为《物联改变未来》的演讲。参见物博会官方网站：http://www.wiotexpo.cn/，最后访问时间：2018 年 7 月 7 日。

④ 知名互联网观察家凯文·凯利对互联网下一阶段发展的“量变到质变”做了形象而深刻的描述：

用玻璃、铜和电磁波组成神经，人类这个物种开始将所有的地区、过程、人口、人工制品、传感器、事实和概念编织成一张复杂到难以想象的巨网……最初看来，这个规模巨大、无处不相连的新平台就像我们传统社会的自然延伸。它似乎只是在已有的面对面的关系中加入了虚拟关系——我们只是在网上加了几个好友，扩大了朋友圈，增加了新闻的来源，让我们的行动更加数字化。但事实上，就像温度和压力慢慢升高，当这些事情持续稳定地发展，我们会到达一个拐点，或是一个复杂的临界点，在这里，变化是不连续的。于是相变发生了——我们会突然处在全新的阶段。那是一个具有新常态的不同世界。

参见：〔美〕凯文·凯利：《必然》，周峰、董理、金阳译，电子工业出版社 2016 年版，第 333，336—337 页。而这种“密集连接的量变最终引发质变”的判断背后，实际上可能存在一种自然逻辑发挥作用，即所谓复杂系统的自组织趋势和功能涌现趋势。复杂性思想自上世纪 60 年代进入交叉学科研究的视野以来，迅速地成为与基础物理学和还原论相对立的逻辑体系，并且在诸如昆虫群落、免疫系统、脑神经网和经济体等复杂巨系统的研究中，提供了客观而有力的解释。有关复杂性学科引人入胜的科普介绍，可以参见：〔美〕米歇尔·沃尔德罗普：《复杂：诞生于秩序与混沌边缘的科学》，陈玲译，生活·读书·新知三联书店 1997 年版；或者〔美〕梅拉妮·米歇尔：《复杂》，唐璐译，湖南科学技术出版社 2017 年版。

⑤ 参见于志刚：《网络安全对公共安全、国家安全的嵌入态势和应对策略》，载《法学论坛》2014 年第 6 期，第 5—19 页。沿着这种概括逻辑可以展望：以“智能”为主的下一级网络形态已经初见端倪，而且它将对我们已知社会结构和生活方式的方方面面产生无比深刻的影响。鉴于其复杂性和重要性，在本文的篇幅和框架内无法对“智能网”进行详细讨论。

（二）从“对象”“工具”到“空间”：网络的性质拓延

借鉴于志刚在其关于“网络在犯罪中的地位演变”的论述中选用的“犯罪对象”“犯罪工具”和“犯罪空间”三种意向，[①] 本文认为：与互联网在客观层面上从平面网络到虚拟社会的维度崛起过程相适应，就主观层面上人们对于互联网的普遍理解而言，也经历了从“对象”“工具”到“空间”的性质拓延。

在其“襁褓期”，互联网常常被单纯视为技术意义上研究或建设的“对象”。虽然当时的主要资助方是美国政府（具体而言是国防部），但是互联网项目的第一代研究人员——同时也大多是互联网的最初使用者——的工作环境十分宽松。[②] 做一个不特别恰当的类比，初代互联网就像技术精英们的实验创造物，面对这个似乎极富潜力的新生事物，他们得以“上帝视角”进行观察和检视；在讨论和制定相关规范时，也经常体现“以互联网为‘对象’”的思考模式。正是在这个意义上，人们才能够理解当时互联网技术规范的确立，能够凭借自下而上、去组织化的宽松模式达成。[③]

作为“对象”的早期互联网诞生 30 年来，却一直受到其赞助商“金主”的禁锢，被限制不得用于私人或商业目的。20 世纪 80 年代，麻省理工学院的阿帕网用户手册中就有这样一条醒目的警告：“通过阿帕网发送电子信息，谋求商业利益或用于政治目的，是反社会行为，而且违法。”[④] 但是，随着“限制民用和商用”的规定被突破，网络联接规模化的效用开始展现，电子邮件、网站浏览等应用逐渐普及，互联网迅速演化成为社交、商务等活动的某种先进“工具”，从而进入“成长期”。在这个阶段，就其性质而言，互联网经常被类比为与广播电报、有线电视等同质的大众传媒工具——当然，前者更为先进高级，因其能够聚合多种信息传播形式成为“多媒体”终端。[⑤]

这种“工具观”的狭隘思维并没有妨碍一些极富洞察力的思想家预见互联网的发展潜力和其性质上的独特之处。例如，号称“因特网第一公民”的霍华德·莱茵戈德（Howard Rheingold）在 1993 年的著作中就将描述了一种虚拟电子家园的图景：

> 人们从事一切在现实中会做的事……人们凭借着屏幕上的字符交换欢笑与争论、进行学

① 于志刚认为：最初，尚未普及的网络仅仅只是作为“犯罪对象”，网络犯罪基本等同于针对计算机的高科技犯罪；随着普遍联接的达成以及接入门槛降低，网络在犯罪活动中的工具属性开始突出，转为“犯罪工具”，网络犯罪实际上是借助网络技术优势实施的传统犯罪；晚近，网络社会极速崛起，构筑了网络和现实交织的“双层社会”，网络也再次升级发展成为可以容纳部分甚至全部犯罪过程的“犯罪空间”。参见于志刚：《网络安全对公共安全、国家安全的嵌入态势和应对策略》，载《法学论坛》2014 年第 6 期，第 10 页。

② See Malte Ziewits and Ian Brown, “A Prehistory of Internet Governance”, in Ian Brown (ed.), *Research Handbook on Governance of the Internet* (Northampton: Edward Elgar Publishing, 2013), pp. 3 – 26.

