网络空间国际法文库

网络主权论

——法理、政策与实践

ON CYBER SOVEREIGNTY

Jurisprudence, Policy and Practice

黄志雄 / 主编

社会科学文献出版社

网络空间国际法文库

网络主权论

——法理、政策与实践

ON CYBER SOVEREIGNTY

Jurisprudence, Policy and Practice

黄志雄 / 主编

社会科学文献出版社

作者简介

（以撰写章节为序）

鲁传颖 上海国际问题研究院全球治理研究所副研究员，博士。兼任国际网络空间军事稳定机制联合主席，网络空间治理与创新共同发起人。主要研究领域为网络空间战略与全球治理（撰写第一章）。

杨剑 上海国际问题研究院副院长、研究员，经济学博士。主要研究领域包括国际政治经济学、极地和网络战略、地区战略等（撰写第二章）。

方芳 上海国际问题研究院博士后，华东政法大学副教授，法学博士，主要研究领域为网络空间治理、国际政治传播等（撰写第二章）。

郝叶力 博士，中国人民解放军少将军衔。中国国际战略学会高级顾问，国家创新与发展战略研究会副会长，中国互联网安全大会（ISC）观潮洲际论坛主席。主要研究领域为全球网络安全与国际合作、全球互联网治理问题（撰写第三章）。

黄志雄 武汉大学国际法研究所副所长、珞珈特聘教授，法学博士。《塔林手册》2.0版国际专家组成员、亚非法律协商组织网络空间国际法工作组特别报告员。主要研究领域为国际公法、网络空间国际法等（撰写第四章）。

张新宝 《中国法学》总编辑，教育部长江学者奖励计划特聘教

授，全国优秀中青年法学家，华中师范大学法学院名誉院长，中国人民大学法学院教授、博士生导师。主要研究领域为侵权法、网络法（撰写第五章）。

许可 法学博士，中国人民大学法学院教师，博士后，中国人民大学亚太法学院特聘硕士生导师，中国人民大学互联网金融与网络安全研究中心研究员、副主任。主要研究领域为公司法、网络法（撰写第五章）。

谢永江 北京邮电大学人文学院副院长、副教授，法学博士，北京邮电大学互联网治理与法律研究中心常务副主任。主要研究领域为网络法和经济法（撰写第六章）。

洪延青 北京大学互联网发展研究中心高级顾问，荷兰乌特勒支大学法学博士，全国信息安全标准化技术委员会2016年重点标准制定项目——“个人信息安全规范”编制组牵头人。主要研究领域为网络安全战略及政策法规（撰写第七章）。

嵇叶楠 中国信息通信研究院互联网治理研究中心根服务器组、平台规则组研究员。主要研究领域为国际互联网治理、网络空间战略和政策、互联网资源管理政策、域名技术与行业发展、电信业务管理政策等（撰写第八章）。

赵旭 中国信息通信研究院互联网治理研究中心平台规则组组长、研究员，墨尔本大学通信工程、软件系统工程双硕士。主要研究领域为互联网治理和域名、IP地址等关键互联网资源政策（撰写第八章）。

徐峰 外交部条约法律司副处长，法学硕士。负责和参与网络空间国际法、网络犯罪国际立法等领域研究以及双多边国际会议和谈判工作（撰写第九章）。

总序一

徐宏[1]

网络空间是全球治理和国际规则制定的新兴领域。十八大以来，以习近平总书记为核心的党中央高度重视全球治理问题，特别是网络空间等新兴领域的全球治理。习近平总书记强调，“大国网络安全博弈，不单是技术博弈，还是理念博弈、话语权博弈”，“要加大对网络、极地、深海、外空等新兴领域规则制定的参与”，“加快提升我国对网络空间的国际话语权和规则制定权”。习总书记在第二届世界互联网大会、网络安全和信息化工作座谈会等场合系统阐述中国的网络治理观、网络安全观、网络发展观、网络主权观、网络人才观等理念。这些重要讲话和理念为我们做好新时期网络安全和信息化工作，更好参与和引导网络全球治理提供了指引，有力促进了我国网络领域各方面工作，提升了我国在网络全球治理中的地位。

近年来，我国网络安全和信息化立法政策不断完善，先后颁布出台《网络安全法》、《国家网络空间安全战略》、《网络空间国际合作战略》等重要纲领性法律和政策文件，有关网络犯罪刑事立法、个人数据保护、网络安全审查等各领域立法不断推进，相关机制体制建设和务实举措稳步跟进，网络安全不断得到加强。与此同时，我国互联网产业和信息化建设也取得了长足进步，国际地位不断提升，更受国际社会的关注和借重。这一切均为我国更加积极参与和引导网络全球治理，争取更多话语权和制度性权力提供了坚实基础。

网络空间国际法是网络全球治理的基础性问题和重要组成部分，关

系网络国际规则如何制定、解释和适用，是网络国际博弈各国必争之地。我们应切实贯彻落实中央关于网络安全和信息化工作的重要部署和习近平总书记相关重要讲话精神，以只争朝夕的精神，推进中国特色网络空间国际法理论发展和能力建设，为我国争取网络空间国际规则制定权提供法理支撑和服务。具体而言，要以习总书记关于网络问题的系列重要讲话，特别是关于倡导尊重网络主权、构建网络空间命运共同体的理念以及全球互联网发展治理的“四项原则”、“五点主张”为指导，结合我国网络发展和网络外交的实践及需要，推进网络空间国际法各领域的研究；同时，我们也有必要运用国际法语言，为进一步阐释和充实上述重要讲话精神和重要理念，不断丰富其法理和价值观内涵，增强其国际感召力和影响力。

“网络空间国际法文库”的出版是推进国际法领域上述工作的实实在在的一步，我衷心期待中国国际法学界同仁以此为契机，加强与政府、业界等网络空间利益攸关方的协作，共同推进中国特色网络空间国际法理论发展和能力建设，为我国更好参与和引导网络空间全球治理提出更多的法理思想、法学理论和法律方案。

2017年6月

---

[1] 外交部条约法律司司长。

总序二

黄志雄

网络空间国际法是随着网络空间的发展，在理论上和实践中日益受到重视的一个国际法新领域。在互联网发展和网络空间形成的较长时间内，倡导网络空间自我规制和“自由放任”、反对国家主权以及在此基础上形成的国际法规则适用于网络空间的观念曾盛行一时。但事实证明，这种乌托邦色彩严重的“去主权化”和“去国际法化”观念无益于网络空间的稳定有序发展。近年来，国际法治在网络空间全球治理和秩序构建中的作用逐渐得到国际社会的普遍认可，各国特别是主要大国越来越注重通过塑造和影响国际规则，在网络空间的建章立制中抢占先机、赢得优势话语权和主导权。

从中国来说，我国政府对于推动网络空间国际法治极为重视，并多次以制定重要战略文件和法律、最高领导人讲话等方式来宣示积极参与网络空间国际规则制定的国家意志。例如，十二届全国人大四次会议于2016年3月正式通过《国民经济和社会发展第十三个五年规划纲要》，不仅明确提出要“实施网络强国战略”，还要求“积极参与网络、深海、极地、空天等领域国际规则制定”。2016年10月9日，习近平总书记在主持第三十六次中共中央政治局集体学习时，对网络强国建设提出了六个“加快”的要求，其中之一就是“加快提升我国对网络空间的国际话语权和规则制定权”。这表明，我国实施网络强国战略的核心要素和重要基石之一，就是通过网络空间国际话语权和规则制定权的提升，成为网络空间国际法强国。