③ “（当时的）互联网原则不应视为僵化的权威规则，它们实际上更像在不同场合下、关于互联网的合适设计和恰当行为的讨论中催生的共有信念和指导原则。” See Malte Ziewits and Ian Brown, “A Prehistory of Internet Governance”, in Ian Brown (ed.), *Research Handbook on Governance of the Internet* (Northampton: Edward Elgar Publishing, 2013), p. 14.

④ 转引自〔英〕马特·里德利：《自下而上》，闾佳译，机械工业出版社 2017 年版，第 323 页。

⑤ 如果赋予这些工具以政治意义的解读，也许还能够声称：广播和电视的大规模通信技术因为其适用于一对多的传播模式，因而可能导致权力在短期内转向集权主义；而互联网（也许还有电话）这样的多对多传播模式，却将削弱而非加强专制政权。参见〔英〕马特·里德利：《自下而上》，闾佳译，机械工业出版社 2017 年版，第 322—323 页。

术讨论、传达商业信息、交换知识、分享情感、拟定计划、脑力激荡、聊八卦、争吵、堕入情网、寻找与失去朋友、打情骂俏、创造高水平的艺术成果以及更多的懒散讨论。①

但这种能够包容现实中几乎所有类型的社会行为和社会关系的“虚拟空间”，则需要一直等到前述互联网的维度崛起之后才能真正确立。至此，互联网进入“成熟期”，并完成了从“工具”向“空间”的性质升级——以依托互联网的商业活动为例，包括支持全程在线完成交易的“网购平台”、打通线上线下联系（即 Online to Offline）的“O2O 商业模式”等在内的空间描述，便完成了对于“电子商务”这种简单工具描述的升级；以依托互联网的社交活动为例，包括实时分享位置和心情状态、通过视频语音媒介提供接近面对面的交流体验等在内的空间描述，便完成了对于“即时通讯”这种简单工具描述的升级。

（三）从技术协调规范到多层治理架构：网络治理的发展

应该说，囿于不同阶段互联网发展程度的客观状态，人们对互联网的性质必然具有不同层次的理解；而这种有关互联网性质的普遍理解，又直接关系到人们对于网络治理实践的思维范式。

1. “对象”互联网的技术协调规范：“请求评论”和“开源合作”

即使在其最早期，要维持互联网的基本运作仍然需要一定的秩序规范、以及对于技术创新的大量协调。现在看来令人惊奇的是，这些规范和协调大多是通过一种自下而上的方式、在一种欠组织管理的状态下近乎“自动达成”。当时最为重要的两种秩序生成模式，一种是在技术圈广泛采用而且效果甚佳的“请求评论”（Request for Comments）机制，另一种是在互联网技术社群经由自律凝聚出的关于“开源合作”（Open Source）的共识。

“请求评论”机制的产生是基于协调技术更新的现实需要。互联网的初级研究员们希望通过一种快速有效的方式对特定技术问题或者拟适用的技术标准获得反馈、形成共识，在一种具有偶然性因素的促使下，他们尝试将相关倡议转为书面形式并加上“请求评论 1 号文”（RFC 1）的标签开始传播。由于这种进行技术协调的方式被证明切实有效，1985 年被互联网工程任务组（The Internet Engineering Task Force，简称 IETF）采纳为标准流程。② “网上礼仪”（netiquette）即是此类通过 RFC 方式自发讨论产生的早期互联网规范的代表。③

“开源合作”机制是又一种在早期互联网技术社群中自发产生且被广泛采用的规范方式。针对互联网各领域的“子对象”，技术精英们松散地自组织，开源共享就是他们之间进行技术协调的指导规范。当然，在对各“子对象”的研究和实现过程中，具体协调规范可能并不一致——有的会出现核心领导团体，有的则极度依赖分散的参与者个人。④

在把互联网视为研究和建设“对象”的、以工程师为主的技术团体内，这些并没有确定规

---

① See Howard Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (Boston: Addison-Wesley, 1993), pp. 3 – 5.

② IETF 的官网上仍然有一块区域划为 RFC 文件区（http://www.ietf.org/rfc.html），与 RFC Editor 网站上的内容（https://www.rfc-editor.org/）保持同步更新。据查询，最新的 RFC 文件是 2017 年 9 月上传的“请求评论 8247 号文”（RFC 8247），https://www.rfc-editor.org/info/rfc8247 (last visited July 7 2018).

③ See RFC 1855, “Netiquette Guidelines”, Oct. 1995, https://www.rfc-editor.org/info/rfc1855 (last visited July 7, 2018).

④ See Malte Ziewits and Ian Brown, “A Prehistory of Internet Governance”, in Ian Brown (ed.), *Research Handbook on Governance of the Internet* (Northampton: Edward Elgar Publishing, 2013), pp. 23 – 27.