事实上，“大国外交必重法律”。只有真正成为网络空间国际规则的积极主导者而不是被动接受者，中国才能在网络事务中占据道义制高点，使自己的利益和诉求更好地得到国际社会的认同和支持。在网络空间国际法领域的无所作为，必将导致我国在网络空间国际博弈中的被动挨打。为此，有必要进一步提高参与国际规则制定的主动性和自觉性、加快提升我国对网络空间的国际话语权和规则制定权，进而为我国实施网络强国战略奠定坚实基础。

但不能不看到，我国在有效利用国际法这种国际通行话语的“软实力”方面还存在着若干问题和“短板”，严重制约着我国向网络空间国际法强国迈进。问题之一在于，与我国对网络空间国际法领域理论研究和政策建议的巨大需求相比，学界（包括智库）相应的供给能力十分有限，“供不应求”甚至“有求无应”的矛盾较为突出。尽管学者在这一重要领域“失声”和“缺位”的原因是多方面的，但显而易见的是，这不利于中国提升对网络空间的国际话语权和规则制定权、维护本国利益，也不利于中国作为网络大国为网络空间全球治理提供公共产品、践行国际法治。

由武汉大学国际法研究所策划、推出的“网络空间国际法文库”，正是为了服务我国加强网络空间国际法研究、积极参与网络空间国际规则制定的现实需要。武汉大学国际法研究所是1980年由教育部批准成立的中国高校第一个国际法研究机构，也是目前国内公认在国际法领域实力最强、影响最大的研究机构，2000年被教育部批准为普通高等学校人文社会科学重点研究基地，2015年被中宣部批准为国家高端智库首批试点建设单位。近年来，武汉大学国际法研究所的相关研究团队，不仅在国内较早投入网络空间国际法这一新领域的研究，对网络空间治理的相关国际法问题进行了具有一定开拓性的探索，而且以不同身份积极为我国相关政策制定和外交实践提供学术智力支撑，参与和推动网络空间国际规则制定，并已在国内外产生一定的社会影响力。

当然，学术乃天下公器。秉承开放、平等、协作的网络精神，本文库无意成为一校、一所的“局域网”，而是致力于推动学者之间以及学者与实务部门之间的互联互通，构筑面向学界和实务界所有同仁的“互

联网”。在成果形式上，网络空间国际法领域的专著、文集和译作都在本文库的涵盖范围内。在遴选标准上，本文库奉行唯学术水准是从的宗旨。为此，我们由衷欢迎所有专家学者惠赐佳作，使文库得以聚沙成塔、集腋成裘；我们也恳请广大读者提出宝贵的批评建议，使文库的质量能够日就月将、精益求精。

“花径不曾缘客扫，蓬门今始为君开。”网络空间国际法正处于发展的起步阶段，这为我国深度参与和积极影响相关国际规则提供了前所未有的契机，我国政府和学界在这个方兴未艾的领域都大有可为。诚盼“网络空间国际法文库”的推出，有助于汇集学界和实务部门专家学者的真知灼见，在网络空间国际法领域发出中国声音、提出中国方案、贡献中国智慧，为我国加快成为网络空间国际法强国尽绵薄之力。

是为序。

2017年5月

网络主权的辩证法

——代前言

一 问题背景

在网络空间所涉及的诸多问题中，网络主权问题无疑占据着特殊的重要地位。正如郝叶力研究员所说，“网络主权问题在网络空间国际规则中有着特殊的重要性，成为诸多问题树的树根，其他问题由此衍生。在这一问题上理清分歧、达成共识，才有国际合作的基础。”[1]从另一个角度看，正如国家主权原则是现代国际秩序和国际法的基石，网络主权原则也将是网络空间国际秩序和国际法的基石。谁能够掌握网络主权问题的话语权和主导权，谁就能够在网络空间秩序构建和规则博弈中占据制高点。从这一意义上说，当前国际上的网络主权之争也就是网络领域的主导权之争。[2]

同时，网络主权也是网络空间诸多问题中有着特殊复杂性的一个问题。从电子前线基金会创始人约翰·P.巴洛在《网络空间独立宣言》中向各国政府宣称“你们在我们居住的地方没有主权”，到一些西方国家推崇的网络空间“全球公域说”，再到中俄等国在《信息安全国际行为准则》中倡导“遵守《联合国宪章》和公认的国际关系基本原则和准则，包括尊重各国主权、领土完整和政治独立”，围绕网络主权的各种主张和争议不绝于耳。归根结底，穿梭于现实空间和网络空间的是同一群人（和同一批国家），究竟他们要遵守完全独立的两套规则体系还是现实空间“照亮”网络空间，规则被延伸或映射？与领土要素密切相关的主权是否可以向无边界的网络空间传递？现实世界和虚拟世界的主权

如何在互动中相互建构？在网络空间建立主权面临何种挑战？中国如何主张和建立国家的网络主权？这些都是值得学界当下思考的问题。[3]

其实，在围绕网络主权的各种讨论乃至争议背后，既可以看到由于技术因素而对网络空间本身以及国家主权如何适用于这一新空间的不同认知，[4]又可以看到出于不同的国家利益和意识形态、价值观，不同国家在网络主权问题上自觉或不自觉的“选边站队”。近年来中国有关网络主权的主张在西方世界受到的某些曲解、抹黑乃至“妖魔化”，其背后的意识形态和价值观因素可以说是不言自明的。

二 本书缘起

网络主权是中国关于网络空间全球治理和网络空间国际规则的核心主张之一。有鉴于此，加强对我国倡导的网络主权观的理论研究，进而借此澄清实践中的相关争议问题，已成为学界同仁不可回避的历史使命。一方面，能否提出一套能够融入国际话语体系、有可能得到普遍认可的网络主权表达框架，直接关系着中国在网络空间国际博弈中的形象和话语权；另一方面，由于网络空间全球互联互通的特点，国际社会只有在以网络主权为代表的网络空间治理若干焦点问题上达成共识，才有可能开展有效的国际合作，推动网络空间的共享共治。

对网络主权问题的上述认识和由此产生的使命感，成为本书12位作者策划和撰写本书稿的“集结号”。2016年下半年以来，本书主编和部分作者在多个不同场合进行正式或非正式讨论、交流时，产生的一个共同感受是：尽管网络主权问题已经成为一个热点话题，受到了我国政府和学界的大量关注，但客观地说，对这一问题比较系统、深入的研究还不多见，跨学科、多视角的共同研究尤为缺乏。由此，策划和撰写本书的设想逐渐萌生。

2016年12月17日，借着由本书主编担任首席专家的国家社科基金重大项目“中国参与网络空间国际规则制定研究”举行开题研讨会的机会，武汉大学国际法研究所邀请了来自中央网信办、外交部、上海国际问题研究院、中国现代国际关系研究院、中国信息通信研究院、中国社会科学院法学研究所和国际法研究所、北京邮电大学、北京师范大学、

四川大学、武汉大学等实务部门和科研机构的一批专家学者（包括本书的多位作者），在武汉举办了“网络主权研讨会”。[5]会议期间的深入研讨，进一步为本书随后的写作奠定了坚实的基础。

质言之，本书作为国内第一本关于网络主权问题的学术著作，缘起于一个“自发”和“自下而上”的写作计划。从工作单位来看，本书作者有的是高校和科研机构的知名专家学者，有的是相关实务部门的一线工作人员；从专业背景来看，本书作者分别来自法学、国际关系（国际政治）、公共政策等不同领域；从工作经历来看，本书作者有的已经在网络空间治理领域建树颇丰，有的则是近年来崭露头角的后起之秀；从具体观点来看，他们对网络主权的若干认识也不尽相同。如果一定要举出各位作者之间的共同之处，大概就是对网络主权问题共同的研究兴趣以及“位卑未敢忘忧国”的情怀。正是有赖于作者们在各种繁忙工作之余的宝贵支持和投入，本书才得以按期面世。

当然，必须指出的是，还有多位专家虽然由于种种原因未能加入本书的作者队伍，但他们以不同方式提供的真知灼见，同样是本书弥足珍贵的资源。

三 主要内容

除前言和附录外，本书共分为九章，大致按照“法理—政策—实践”的逻辑顺序来编排组织，但各章之间也存在若干彼此交叉和相互印证、对照之处。

国家主权是一个历史久远、历久弥新的概念，而网络主权正是这一概念在网络时代的新发展。在第一章“网络主权的历史维度”中，上海国际问题研究院鲁传颖副研究员对主权概念自古希腊以来的历史演进和功能及其在网络时代面临的挑战进行了分析。作者认为：主权是人类创造出来的权力概念，其内涵和条件随着时代的发展而不断演进。全球化冲击了主权概念的基础，并扩大了发达国家与发展中国家对主权概念的认知差距。而到了网络时代，国家在网络空间中的主权遭遇更加激进的侵蚀。一方面，政治、军事、文化、经济遇到了信息革命所带来的结构性挑战；另一方面，国家间、国家与非国家行为体在强制性、制度性、

结构性、解释性等四种网络权上的权力形态使得各方对网络主权的内涵和条件难以形成统一认知，导致各国的政策实践出现分野。

网络空间是一个与地理空间相对疏离的全新虚拟空间。现实空间既有的主权原则如何适用于这一新空间，是一个不容回避的根本性问题。在第二章“国家主权在网络空间的适用性”中，上海国际问题研究院杨剑研究员和方芳博士后指出：尽管互联网技术对国家主权概念的挑战前所未有，但互联网并非为主权概念敲响丧钟，而是更加丰富了主权概念的内涵和外延。具体而言，在构成网络空间的四个层面即物理层面、社会层面、逻辑层面和内容层面中，分别体现了现实世界国家主权在网络空间的延伸（物理层面和社会层面）、映射（内容层面）和特殊逻辑（逻辑层面）。在逐一剖析当前建立网络主权面临的三大挑战即国际社会对网络主权存在认识赤字、国家主权在网络空间适用模式受限以及国家主权在网络空间受到来自治理主体和客体多样性的挑战之后，两位作者提出：中国在主张网络主权时应坚守伦理基础、体现大国担当、坚持主张表述的一致性，并以科学的、和平的、发展的手段建立网络主权，向国际社会传递中国的全球治理观，提升中国在全球治理的影响力。

尽管国际社会在很大程度上已经接受国家主权适用于网络空间的主张，但不同行为体对其内涵和外延各执一词、难以调和的僵局并未根本改观。在第三章“三视角理论框架下的网络主权”中，中国国际战略学会高级顾问郝叶力研究员试图基于一个新的“三视角”理论框架，为破解这一难题另辟蹊径。郝叶力研究员认为：世界各国围绕如何进行全球网络空间治理、构建公平正义的国际规则存在的诸多争议，实质上是国家、国际和国民三大网络空间行为体各自从自身出发、谋求不同利益诉求的结果。因此，网络空间新秩序的建立，需要从三大行为体的视角审视全貌。2016年开始提出并产生较大反响的三视角理论，就是从国家、国际、国民这“三点”出发，引出三个边界条件，在稳定的三角形共视区内将网络空间分成“三层”——物理层、应用层、核心层；不同层面区别对待、求同存异，从而跳出单点迷思和二元对立，站在网络空间命运共同体的维度，以俯瞰的视角，科学把握排他性与让渡性的对立统一。

随着传统国际关系向网络空间的延伸，网络空间来到了一个秩序构建和规则博弈的关键时期，国家主权在网络空间适用就是其中最为复杂、最具根本性的问题之一。在第四章“网络空间秩序构建中的网络主权”中，武汉大学国际法研究所黄志雄教授认为：近年来，各国越来越多地在网络空间行使国家主权，从而使网络空间从早期的“去主权化”阶段，开始进入一个新的“再主权化”阶段。网络主权的确立，成为网络空间国际秩序和国际法制度构建中不可或缺的奠基之石。国家在网络空间的主权，不仅及于各国境内的网络基础设施，也及于网络空间的虚拟信息和数据。当前国际上的网络主权之争，本质上是网络领域的主导权之争。中国作为最早倡导网络主权的国家之一，应当立足于“网络空间命运共同体”理念，通过网络主权实现国家利益和人类共同利益的平衡，维护网络空间的互联互通、共享共治。

鉴于网络主权问题的重要性和复杂性，如何构造出既反映网络空间特征又体现中国特色的网络空间主权法律理论和制度体系，殊为不易。在第五章“网络空间主权的制度建构”中，中国人民大学法学院张新宝教授和许可博士后对这一颇具挑战性的难题进行了回应。他们认为：尽管网络空间主权已经成为我国处理网络事务的根本指针和制度基石，但其理论价值和法律意蕴均未得到充分阐明。面对与现实空间既区分又交融的网络空间，国家主权既要坚持对网络空间的适用性，反对消解主权的“网络自身主权论”和弱化主权的“多利益攸关方治理模式”，又要根据网络空间“互联、互通、互动”的特质适时而变。两位作者还试图从法律体系的观点探求网络主权的意蕴，即：在内部主权的层面上，建构基本立法权、简约行政权和类型化的司法管辖权；在外部主权的层面上，主张网络安全、平等参与、共同利用、善意合作的国际法新秩序；在此基础上，实现用网络空间主权建构法律制度，用法治框架落实网络空间主权。

在互联网和网络空间的发展过程中，网络的技术属性、媒体属性和社会属性逐一呈现，网络空间主权原则在网络法上的重要性也与日俱增。在第六章“网络法上的网络空间主权原则”中，北京邮电大学人文学院谢永江副教授基于网络空间的构成要素分析了网络空间与国家主权的关联性，明确网络空间不属于全球公域，进而阐述了将网络空间主权

原则确立为网络法基本原则的必要性，最后探讨了网络空间主权原则在网络法中的体现。作者认为：网络空间的现实性和社会性，决定了网络空间不是法外之地，而是受法律管辖的空间；网络空间是构建在各国主权之上的电子空间，不是排除国家主权管辖的全球公域，因此应该尊重各国自主选择网络发展道路、网络管理模式、互联网公共政策的权利。网络空间主权的内容，可以从传统国家主权的管辖权、独立权、防卫权、平等权等四个方面进行引申理解，但与传统国家主权的内涵相比，网络主权也的确存在若干特殊之处。