则支撑的协调与规范体系运行流畅，并促生了某种程度的“技术乐观主义”。例如麻省理工学院的一位早期 RFC 机制参与者戴维·克拉克（David Clark）就宣称：“我们无需国王或总统，也不必投票。我们的信仰就是粗略的共识和运行的代码。”① 这种乐观错觉在后续的互联网治理辩论中仍然不时出现。

2. “工具”互联网的典型规制主张：“马匹法”和“代码法”

20 世纪 90 年代，不少前瞻性的理论家开始超越技术层面探讨“互联网如何治理”。例如，1995 年，知名互联网法律学者劳伦斯·莱斯格（Lawrence Lessig）就此提炼出了两个问题：第一，网络空间是否可以经由类比既有经验的方式得到有效治理？第二，网络空间是否在性质上有新的地方？② 可见，囿于理解新事物的一般习惯，在网络治理的问题上，人们仍然是从类比已有经验切入。

在 1996 年的演讲和文章中，弗兰克·伊斯特布鲁克（Frank Easterbrook）法官就做了这样的类比，并概括提出“马匹法”（Law of the Horse）的观念，其核心主张是：正如不需要为了解决与马有关的一切法律问题而专门新建一门“马匹法”的道理一样，我们也不需要特别创设一门“网络法”才能应对互联网带给我们的法律问题；已有法律体系中的物权、合同、侵权、犯罪等规范，都可以直接、而且是完美地得到延用，并足以解决与互联网相关的新问题。③ 在当时，这个主张还具有引发一定争论的能量。④ 现在看来，弗兰克·伊斯特布鲁克法官很大程度上是受限于他所处的时代，他所能理解的网络，只不过是一种较为先进的“工具”而已。从本质上来说，当然也就像对作为工具的“马匹”一样，不需要专门创设法律体系来进行特别规制。

如果说之所以出现“马匹法”的主张，是因为论者采取了将互联网视为“工具”的视角，那么，另一种“代码法”（Code is Law）的主张，则可以说是对互联网“工具”性极致利用的体现。“代码法”主张的核心观点认为：在网络空间中凭借代码作为手段，可以实现、甚至超越现实社会中法律规制的效果。⑤

按照前文所述，当代互联网已从“工具”最终演化成为“空间”。对于“工具互联网的治理”（governance of the Internet）、以及“利用互联网工具的治理”（governance by the Internet）的规制主张，就也要相应演化为在“空间”语境下的治理思路（governance in the Internet）。对于能够容纳社会行为和社会关系的网络空间，需要一套适配其特性的系统治理方案；而这种需要考虑适配的特性，就主要来自于网络空间的多层架构。

---

① See Paul Hoffman, “The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force”, 2001, http://www.ietf.org/tao.html (last visited July 7 2018).

② See Lawrence Lessig, “The Path of Cyberlaw”, (1995) 104 *Yale Law Journal* 1743, pp. 1743 – 1755.

③ See Frank Easterbrook, “Cyberspace and the Law of the Horse”, (1996) *The University of Chicago Legal Forum* 207, pp. 207 – 216.

④ 事实上，劳伦斯·莱斯格次年即发表一篇争锋相对的文章，认为网络空间需要发展适应其自身特点的一整套法律体系。See Lawrence Lessig, “Cyberspace and the Law of the Horse: What Cyberlaw Might Teach”, (1997) 113 *Harvard Law Review* 501, pp. 501 – 546.

⑤ See, e.g., Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006), pp. 1 – 9. 这一主张为 Lessig 教授赢得了众多拥趸，例如 Lee & Liu 即借用此洞见，认为中国政府利用代码规则构建网络防火墙以及信息滤查机制就是此推论得以适用的现实案例，see Jyh-An Lee and Ching-Yi Liu, “Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China”, (2012) 13 (1) *Minnesota Journal of Law, Science and Technology* 125, pp. 125 – 151.

3. “空间”互联网的匹配治理范式：网络通信的多层架构和“层级治理”主张

立体的网络空间所以能够包容海量数据和关系、提供丰富应用可能性，同时还能够保持稳健的运行和顺畅的迭代，都得益于它技术意义上的多层架构。

所有网络行为在其本质上都是网络通信过程。因此，以一个简单的网络信息传输的操作为例，就能够清楚展现网络多层架构的功能细节：（1）终端用户形成一条信息并产生传输愿望，这条信息在顶端的意义层面可能具有某种社会意义——包括积极意义（例如社会协作邀请）或消极意义（例如仇恨言论散布）；（2）信息在网络终端（例如个人电脑或智能手机）完成输入并确立其在内容层的存在；（3）根据具体使用场景的不同，可能涉及应用层不同网络应用的介入——例如，如果使用浏览器发布论坛留言，那么介入的就是浏览器应用，如果使用社交工具发布群聊信息，那么介入的就是该社交软件应用；（4）在协议层，通过计算机或手机系统，根据既定协议和规范，内容被转化为适宜于电子发送的形式——例如将信息拆分装包、在各个数据包贴上地址标签、添加冗余校验信息提高容错率等；（5）数据包按照既定技术标准通过软件系统和硬件系统的接口，最终进入硬件层，被提交给承担最终传递的网络；（6）通过路由器、域名解析制度等网络层的核心技术安排，以及 Wi-Fi、4G、光纤等无线或有线的物理意义上的连接，最终将数据包传递到目的终端。目的终端会沿着一个与此前描述相反的过程，将信息接收、整理并还原成其本来面目。下一页图 2 展示了多层架构的网络通信过程。

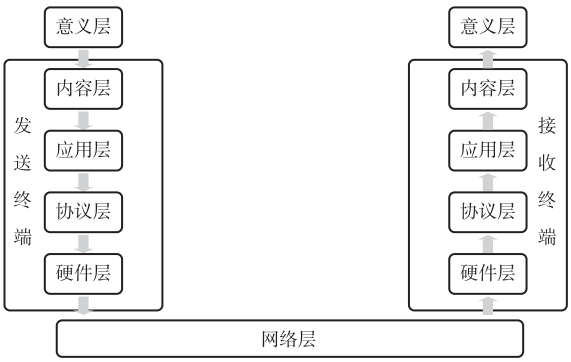

图 2　多层架构的网络通信示意图

说明：本图例展示了网络通信的基本过程。按照箭头方向的指示，信息从发送者起意（左侧意义层）、经发送终端逐层处理和网络层传输，在接收终端逐层还原，最终被接收者收取和解读。内容层、应用层、协议层、硬件层和网络层在网络通信中均发挥了相对独立的技术功能，在本示意图中被合称为功能层。