数据主权特别是数据本地化存储问题，是国际上有关网络主权争论的焦点问题之一，也是西方对中国网络主权观批评、非难颇多的一个问题。在第七章“数据主权的必要谦抑：以《网络安全法》数据境内留存规定为例”中，北京大学互联网发展研究中心高级顾问洪延青博士聚焦我国《网络安全法》第37条规定的数据本地化存储要求，探讨如何通过制度设计，实现发展和安全之间的平衡，以期厘清数据主权应当具备的必要谦抑，为解答网络主权行使过程中应当遵循的原则提供一定的基础。作者通过考察数据本地化存储的中外实践和对数据本地化存储的反对意见，着眼于数据本地化存储的严苛度模型、拟实现目标以及目的与手段的适当性和必要性关系，着力构建“数据本地化存储合理界限理论”，借此检视《网络安全法》的相关规定并提出进一步的立法建议。上述研究的特点和潜在意义，在于将比例原则的精神贯穿于数据跨境的监管过程之中，并使国家在行使数据主权的过程中，更好地在安全和发展之间取得平衡。

脱胎于冷战期间的互联网，在过去几十年中不断与现实世界融合发展，并导致了互联网全球化、跨边界特性与网络主权原则并存。在第八章“全球互联网关键资源管理中的主权问题”中，中国信息通信研究院研究员嵇叶楠和赵旭通过梳理美国在根区管理中施加的主权影响以及根区管理模式相应的历史沿革，分析了根区和顶级域等全球互联网关键资源管理中的主权问题。两位作者指出：作为国际互联网治理和全球互联网关键资源管理的核心平台，美国非营利机构ICANN遵循私营部门主导、多利益相关方治理的模式，政府部门的作用被其显著弱化，ICANN承担的根区管理及顶级域发展与管理政策制定职责无一例外地

与主权问题密切相关。积极把握国际互联网治理体系发展变革期的历史机遇，深度参与国际互联网治理和全球互联网资源管理规则制定，提升我国在相关领域的影响力和话语权，是维护我国网络主权，推动全球互联网关键资源管理向公平、合理、稳定、有序方向发展的重要举措。

2017年2月出版的《塔林手册》2.0版，在开篇第一章中以较大篇幅对网络主权的内涵、侵犯网络主权的法律标准以及主权豁免等问题进行了专门阐述。本书第九章“《塔林手册》2.0版的网络主权观”中，长期关注《塔林手册》2.0版编纂的外交部条法司徐峰副处长对该手册网络主权观的主要内容进行了分析和评述，认为《塔林手册》2.0版总体较1.0版以及现有的国际文件成果有所发展，对网络主权的阐述更系统、全面和具体；但由于《塔林手册》2.0版的封闭性和倾向性，其网络主权观在框架结构、具体内容上存在不足，该网络主权观的可接受性、适应性和可操作性也有待观察。作者最后指出：应当深入开展网络空间国际法特别是网络主权法律问题的研究，包括对《塔林手册》2.0版网络主权观的研究；同时，也有必要为进一步丰富我国网络主权观的法理基础、进一步完善中国网络主权观提供更多的法理和规则层面的思想和方案，更好地服务我国参与和引导网络空间全球治理和规则制定进程。

四 几点余思

已故著名国际法学家曾令良教授曾经在冷战后的1990年代提出“国家主权的辩证法”，认为“我们一方面不可被特定时期的突发事件和纷繁现象蒙住眼睛，看不清主权这块‘基石’，另一方面又不可忽视‘基石’周围的‘气候变幻’及其影响”；国家主权是神圣的，但又不是绝对的，“我们强调国家主权的神圣地位，并不等于将它推至极端”。[6] 这种关于国家主权的辩证法，对于研究和认识网络主权问题同样有着极为重要的指导意义。

在一定意义上，网络主权乃是现实世界国家主权“嫁接”到虚拟网络空间的产物，这就决定了网络主权一方面是传统国家主权的延伸，另一方面又必然需要适应网络空间的独特属性加以新发展。辩证、全面地考察网络主权较诸现实空间主权的“变”与“不变”，不仅有助于对网络主权的理论基础和法律内涵做出更为清晰、完整的解读，同时也有助

于澄清一些关于网络主权的偏颇甚至谬误的观点。

例如，那些基于网络空间的全球性、虚拟性等属性，根本否定网络空间国家主权存在的网络主权“虚无论”，不仅无视网络空间基础设施、人员和信息与现实世界之间的密切关联，也与近年来联合国内外形成共识的各种法律文件和各国普遍实践相悖，必须旗帜鲜明、理直气壮地加以批驳和反对。谢永江教授针对约翰·P.巴洛倡导的《网络空间独立宣言》指出：“巴洛乌托邦式的理想诞生于互联网发展的早期，《网络空间独立宣言》发表20年来的各国实践已经证明，互联网不是一个法外之地。巴洛幻想的一个免于政府介入的互联网早已被形形色色的网络入侵、网络攻击、网络犯罪等网络安全问题击得粉碎”，网络法贯彻网络主权原则，是实现网络空间依法有效治理的前提，是构建清朗网络空间的法律保障，有助于实现信息自由流动与维护国家安全、公共利益的有机统一”。[7]

与此同时，网络主权的行使，也不可避免地需要适应网络空间的全球性、虚拟性等独特属性。网络空间互联互通的特点，为各国带来了巨大的便利，加深了国际社会的相互依存，并成为持续创新的源泉。全球一网、全球共治的现实，要求各国政府在行使网络主权以及网民在开展各种网络活动时，都应当顾及国际社会的共同利益，维护网络安全和网络空间互联互通，维护网络空间命运共同体。正如杨剑研究员和方芳博士后所说，“作为崛起中的大国，中国对网络主权问题的思考既要考虑对本国利益的维护，也要考虑网络空间治理的全球需要；既要考虑今日战略环境和维护国家安全利益和发展利益，也要顾及今后国家利益全球布局的需要，并着眼于信息技术发展和网络社会功能发展的未来趋势”。[8]如果在网络主权问题上走向片面化、绝对化和极端化，最终致使网络空间的互联互通难以得到保障，那么，网络主权本身也将会“皮之不存，毛将焉附”。

同样地，对于全球互联网关键资源的管理，“在坚决维护网络主权的同时，还应充分尊重互联网诞生发展至今的基本运行机制，以保持全球互联网标识符的唯一性和统一性为前提，加强全球互联网关键资源管理相关事务的参与及合作，避免过度强调国家控制而导致根区分裂和互

联网碎片化加剧，实现网络全球化与网络主权之间的平衡”。[9]这种“平衡”的理念，也是贯穿本书各章的一个重要主题。[10]

总之，网络主权是现实世界国家主权和网络空间独特属性的对立统一，二者缺一不可。问题的关键，并不在于要不要讲网络空间的国家主权，而是如何科学、辩证地认识和落实网络空间的国家主权。

最后，用张新宝教授和许可博士后的下列表述来结束这个前言也许是合适的：

“面对历久弥新的主权观念和日新月异的网络空间，包容了自由、法治、民主的网络空间主权是中国给予世界的又一贡献。我们应不懈坚持之，努力践行之。……网络空间主权必将大行天下，最终铸成和平、安全、开放、合作的全球网络空间。”[11]

---

[1] 郝叶力：“三视角理论框架下的网络主权”，见本书第三章。

[2] 黄志雄：“网络空间秩序构建中的网络主权”，见本书第四章。

[3] 杨剑、方芳：“国家主权在网络空间的适用性”，见本书第二章。

[4] 例如，应当如何看待网络空间的虚拟性和现实性；国家主权传统上具有鲜明的地域属性和明确的边界，但网络空间的国家主权应当如何界定其“边界”；等等。

[5] 会议详情可见http：//fxy.whu.edu.cn/archive/detail/102373。

[6] 曾令良：《论冷战后时代的国家主权》，《中国法学》1998年第1期。

[7] 谢永江：“网络法上的网络空间主权原则”，见本书第六章。

[8] 杨剑：“国家主权在网络空间的适用性”，见本书第二章。

[9] 嵇叶楠、赵旭：“全球互联网关键资源管理中的主权问题”，见本书第八章。

[10] 例如，洪延青副研究员在探讨《网络安全法》数据境内留存规定时，正是着眼于厘清数据主权应当具备的必要谦抑，实现发展和安全之间的平衡。洪延青：“数据主权的必要谦抑：以《网络安全法》数据境内留存规定为例”，见本书第七章。

[11] 张新宝、许可：“网络空间主权的制度建构”，见本书第五章。

第一章

网络主权的历史维度

鉴于网络空间中的行为体在网络主权上的认知和实践存有广泛分歧，对主权概念的起源和演变做一个恰当梳理，有助于进一步厘清网络主权的理论和实践，从而为分析各国在网络主权上的政策主张提供依据。

主权是现代民族国家的基石，但主权概念自诞生之日起就是一个在争议中不断演进的概念。尤其是在全球化时代，主权的内涵和条件都在发生变迁，并引发了各国之间不同的认知观念和政策实践。网络空间的诞生再次向国家主权发起了全方位的挑战。国家作为主权的享有者，提出了网络主权这一概念，试图通过在网络空间伸张主权的方式应对挑战。但在网络空间权力格局中处于不同位置的国家在是否存在网络主权、网络主权的内涵上存有不同认知，并且政策上多有矛盾之处。本章试图从主权概念的源起、演变出发，对上述不同观点做出回应，并逐一考察网络发达国家、网络新兴国家和网络发展中国家在网络主权上的政策实践。

一 主权概念的演变、功能和挑战

网络主权是主权概念在网络时代的新发展，虽然外部条件发生了变化，但其内涵和逻辑并没有颠覆主权范畴。鉴于网络空间中的行为体在网络主权上的认知和实践存有广泛分歧，对主权概念的起源和演变做一个恰当梳理，有助于进一步厘清网络主权的理论和实践，从而为分析各国在网络主权上的政策主张提供依据。

主权由人类创造，因其被不同的国家赋予了不同的定义，有必要厘清主权概念的起源和历史，以便我们更为客观地了解其性质和内涵，判断其今后的发展方向。从政治学说史发展历程来看，主权概念的诞生和演变可以划分为古希腊时代、启蒙时代和全球化时代、网络时代四个阶段。

早在古希腊和古罗马时期，先哲们就对主权概念的内涵进行了相关的讨论。虽然这种讨论没有明确提出主权这一政治概念，但围绕着国家的产生、功能、政体的类型和对国家治理的讨论，实质上已涵括了我们今天所认知的主权概念，并为启蒙时期主权概念的明确提出奠定了基础。苏格拉底认为国家只有在统治者与被统治者各安其分、各司其职、互不僭越时才是正义的，统治者的智慧、勇敢、节制等高尚道德水平是其之所以成为统治者的原因。[1]亚里士多德认为，城邦是公民团体的组合，凡顾及全邦人民的共同利益而为之图谋优良生活者列为正宗政体；反之，仅图谋统治阶级的利益者为变态政体。[2]西塞罗认为，治理国家就是依据行政权威以及法律施加的惩罚迫使所有他人服从法规。[3]亚里士多德认为，人是政治性的动物。弗朗西斯·福山在《政治秩序的起源》一书中，从生物学角度再次确认了这一政治学观点。[4]

古希腊时期关于主权概念的讨论，已经包括了统治者与被统治者之间的关系和法律作为重要统治工具的思想。更为重要的是，这一时期的先哲认识到，统治者自我约束很有必要，一旦统治者将自己的利益凌驾于被统治者之上，就会丧失统治的合法性，成为一种亚里士多德称为“变态”的政体。[5]这一时期关于主权的讨论一方面旨在赋予统治者以合法性，要求被统治者服从；另一方面，也对“主权者”进行道德上和合法性的约束。

中世纪的宗教统治使得关于主权的定义更加复杂化，宗教与世俗、神权与王权、神法与自然法等一系列对抗与融合让主权的定义更加模糊，本章在此不做讨论。但中世纪的宗教对于世俗国家的观念认知产生了巨大的影响，导致了启蒙时期更为激进的主权定义的产生。让·博丹（Jean Bodin）以及其后的格劳秀斯、霍布斯等启蒙思想家，虽然被誉为启蒙之父，为现代民族国家的诞生奠定了理论基础，但他们一方面在与神权和宗教进行斗争，另一方面也深刻地受到了宗教的影响。乔治·萨拜因认为：“博丹的政治哲学乃是新旧政治哲学的一种奇特混合物……他既不属于中世纪，也没有进入现代。”[6]

法国启蒙思想家让·博丹最早提出主权概念并给出了定义。[7]他认为，国家存在的基本要素是共同主权者的存在，主权是“不受法律约束的、对公民和臣民进行统治的最高权力，不受时间、法律限制，永恒存在”。博丹的主权论可以被称为一种“君主主权论”。阿尔色修斯在部分接受博丹思想的基础上提出了“人民主权论”，认为国家行使主权，但主权属于人民，不能转让也不能交由一个统治阶级或某个家族所有。权力根据国家的法律被授予该国的行政官员。[8]格劳秀斯的贡献在于他讨论了主权对于国际关系的重要意义，他把主权定义为不受另一主权控制的权力，独立的国家间关系应当在国际法的指引下进行调整。[9]这是最早关于国家之间主权平等的理论，为威斯特伐利亚体系的建立提供了理论依据。

主权概念在威斯特伐利亚体系建立后被广泛接受为国家和国际关系的基石，为无政府状态下的国际秩序和处理有关国家间关系中的冲突与合作提供了法理基础，它深刻影响了国际关系的发展进程。霍布斯在《利维坦》中做出的定义将主权推向了极端。他将国家比作圣经中残暴的利维坦，而正是这只对臣民无条件享有主权的怪兽，才使得国家之所以成为国家。霍布斯认为，这个主权者是无所不能的。国家、政府、社会、法律、道德都必须集中在主权者的权力之中。只能在这种专制主义的利维坦和一盘散沙中做出选择，没有其他的路径可选。无论怎样，民众都不可以反抗主权者，因为这样会导致回到自然状态，回到“一切人反对一切人的战争”当中去。[10]

启蒙思想家们在主权这一概念上并没有达成共识。一方面，他们受到了中世纪宗教思想的影响；另一方面，他们的思想是对宗教教权的宣战。“利维坦”和“人民主权论”看似互相矛盾，但它们都有共同的反对对象，就是罗马教廷以及宗教对于世俗政治的干涉。最终，关于主权的学术思想在欧洲大陆得到了实践。象征着三十年战争结束的《威斯特伐利亚和约》，将主权思想落实到了国家间关系的准则当中。主权的对内统治和对外独立两项基本内涵正式被确立为现代民族国家和国际关系的基础。主权概念不仅将现代民族国家从中世纪的宗教统治中解放出来，对于后来的“反殖民”、“民族独立运动”也提供了宝贵的理论基础。特别是在二战结束和联合国成立以后，主权独立和平等逐渐成为国际关系的基础。