网络空间治理的复杂即来源于它的这种多层架构。本文主张，理解网络空间治理的议题都应将相关议题涉及的主要网络行为还原到这种多层架构的场景当中，并尽可能地明确各层级的意义和功能。这意味着，有必要构建网络空间的层级理论模型。

（四）从技术过程到分析框架：网络空间的层级理论模型

1. 层级理论模型的提出

应该指出，不少论者已经意识到有必要将复杂的网络空间进行拆分，以便能够对网络议题进行更精准的分解研讨。在网络治理的法理讨论中，也存在诸多版本的“层级理论”，其中：劳伦斯·索伦（Lawrence Solum）和钟明（Minn Chung）识别出的网络层级最多，包括物理层、连接

层、互联网协议层、传输层、应用层以及内容层；此外，他们还提出网络治理的“层级原则”，包括“层级间独立”以及“最小限度越层”两项子原则。[①] 约瑟夫·奈（Joseph Nye）在他有关“网实力”的主张中，简单区分了网络的软硬件分层架构，并认为“网实力”的存在基础在于：网络行为虽然发生在软件层面，但是其后果能够穿越层级架构辐射至硬件层面，从而对现实世界造成影响。[②] 张晓君借用劳伦斯·莱斯格关于互联网的经典论述，[③] 将网络分为物理层、规则层和内容层，并在此认识的基础上构建了互联网的全球混合场域治理模式。[④] 于志刚创造性地提出除技术层面、应用层面之外的意识层面，认为网络具有意识形态性，而且立基于前两者的意识层面虽然形成时间最晚，在网络的社会治理中所占比重却日趋扩大。[⑤]

本文认为，基于图 2，容易总结网络空间层级理论模型。在这个模型下：

第一，网络行为被拆解为历经意义层、内容层、应用层、协议层、硬件层、网络层的过程。其中，意义层和网络层构成了网络空间与现实空间的基础连接界面——前者完成网络空间行为的社会意义的转化，后者为网络空间行为提供物理意义上的可能；协议层主要解决网络传输的技术协议问题，基本可以视为前述“对象互联网”阶段的当代延续，而前文提到的技术协调规范在协议层治理中也得到一定程度的沿用；应用层和内容层大致对应此前的“工具互联网”，“代码法”的规制思路在这两个层面都仍然具有一定的现实指导意义。

第二，层级理论模型为网络治理提供了恰当的分析框架，相关议题也自然要还原到各个层级的特定场景中进行探讨。根据模型的指引，网络治理的具体需要，均植根于意义层；针对具体治理议题，通常需要在其主要发挥作用的功能层级上寻找相适应的利益连接点（通常是该层级的功能管理者、服务提供者或者设施运营/拥有者），作为规制的抓手；或者，在某些情况下，也可以利用层级间在技术事实上的关联，考虑跨越到其它层级采取措施，从而达到对本层级议题进行规制的目的。

2. 层级理论模型适用示例

仅以网络治理中的安全关切为例，对层级理论模型的适用进行初步展示。

根据层级理论模型的指引，网络安全威胁形式多样，具体威胁的功能发挥层级各异。但不管网络安全威胁体现为何种形式，也不论其是在哪个网络层级上产生作用，对它的性质和程度的相关评判最终都要落脚于它在网络空间多层架构体系的意义层中释放出的具体社会意义。例如：（1）某种煽动民族仇恨的网络言论，其在意义层的负面社会评价是释放了危害民族团结和社会稳定的、易于传播扩散的信息，其功能发挥层级是内容层；（2）某种盗取个人电脑数据的恶意软件，其在意义层的负面社会评价是侵犯了个人的数据权以及隐私权，其功能发挥层级是应用层；（3）某种特定的计数机通讯协议标准，其在意义层（由相对国做出）的负面评价是弱化一

① See Lawrence Solum & Minn Chung, “The Layers Principle: Internet Architecture and the Law”, *Public Law and Legal Theory Research Paper 55*, 2003, pp. 1 – 114.

② See Joseph Nye, *The Future of Power* (New York: Public Affairs Press, 2011), pp. 113 – 153.

③ See Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (New York: Random House LLC, 2002), p. 23.

④ 参见张晓君：《网络空间国际治理的困境与出路——基于全球混合场域治理机制之构建》，载《法学评论》2015 年第 4 期，第 50—61 页。

⑤ 参见于志刚：《网络安全对公共安全、国家安全的嵌入态势和应对策略》，载《法学论坛》2014 年第 6 期，第 5—19 页。

国技术标准话语权，其功能发挥层级是协议层；（4）某种在厂商生产过程中留有后门的政府办公设备，其在意义层的负面社会评价是可能危及政府信息机密性，其功能发挥层级是硬件层；（5）某种对于域名解析根服务器的单边控制，其在意义层的负面社会评价是影响一国网络环境安定性，其功能发挥层级是网络层。上文转述为表格如下：

威胁形式	具体事例	功能层级	意义层上的负面评价
煽动民族种族仇恨的网络言论	使用 twitter 发布挑拨种族关系的内容	内容层	危害民族团结和社会稳定
锁定个人电脑数据的恶意软件	WannaCry 勒索软件病毒	应用层	侵犯个人数据隐私
可能冲击已有标准的网络通讯协议	中国拟推广 WAPI 标准遭阻	协议层	弱化一国技术标准话语权、甚至威胁产业安全
留有后门的硬件设备	某国对政府公务电脑芯片的限制性规定	硬件层	危及政府信息机密性
域名解析根服务器的单边控制	ICANN 机制改革争议	网络层	影响一国网络环境安定性