通过对主权概念的历史研究发现，主权概念的性质具有开放性，其内涵也在不断在演进。进入全球化时代以后，人员、资本、商品的跨国

流通日益频繁，传统的主权概念所定义的那种不能分割、不受挑战、至高无上的权力等性质在全球化的浪潮面前，就如同被炮火洗刷过的城墙，布满缺口与弹坑。在这种情况下，学术界对于主权的性质、功能、作用进行了重新的思考。[11]这一时期关于主权概念的学术研究也取得了诸多成果。有学者认为，传统的主权概念面临来自四个方面的挑战，即国家之上的超国家或准超国家行为体，跨国行为体，国家之下的次国家行为体，还有国际社会内部的一个倾向于总体霸权的超级强国。[12]也有学者从理论上创新，提出了主权的层次理论，主张从国际、国家和国内三个层面对主权进行更加深入的分析，以寻求在不同层次采取竞争或合作的策略。[13]还有学者将主权划分为国内主权、独立主权、国际法主权和威斯特伐利亚主权。[14]这些层次主权理论都为研究主权概念在全球化时代面临的挑战和回应提供了分析框架。

从国内主权的层次来看，它受到了新的政治参与者的挑战，工会、商业团体、非政府组织、媒体等都已经成为重要的政治参与力量。与以往相比，政治参与者更为广泛，更加多样。[15]这些多元政治参与者毫无疑问都会要求分享政府所掌握的主权。当然，在不同的国家，这种多元行为体参与的程度和广泛性有较大的差异。从国际层面来看，全球化对于国家在经济、政治、文化诸领域的主权形成了不同程度的侵蚀与削弱。国家的经济主权受到了国际经济组织、跨国公司以及其他国家宏观经济政策的制约；国家的独立自主、安全和领土完整等政治主权受到了来自国际社会强行干预的风险，这种干预往往具有某种合理性和合法性；国家的文化主权则在不断增加的单向交流沟通中受到了西方文化霸权的影响。这些现象，实际上导致了某些国家更加适应全球化，另一些国家对挑战的回应不及时。[16]

上述对主权在全球化时代遇到的内部和外部挑战的分析，表明主权的定义和内涵正在发生演变。而网络时代的来临加大了对国家主权的冲击，放大了各方在认知和实践上的差距，这给网络主权概念的界定和内涵厘清带来了更大的挑战。从实质上看，处于不同的政治体制、历史记忆和社会文化背景下的国家对主权存在不同的定义，这也为分析各国在网络主权上的矛盾提供了有益视角。

二 主权在网络时代面临的挑战

网络对主权的挑战是国家在全球化时代面临的巨大挑战之一。首

先，网络的开放、多元、互通、匿名等特性，使Web 2.0、大数据、云计算、3D打印等新技术、搜索引擎、社交网络等新的信息平台不断催生新的生产方式、生活方式、军事变革乃至社会结构变迁。其次，网络已经成为承载并联结各国政治、军事、文化、经济的载体，网络成为国家有效运转的中枢。最后，网络空间中的资源量急剧上升，网络权实质已经超越了单一工具性的作用，成为具有战略性意义的权力资源，并成为国家之间、国家与非国家行为体之间争夺的焦点。

网络带来的变化反映在网络空间新的权力形态及其分布的变化之上。网络时代的权力正在从国家行为体向非国家行为体转移，全球性的市场、公民社会正在分享过去由主权国家垄断的权力。如果我们把政治独立主权、军事安全主权、文化和价值观主权、经济自主主权视为国家的主权支柱的话，我们会发现，传统意义上的主权正在面临从理论到实践的巨大挑战。

首先，国家的政治独立主权正在受到推特（Twitter）、脸书（Facebook）等社交网络的挑战。社交网络具有开放、多元、互通、匿名等特性，并且聚集了大量活跃的政治参与分子，他们在社交网络上表达政治诉求，传播政治理念，积极地组织和动员各种形式的政治运动。在2009年伊朗大选中，反对派就曾利用社交媒体向组织成员和国内外民众发布运动信息，号召民众走上街头抗议。在抗议行动中，来自普通民众手机记录的文字、画面、视频实时向全世界推送，极具现场感和说服力，导致政府在事件应对上投鼠忌器，丧失主动。[17]在“西亚北非动荡”中，社交网络更是成为政治运动的核心和全球关注的焦点。美国华盛顿大学和美利坚大学的研究发现，社交网络在“西亚北非动荡”把旧政权拉下马的过程中发挥了重要作用。[18]同样，如果没有社交媒体的参与，“占领华尔街”运动的影响力和对政府造成的压力都会大打折扣。

其次，从军事安全角度而言，维护国家主权就是要保护国土境内的安全，拒敌于国门之外。但网络空间的匿名性和互通性使得传统意义上的国家边界不复存在，从网络上进入一国的成本和时间几乎为零，而且可以做到不被察觉。主权的合法性无法像在现实世界一样，给国家提供安全保障。2007年，爱沙尼亚因迁徙二战中阵亡苏军的纪念碑而引起俄罗斯强烈不满。随后不久，爱沙尼亚全国的网络关键基础设施受到了匿名黑客组织的大规模攻击，金融系统和政府网络以及其他关键信息基础设施被迫停止提供服务，爱沙尼亚政府不得不关闭通往外界的网络接

口，造成了难以估量的政治和经济损失。对此，爱沙尼亚政府既无法依据主权不受侵犯的原则向国际社会控诉，也无法使用常规手段进行武力报复，甚至连对手是谁都没有办法确定。2011年媒体报道，伊朗核电站遭受“震网”（Stuxnet）网络病毒攻击，导致数千台离心机损毁。《纽约时报》随后对这一事件进行报道，原来“震网”病毒是美国政府“奥林匹克计划”的一部分，直接由奥巴马总统下令实施。[19]随后不久，伊朗也通过“电磁战”捕获了美国入侵的“捕食者”无人机，也算是以彼之道还彼之身。作为网络战的经典案例，美伊两国政府并未派一兵一卒进入对方境内，但一场损失巨大的网络战就这样悄无声息地开始和结束。

再次，网络对于文化和价值观主权的侵袭一直存在。网络的一元性和文化的多样性之间存在激烈的冲突。网络一元性主张网络空间是由西方发明创造，空间中的标准、价值观乃至文化都建立在西方文明的基础之上，其他国家既然接入了互联网，就应当接受网络的主导文化，不应当把自己的文化带入网络空间中。[20]在这一大的背景下，发展中国家的文化主权受到了西方文明和价值观的严重冲击。最明显的案例就是国家丧失了对国民使用的网站上的信息内容进行管理的能力。在2013年9月召开的东盟地区论坛网络安全会议上，马来西亚网络安全首席执行官Zahri Yunos在大会发言中就举了两个极具代表性的案例。一是有人在网络上对皇室进行侮辱，另一个是侮辱穆斯林文化。[21]两者都违反了马来西亚的相关法律，但这样的事情在网上经常发生，因为网络服务器和网站位于其他国家境内，马政府同存有大量类似信息的脸谱网站之间进行交涉，要求删除并禁止类似的信息发布。但脸谱网站却以保护信息自由为名而拒绝马政府的请求。[22]