基于层级理论模型，可以对网络安全规制的落实做出以下初步观察：第一，由于网络空间威胁潜在来源的广泛性，使得安全关切往往需要覆盖多个领域和多个角度，安全规制的多层级落实也因此成为必要。第二，对于特定类型的网络空间威胁，原则上应该从其相应的作用层级入手考虑回应策略和规制方案。例如：应对应用层恶意软件带来的安全威胁，应当优先考虑应用层的防范和惩戒。第三，由于网络空间行为在其多层架构之间的潜在连接性，使得跨层级规制和多层级协调的综合方案具有可行性。例如：为了维护国家对于意识形态的正当掌控，有效限制网民对一部分宣言恐怖主义、民族仇恨等极端网站的访问，可以在协议层设立特定的网站屏蔽机制，在应用层限制某些反规制软件的使用，同时在内容层设立信息筛查功能。

三　为国家“正名”：“全球网络公域”抑或“网络空间主权”

如前所述，国家已经在网络空间中逐步“浮现”。本章主要依据前文构建的层级理论模型，试图对网络空间主权进行证成，从而为国家在网络空间中的介入“正名”。

（一）“全球网络公域”的驳斥

抵制国家在网络空间中“浮现”的一个常见手段，就是以“全球网络公域”的主张来否认或减损“网络空间主权”。作为“全球网络公域”的上位概念，“全球公域”（global commons）脱胎于 1968 年哈丁的著名论文《公地的悲剧》，[①] 其后由经济学及公共政策领域的学者将其推广运用至全球范围，指国家主权管辖之外为全人类利益所系的公共空间。目前普遍认为人类社会中典型的全球公域包括公海、国际空域、外层空间和南极极地。[②]

这种全球公域理论逻辑事实上存在两个维度：首先，这些区域应为全人类所共有，是为

① Garrett Hardin，“The Tragedy of the Commons”，（1968）162 *Science* 1243，pp. 1243 – 1258.

② 参见韩雪晴、王义桅：《全球公域：思想渊源、概念谱系与学术反思》，载《中国社会科学》2014 年第 6 期，第 188 页。

“公域”，国家不得按传统主权主张势力范围；其次，这些区域所附资源或衍生物品亦应属全人类所共有，是为“公共物品”，国家不享有排它权利和独断管辖。鉴此，既定全球公域的特征可以被概括为：其作为“公共物品”在经济学意义上的非排他性，以及其作为“公域”在国际政治法律意义上的去主权化、去军事化的特性。然而，在层级理论模型的检视下可以发现，网络资源并非经济学意义上的“公共物品”，网络空间也无法构成国际政治中的“公域”。

1. 网络资源并非经济学意义上的“公共物品”

在微观经济学中，公共物品的最大特征就是没有排他性。[①] 换言之，公共物品是无法阻止人们使用、任何人都可以免费得到的物品；要排除他人的使用，要么在技术上就缺乏实现可能，要么实现起来成本太高。

如果以直觉来粗略评判作为整体的网络空间及其所附资源的话，关于排他性的上述标准似乎能够满足——网络空间似乎无法有效排除他人的进入、因此无法有效阻止人们免费使用网络资源。但是，如果要进行更为细致的检视，就需要按照层级理论模型对网络进行拆解，并在各个层级针对排他性进行分析检验。

首先，网络层存在较明显的排他性。底层网络设施作为本层级的典型资源，一般都能够做到对使用者及其权限的精确控制。以网络运营商为实际操作者，国家不仅能够通过技术手段识别终端用户并决定是否准许其接入网络，甚至还能够精准分配具体用户的网络带宽。

其次，由于网络终端设备通常都是私人物品，所以硬件层也具有排他性。在应用层上的各种应用程序，如果不能说它们都具有排他性的话，至少能够判断它们能够具有排他性——基于技术，同样能够识别授权用户并排除其它用户。网络内容的排他性较难下定论，因为其答案取决于特定内容所依附的应用层程序或者网络层服务。

最后，网络传输协议的公共品特性决定了协议层具有非排他性，这是因为网络传输协议的首要宗旨就是为了无差别提供给所有潜在用户使用，而只有所有潜在用户都能够认同该协议、并按照协议规范进行传输操作，协议层才能够得以建构。但是显然，如果仅以协议层的非排他性为由，推而认为整个网络空间均具有非排他性，那将犯下以偏概全的谬误。

可以将以上观察判断通过表格简明表述为如下形式：

功能层级	资源呈现的典型形式	是否(能够)具有排他性
内容层	缤纷且海量的网络信息	排他性/非排他性
应用层	网络应用程序	排他性
协议层	网络传输协议	非排他性
硬件层	网络终端硬件	排他性
网络层	底层网络设施	排他性

2. 网络空间无法构成国际政治法律中的“全球公域”

对于被普遍承认为全球公域的公海、外空和南极极地而言，其相关治理实践存在一定的共

① 参见〔美〕曼昆：《经济学原理（微观经济学分册）》（第 7 版），梁小民、梁砾译，北京大学出版社 2015 年版，第 233—235 页。

性，即：通过国际条约达成共识，对这些区域实施去主权化、去军事化的安排。[①] 按照这个标准来评判的话，网络空间无法构成“全球公域”。

首先，就网络空间的地位而言，目前缺乏一个类似《联合国海洋法公约》第 89 条、《外太空公约》第 2 条和《南极公约》第 4 条的多边条约对其进行明确定性。其次，如前所述，网络空间的军事化趋势已经显露，有相应网络建设能力的国家都寻求至少是一种防御性的网络军事力量。最后，网络空间去主权化的论断，则与前文对网络空间中国家的“浮现”的观察直接相悖，而且后文亦将对网络空间主权进行理论证成。