最后，经济主权是国家主权的重要支柱，货币发行权又是重中之重，然而比特币的诞生并迅速发展向国家的经济主权发起了挑战。比特币是一种完全脱离政府和银行掌控、总量“封顶”、可实时兑换法定货币且价格由供求决定、被认为有可能彻底改变全球金融行业格局的数字货币。[23]比特币问世后受到了市场的热捧，币值从5美分上涨到最高1000美元，被誉为是“电子黄金”。虽然各国政府对比特币持质疑甚至反对态度，但越来越多的商家开始接受比特币，打开了比特币的流通渠道。[24]除此之外，网络金融、电子商务的蓬勃发展不仅给传统的商业带来了挑战，也给国家的金融监管和税收监管体制带来了难以克服的困难。

三 网络主权和网络权

国家作为唯一享有主权的行为体，为了应对网络时代主权所遭遇的挑战，提出了网络主权这一概念，试图通过明确网络主权定义、行使网络主权来做出回应。但网络主权概念一经提出，就在各国之间引起了巨大的争议。首先，网络发达国家和网络发展中国家在网络空间有没有主权问题上存有争议。前者认为网络空间属于全球公域，后者认为网络空间具有主权属性。其次，空间中的非国家行为体认为应当限制国家行使主权，由市场和社会对网络空间的运营和管理负责，并提出了网络空间治理的“多利益攸关方”管理模式。最后，网络技术还在不断地推陈出新，对于国家、社会所造成的变革尚在进行中。在这种情况下，各方都难以对网络主权提出一个概念明确、内涵清楚、逻辑清晰的定义和被广泛接受的规范。

虽然网络主权的条件和内涵还有待进一步研究，但传统主权的定义告诉我们，作为一种重要权力形式，它是对国际和国内各种权力的提炼和集中。因此，我们可以考察网络空间，并从中归纳网络空间中的权力形态，进而分析网络主权的条件和内涵。目前对网络空间具有代表性的定义分别来自美国政府和社会学大师曼纽尔·卡斯特（Manuel Castells）。前者将网络空间定义为由互联网、电信网络、计算机系统和嵌入式处理器组成的相互依赖的信息基础设施。[25]卡斯特在《网络社会的崛起》中，则将网络空间定义为由历史性的社会关系赋予空间形式、功能和社会意义的物质产物。[26]根据上述两种具有代表性的定义，可以将网络空间中的权力归纳为具有强制性（compulsory）、制度性（institutional）、结构性（structural）、解释性（interpretative）特性的四种不同形态的权力。[27]它们涵盖了网络基础设施的所有权、互联网的管理权、网络文化管理权以及在网络空间制定和执行法律法规的权力。

强制性网络权和制度性网络权主要反映了国家行为体之间的网络权力关系。强制性网络权是建立在进攻和防御网络能力之上的权力，是指通过网络对他国实施惩罚的权力。如伊朗受到的“震网”病毒攻击和爱沙尼亚和格鲁吉亚网络关键基础设施受到的攻击，都是他国行使强制性网络权的案例。国际社会对于强制性网络权尚缺乏明确的界定和规范，在上述的案例当中，各国政府都不承认自己发动了网络攻击，甚至是受害者在某些情况下也保持了沉默，国际社会更是难以知晓事件的来龙去

脉。但通过媒体的报道和研究分析，学术界基本都认可上述的事件就是行使强制性网络权的案例。制度性网络权是指通过控制网络空间当中某些正式的和非正式的机构，对国际互联网进行管理的权力。美国通过掌控互联网名称与数字地址分配机构（ICANN）建立对国际互联网的管理权，并将其作为一种权力对他国进行惩罚。美国曾经通过停止对特定域名的解析，使其他国家在互联网上消失，从而造成巨大的政治、经济损失，关键时还会造成社会动荡、政权更迭。2003年美国政府在对伊拉克发动战争前，指令ICANN停止对以.iq结尾的伊拉克国家顶级域名的解析服务，使得伊拉克境内的网站全面停止提供服务，给伊拉克造成了严重的社会、政治、经济混乱。[28]

结构性网络权和解释性网络权与国家行为体和非国家行为体在网络中的权力形态有关。目前在国际上比较有影响力的多利益攸关方模式认为，网络空间主体既包括国家行为体，也包括公司、非政府组织、学术团体乃至个人用户等非国家行为体，后者对于网络空间的开放、繁荣、透明与国家同等重要，两者共同构成了网络空间的权力体系。因此，国家的作用应当受到限制，市场和社会应当在网络的运营和繁荣中发挥主要作用。但随着非国家行为体在网络安全和网络犯罪问题上的束手无策，国家的力量正在彰显，权力的结构正在朝着国家的方向转移。解释性网络权是国家的政治权力，包括对意识形态、政治事件的解释权力，这种权力在现实世界中由国家所垄断。但网络给非国家行为体提供了分享这种主权权力的平台。如社交网络为网民成为积极的政治参与者提供了话语权、舆论场和意见领袖，同时削弱了政府的权威。在“西亚北非动荡”中，解释性网络权的丧失是导致当局失去对政局控制并最终下台的主要原因。[29]

四种网络权的性质及其内涵，展现了网络空间中独特的权力形态和生态。强制性网络权和制度性网络权主要是由于网络的无边界而网络基础设施和管理机构被特定国家垄断而产生。网络强国倾向于利用自身优势，进一步模糊网络边界，把自己的网络权延伸到弱国空间内。结构性网络权和解释性网络权可以被视为包括发达国家和发展中国家在内的所有国家行为体所面临的挑战，主要表现为网络技术和空间特性推动了国家的权力、权威被非国家行为体分享。

四 各国在网络主权上的主张及展望

网络空间中的国家行为体按照权力分布可以划分为网络发达国家、网络新兴大国和网络发展中国家，由于在网络权力格局中的位置不同，这三类国家在网络主权上的立场和观点，既有矛盾也有相似之处。

第一，网络发达国家由于在强制性网络权和制度性网络权上占据了主导地位，倾向于减少网络主权对网络权的限制。以美国为例，其认为网络空间属于全球公域，国家不应当在网络空间中行使主权。但实际上，美国的战略目标是通过在全球公域中建立霸权，攫取这些没有明确国家属性的空间的资源与权力；同时，限制美国竞争对手进入有关空间，获取政治、经济、军事上的资源。[30]没有了网络主权这层保护，美国就可以通过在强制性网络权和制度性网络权上的优势，在网络安全上威慑他国，并且随意进入并控制他国网络资源。“棱镜门”事件向世人展示了美国如何通过全球信息基础设施和大型信息企业开展情报收集和信息监控工作。美国就像编织了一张张大网，拦截全球网络上的信息数据。[31]但在涉及具有国内属性的结构性网络权和解释性网络权方面，美国是积极行使网络主权的开创者和领先者。“9·11”之后，美国政府不顾企业和民众反对，加强了网络审查制度，特别是借反恐之名，通过了《爱国者法案》加大对网络和通信的监听力度，并且还在不断地推出诸如《网络情报共享和保护法案》（CISPA）、《禁止网络盗版法案》（SOPA）、《防止实时线上对经济创新能力的威胁和对知识产权盗窃法案》（PIPA）等，加强在网络空间行使主权。简而言之，以美国为首的网络发达国家在网络空间的主权属性上采取了“双重标准”。当美国在网络空间收集他国信息，干涉他国网络政策时，则宣称网络空间的“全球公域”属性。当需要加强网络监管，推动国内的公共—私营（Public-Private）合作时，则认为网络空间是主权领域，即使网络基础设施是私营部门所有，国家仍对网络空间有管辖权。