综上，“全球网络公域”的论断经不起推敲，以此为依据、主张国家从网络空间退出的主张，自然也就站不住脚。甚至于应该警觉部分国家对于“全球网络公域”论的不正常热情，以防其以“公”谋“私”，将“全球公域”异化为其“国家私利”；抑或是将他国主权范围内的“私域”异化为全球公域，从而为自身的新国际干涉主义寻求合法借口。[②]

（二）“网络空间主权”的证成

在层级理论模型下，“网络空间主权”可以得到有力的构建。

1. 网络空间主权生成的必要性：基于协议层和意义层的解读

如前所述，通常是在技术精英的鼓吹引导下，人们总是或多或少地抱有某种关于“全球网络公域”的看法。这种误解实际很大程度上是源于对协议层重要性的病态放大。诚然，在协议层实施统一的技术标准是网络空间的存在基础之一，但是这并不意味着互联网在所有层级上的“统一”。[③]

随着网络空间的扩张以及对于不同团体实现覆盖，同时考虑到这些众多团体自身的认知范式和价值偏好，在意义层上涌现不同的主张就成为必然。以网络空间治理本身为例，尽管几乎所有国家都认为需要某种形式的网络管制措施，但是对于管制的目的、程度、方式等等具体问题，各个国家——尤其是主要网络国家——在现阶段分歧巨大。网络空间治理的目标，可能是保护个人信息安全、维护国家关键技术领域安全、促进信息时代的生产效率、等等。而同样是对内容的管控，有的国家出于宗教原因，有的国家出于意识形态原因；有的国家持紧缩政策，有的国家则持放任态度；有的国家主要通过自上而下且较具强制力的行政干预，有的国家主要通过自下而上的行业自律。

上述分歧初步展示了网络空间分化的意识基础。从意义层中存在不同价值偏好入手，人们也可以更好地理解前文所述网络技术先发者与后发者对于网络空间主权的不同态度。网络技术后发者希望凭借其网络主权主张而建立有效的理论防御态势，一如上世纪国际经济新秩序运动中，针对发达国家全方位的经济扩张，第三世界国家试图从强调“经济主权”入手，为其所倡议的平等国际经济交往和对内经济管制权提供法理基础。相反，网络技术强国在世界范围内已经获得显

---

① See Kristen Eichensehr, “The Cyber-Law of Nations”, (2015) 103 *The Georgetown Law Journal* 317, pp. 340 – 346.

② 参见韩雪晴、王义桅：《全球公域：思想渊源、概念谱系与学术反思》，载于《中国社会科学》2014 年第 6 期，第 204 页。

③ 例如，美国战略与国际研究中心的詹姆斯·刘易斯（James Lewis）是奥巴马网络战略文件的主要起草人，他明确反对网络技术开创者将一个“自我组织的全球公域”的意识形态植入互联网。他在美国参议院听证会上陈述：“现在最紧迫的任务就是如何把法律带到荒蛮之地的问题，从各自为政的方法转变成真正意义上的网络安全。”

著的先发优势并控制了绝大部分的市场，因此往往不会主动提及网络空间主权，相反，它们大都主张沿袭保守的治理思路，推行宽松的规制措施，并且否定或弱化网络空间主权的存在。

简言之，建构在语言、文化、共同记忆等基础上的民族认同，构成了现实世界中主权国家的主要观念依据和合法性来源。这种逻辑有望以某种相反的方式在网络空间中得到延续：既有主权国家凭借其权威地位，可能在其势力范围内强化某种价值偏好；一旦完成了对受众的表面驯化，这种很大程度上系因人为打造的认同感，反过来又构成了强化国家主张网络空间主权的观念依据和合法性来源。

2. 网络空间主权实现的可行性：基于网络层、硬件层、应用层和内容层的分析

如果只是停留在呼吁的说辞上，那么网络空间主权仍无法成为国家构建网络管控的真实基础。下文在层级理论模型中的四个层面上，为网络空间主权实现提供可行性论证支持。

在网络层，国家可以确定网络空间的“边境措施”。但是，由于各个国家组织建设其国内网络基础设施的总体规划和接入国际互联网的总体方案不尽相同，这种能力并非每个国家都在同等程度上拥有。根据是否能够在国家级别上对网络层进行封锁、限行等操作，可以将国家在网络空间的主权“能力”进行区分。①

硬件层构成了国家行使主权管制能力和可能的被管制对象的连接点，因为硬件既构成了网络空间行为的物理基础，同时又能够维系其在现实世界的物理存在从而具有地域性。但是从技术的角度而言，这种从虚拟网络到现实地域的指向和连接并不可靠，“互联网是主张合理推诿的完美场所”（The Internet is perfect for plausible deniability），② 因此国家行使主权管制常常只能针对事情本身、而无法总是追究到最终直接责任主体。这就导致：

在内容层和应用层，国家可以通过对其境内网络运营商和应用产品或服务提供商等“中间人”（intermediaries）进行规范，最终实现对于网络空间行为的规制。③ 这些“中间人”一方面对于内容和应用有直接的管控手段和能力，另一方面又因为其通常具备的有形实体（例如公司）和资产（例如银行账户、固定设备等），可以由国家比较方便地进行传统意义的有效管控。在 2002 年“雅虎美国案”中，法国法院最终对于处在其管辖域外的美国公司成功采取了强制措施，所依靠的就是这家外国网络服务提供商在法国开展业务所必需的经营实体和相关资产。④

四　网络空间的主权化与网络空间基本法律秩序的展望

根据前文层级理论模型的分析，“网络空间主权”从其存在的意识基础和实现的可行路径上都得到了一定程度的证成，从而为“网络空间的主权化”奠定了理论基础。但据此是否即可进

① 例如，2017 年坦桑尼亚希望获得中国援助以规范社交媒体，即可视为中国的网络主权能力的一种认可和出口，参见：“坦桑尼亚希望获得中国的援助以规范社交媒体，打击网络犯罪”，观察者网，http：//www. guancha. cn/global-news/2017_ 08_ 04_ 421469. shtml，最后访问时间：2018 年 7 月 7 日。

② Susan Brenner, *Cyber Threats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009), p. 5.

③ See Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006), pp. 65 – 85.

④ See *Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France* (LICRA c. Yahoo!).

一步推论：网络空间必将复制现实世界的主权国家体系格局？事实上，在这个问题上，向来存在两种相互竞争的主张：[①] 以美国为首的信息网络技术先发国家倾向于支持“多利益攸关方”（Multi-stakeholder）的治理模式，强调在网络空间中弱化国家存在，相反需要照顾除国家之外包括企业、技术团体、市民社会等其它攸关方的利益，并赋予这些非国家利益攸关方以一定的话语权；[②] 以中俄为首的信息网络技术后发国家倾向于沿袭传统意义上、以“威斯特伐利亚”主权国家体系为基础的治理模式。[③]

对网络空间主权化进行更精细化的判断，将在很大程度上影响关于网络空间基本法律秩序的展望和想象。本文认为，囿于其底层技术逻辑的先决性限定，网络空间主权在法律秩序建构中仍然会体现出与传统主权不同的特性。对此，下文从两个方面展开初步讨论。

1. 网络空间不会完全“再主权化”

虽然从其表达含义而言，“再主权化”和“巴尔干化”两个术语都在试图描述网络空间分裂为利益不完全相互包容的众多子群的趋势；[④] 但“再主权化”术语后面其实隐含了一个进一步的判断，即现实世界中的主权国家体系将完整投射到虚拟世界，从而使得网络空间的格局最终演变为与物理空间同质化的主权国家体系。至少在现阶段，本文对笼统的网络空间“再主权化”的提法持谨慎异议的态度。这是因为：这个隐含判断的成立与否，在许多方面存在质疑的空间；相反，如果保留对于网络空间“再主权化”的判断，却能够提供更多的理论可能性。具言之：

首先，从某种意义上来说，传统主权国家体系的生成本身就具有不确定性，并导致以此为基础的全球政治和法制存在结构性问题。主权国家首先作为地区秩序范式的基本单位形式确立于西欧，随着殖民主义扩张和战后殖民地独立，才进而扩展成为全球秩序。[⑤] 因此，在缺乏类似机缘的情况下，没有任何理由抱守成规，坚持主张将主权国家体系的秩序范式僵化照搬到网络空间中；同样也没有任何理由坚持既定国际法体系中的主权原则可以不做任何适配修正就在网络空间得到完整延用。

其次，在网络空间中划定包括网络主权体在内的团体边界需要若干基础要件，其中最终要的是团体成员的共同想象、以及团体主导者的治理能力。从这个角度来看，许多现实中的小国和弱国可能会因为缺乏统一的网络共同意识或足够的网络治理能力，从而事实上无法在网络空间维持其边界，作为主权理念存在基础的“主体身份”也可能无法得到构建。按照类似的逻辑，也可以沿着另一个方向大胆预设：可能存在多个现实中的国家组成意识一致的团体，因为试图在网络

① 许多研究报告和学术论文都观察到了这种冲突，see，e. g. ，Kimberly Hsu & Craig Murray，China and International Law in Cyberspace，（2014）*U. S. -China Economic and Security Review Commission Staff Report*；also Kristen Eichensehr，“The Cyber-Law of Nations”，（2015）103 *The Georgetown Law Journal* 317，pp. 317 - 380；或者参见蔡翠红：《网络空间的中美关系：竞争、冲突与合作》，载《美国研究》2012 年第 3 期，第 107—121 页。

② 有关“多利益攸关方网络空间治理理论”的介绍，参见鲁传颖：《网络空间治理与多利益攸关方理论》，时事出版社 2016 年版，第 68—97 页。

③ See，e. g. ，Delegation to UN General Assembly（PRC），“Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 68th Session UNGA”，New York，October 2013，https：//unoda-web. s3-accelerate. amazonaws. com/wp-content/uploads/assets/special/meetings/firstcommittee/68/pdfs/TD_ 30-Oct_ ODMIS_ China. pdf（last visited July 7，2018）.

④ 关于网络空间“再主权化”的提法，可以参见刘杨钺、杨一心：《网络空间“再主权化”与国际网络治理的未来》，载《国际论坛》2013 年第 6 期，第 1—7 页。

⑤ 参见杨帆：《从自发到自觉：国家主权的祛魅与重构》，厦门大学博士学位论文，2016 年，第 39—63 页。

空间维护其共同诉求而聚合成某种“网络空间超国家组织”。

最后，某些非主权国家单位的团体（例如巨型互联网公司）事实上有意愿也有能力在网络空间进行某种程度的边界划分，参与虚拟世界的“圈地运动”。这些团体在现阶段因为无法满足需要多层级落实的网络安全诉求，进而无法维系其网络空间的边界；但是，它们可能转而以利益、价值观、或者行为模式等为标准进行身份识别和共同体构建。一旦外部网络空间能够因为某种方式或机制维持一定标准的普遍安全，这些团体很可能就将成为网络空间“巴尔干化”的新一轮推动主体。

2. 迈向“网络空间版主权原则”

如果存在“网络空间版主权原则”的话，它是否、或者将在多大程度上沿袭传统主权原则？这个问题可能在现阶段尚不明确，因为面对网络空间种种情形的具体冲击，传统主权原则仍在不断适应演化。作为一种展望，本文对“网络空间版主权原则”可能存在的问题和挑战刍议如下。

首先，“网络空间版主权原则”有可能仿照传统主权原则的理论进路，成为若干关键子概念的逻辑前提。具言之，作为传统主权的衍生概念，经济主权、政治主权、领土主权、自然资源主权等都能获得天然法理支撑；那么，网络空间中的资源是否也可类比此逻辑、因为网络空间主权而获得法理支撑？例如，可以将数据资源定义为网络空间中的生产要素，从而将“数据主权”问题转化成为数据生产要素资源在网络空间中的主权归属问题。

其次，在“网络空间版主权原则”下，主权者可能无法清晰维持主权域的内外差别。这是因为，即使对于有能力在网络层进行一定界限划分的国家而言，网络空间主权的管辖边界也仍然是模糊的，更遑论那些没有网络层行为能力的国家了。反过来说，如何处理网络空间中的主权边界，是“网络空间版主权原则”需要妥善回应的一个理论挑战。

再次，网络空间主权行使逻辑将不同于传统主权，因为针对网络空间行为最终责任主体的责任归咎存在困难。传统主权行使时，可以依据既定法律和执法者，在违法后果发生后进行责任认定和实施惩处；但是网络空间主权行使时，需要优先遵循事前防御的策略，并借由对“中间人”施加明确责任，来充分调动“中间人”的治理功能。

最后，按照“网络空间版主权原则”，主权者身份的认定逻辑很可能与传统情形下的逻辑相反——在网络空间中只有拥有足够能力并事实上参与了“国际规则”的协调与制定进程，才会间接反映网络空间主权者的身份；而在现实世界中，人们通常认同与之相反的逻辑：因为被认定为主权者身份，才能参与“国际规则”的协调与制定。

五　结语：法律秩序的技术维度

经过几百年发展和积淀的科学精神表明，还原论是一种分析复杂对象的有效进路。本文在网络空间物理运行规律和网络通信基本技术过程的基础上，拆解出必要的网络层级并据此构建层级理论模型。这个模型一方面能够充分容纳纷繁多样的网络空间行为，另一方面又能够合理对接网络规制措施，从而在这个原本混乱不堪的空间内假设起一座沟通行为及其规制的理解桥梁。

基于技术架构的层级理论模型不仅能够对既有技术框架下衍生的现实进行解释，同时还能够在一定程度上预示技术变迁与法律秩序的关联。该模型显示，如果网络基本技术架构发生改变，那么有关网络空间法律秩序的基本判断也需要重新修正。这方面的一个思维实验是：如果未来类

似马斯克所畅想的全球卫星互联网得以实现,[①] 全球任何地方的终端均通过卫星接入互联网,那么在该种技术架构的网络空间中,本文所论证的国家的网络边境管控措施将被颠覆,网络空间国家主权也可能难以成立。

质言之,网络空间是人为构建的技术空间,网络治理必须充分考虑技术逻辑;对网络空间法律秩序的理论探讨,也不可脱离基本技术逻辑而单独开展;而在该论域中最为基本的理论判断,也有可能随着一次底层技术变迁需要得到修订甚至推翻重建。

最后需要指出:为了构建本文所称的“从技术逻辑到法律秩序的理解桥梁”,文章主要关注网络空间的技术过程。这种处理方式是否可能忽视了其它关键的、甚至是具有更大决定性的变量?是否可能过于关注现实技术逻辑,而忽视了法律应然逻辑?显然,对这些问题的后续思考将有助于进一步廓清网络空间主权的应有内涵。

The Emergence of the State in Cyberspace and Its Theoretical Bases: Cyber-Sovereignty from the Perspective of Layer Model

Yang Fan

Abstract: Cyberspace is a man-made technical space, so that cyberspace governance has to take into account of technical logic. In order to better understand the recent trend of emergence of state in cyberspace, this Article, by combining the evolution course of cyberspace and the technical process of internet communication, proposes the Layer Model as an analytical framework. According to this Model, any issue on cyberspace governance can be disassembled into six different layers for a close analysis, including the Meaning Layer, Content Layer, Application Layer, Protocol Layer, Hardware Layer and Network Layer. Under the scrutinization of the Layer Model, the proposal of “Global Cyber Commons” cannot sustain its existence except for the Protocol Layer. Because of the contradictions, often hard to reconcile, among states in the Meaning Layer, as well as the governance capability that can be achieved and secured in the Network Layer, cyber-sovereignty can be both necessary and feasible. Restricted by the technical logic which forms its basis, cyber-sovereignty may play a different role than traditional sovereignty in the sense of contribution to legal order; and the cyberspace is highly unlikely subject to re-sovereignization.

Keywords: Cyberspace, Layer Model, Global Cyber Commons, Cyber-Sovereignty

(责任编辑:李庆明)

① See The Guardian News, “Elon Musk wants to cover the world with internet from space”, https://www.theguardian.com/technology/2016/nov/17/elon-musk-satellites-internet-spacex (last visited July 7, 2018).