第二，网络新兴大国认为网络空间具有明确的主权属性，为了维护网络安全和社会稳定，国家应当在四种网络权的基础上建立并行使网络主权。网络新兴大国指的是一些在网络技术、网络能力和网络基础设施上具有强大实力的国家，这些国家正在通过加大对网络领域的投入，分享发达国家在网络空间中的支配地位。俄罗斯作为网络新兴国家之一，在网络主权上的认知具有一定的代表性。俄罗斯认为，网络基础设施位于国家的物理疆域中，每个国家都有权根据国内法律管理网络空间，并且设定自己的网络标准。2011年，俄罗斯联合中国等上合组织成员国，向第六十六届联大提交了《信息安全国际行为准则》，[32]认为互联网有关的公共政策问题的决策权是各国的主权，应尊重各国在网络空间中

的主权，尊重人权和基本自由，尊重各国历史、文化和社会制度多样性等。除此之外，网络新兴大国更注重通过竞争方式在网络技术、网络标准和网络技术上抵御网络发达国家对网络权的垄断；并且积极立法规范和限制境内外的非国家行为体在网络空间中的行为，将其纳入政府的管理当中。俄罗斯联邦法律规定，外国资本不能控股境内重要的信息企业、网站，如Yandex、Mail.ru，不能和社交网站“联系”等。[33]

第三，网络发展中国家在网络权力分配格局处于不利的局面，导致网络主权受到的挑战和侵蚀最为严重。网络权与国家在网络空间的技术能力、网络使用能力直接相关，由于互联网及相关的技术都是在西方国家诞生和发展，发展中国家只能被动地接受相关的网络技术和标准，使得自己处于不利的地位。为了伸张网络主权以应对不利局面，首先，发展中国家通过积极参与网络空间的全球治理，寻求确立网络主权的合法性，以国际法律、法规来弥补自己在网络技术和网络能力上的短板。[34]其次，发展中国家积极推动联合国、国际电信联盟等国际组织在网络空间建章立制中发挥作用，通过国际组织平衡和制约西方网络权力渗透导致的对主权的侵蚀。再次，加强与网络新兴大国之间的合作。两者同属于发展中国家阵营，在网络主权上的认知接近，在很多国际性的谈判中都拥有相同的立场。2012年在迪拜举行的国际电信联盟大会上，89个发展中国家与新兴国家协调一致，要求将“成员国拥有接入国际电信业务的权力”和国家对于信息内容的管理权写入《国际电信规则》。[35]此外，双方在通过技术转移缩小数字鸿沟方面业已开展了诸多合作，并为今后的进一步合作奠定了基础。[36]

当然，上述三个群体内部在观点和立场上也不完全一致，存在各种矛盾。然而，在网络空间建章立制的大背景下，考察网络发达国家、网络新兴大国和网络发展中国家在主权问题上的立场和主张，可以为当前网络空间建章立制确立相应的基础，维护网络空间的开放、稳定、繁荣。

---

[1] 参见〔古希腊〕柏拉图《理想国》，商务印书馆，1986，第145～176页。

[2] 参见〔古希腊〕亚里士多德《政治学》，商务印书馆，1965，第132～145页。

[3] 参见〔古罗马〕西塞罗《国家篇 法律篇》，商务印书馆，1999，第11～23页。

[4] 参见〔美〕弗朗西斯·福山《政治秩序的起源》，广西师范大学出版社，2012，第31～38页。

[5] 参见〔古希腊〕亚里士多德《政治学》，商务印书馆，1965，第236～313页。

[6] 〔美〕乔治·萨拜因：《政治学说史》（下卷），邓正来译，上海人民出版社，2010，第77页。

[7] 参见〔法〕让·博丹《国家论》六卷，转自〔美〕乔治·萨拜因《政治学说史》（下卷），邓正来译，上海人民出版社，2010，第75～90页。

[8] Althusius，Die Philosophie der Aufklaung，转自〔美〕乔治·萨拜因《政治学说史》（下卷），邓正来译，上海人民出版社，2010，第95～97页。

[9] 〔美〕乔治·萨拜因：《政治学说史》（下卷），邓正来译，上海人民出版社，2010，第98页。

[10] 参见〔英〕霍布斯《利维坦》，商务印书馆，2012，第133～141页。

[11] 参见蔡拓《全球化的政治挑战及其分析》，《世界经济与政治》2001年第12期。

[12] 参见时殷弘《论民族国家及其主权的被侵蚀和被削弱——全球化趋势的最大政治效应》，《国际论坛》2001年第4期。

[13] 参见陈玉刚、俞正梁《国家主权的层次分析》，《欧洲》2001年第3期。

[14] Stephen Kranser，Sovereignty：Organized Hypocrisy，Princeton University Press，1999.

[15]〔美〕弗朗西斯·福山：《政治秩序的起源》，广西师范大学出版社，2012，第471页。

[16] 参见蔡拓《全球化的政治挑战及其分析》，《世界经济与政治》2001年第12期。

[17] 鲁传颖：《中东动荡中的社交媒体》，《上海外事》2011年第6期。

[18] Philip N.Howard，Opening Closed Regimes：What Was the Role of Social Media During the Arab Spring? http：//pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf.

[19]“Obama Ordered Wave of Cyber-attacks Against Iran，” New York Times，1 June，2012，http：//www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[20] 鲁传颖：《试析当前网络空间全球治理困境》，《现代国际关系》2013年第11期。

[21]《我国首次举办东盟地区论坛网络安全研讨会》，2013年9月13日，http：//www.mfa.gov.cn/mfa_chn/wjbxw_602253/t1076333.shtml。

[22] 参见Zahri Yunos，Role of States in Cyberspace，Speech at ASEAN Regional Forum Workshop on Measures to Enhance Cyber Security-Legal and Cultural Aspects，11-12 September，2013，Beijing，China。

[23] 吴洪等：《疯狂的数字化货币：比特币的性质与启示》，《北京邮电大学学报》（社会科学版）2013年第3期。

[24] 参见中国人民银行《关于防范比特币风险的通知》，http：//www.pbc.gov.cn/publish/goutongjiaoliu/524/2013/201312051531568

[25] The White House，Cyberspace Policy Review：Assuring a Trusted and Resilient Information and Communications Infrastructure，http：//www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_f

[26]〔英〕曼纽尔·卡斯特：《网络社会的崛起》，夏铸九、王志弘等译，社会科学文献出版社，2003，第504页。

[27] David J. Betz and Tim Stevens，Cyberspace and the State：Toward a Strategy and the State，Routledge，2011，pp. 42-53.本章根据主权学说对理论架构做了修订，用解释性网络权替代了生产线网络权（productive cyber power）。

[28] 杨剑：《数字边疆的权力与财富》，上海人民出版社，2012，第208～211页。

[29] Philip N. Howard，Opening Closed Regimes：What Was the Role of Social Media During the Arab Spring? http：//pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf.

[30] Barry R. Posen，“Command of the Commons：The Military Foundation of U.S. Hegemony”，International Security，vol.28，no.1（Summer 2003），pp.5-46.

[31] The Guardian，Prism，11 June，2013，http：//www.theguardian.com/world/prism.

[32] 参见中俄等国向第六十六届联大提交的《信息安全国际行为准则》，http：//www.fmprc.gov.cn/chn//pds/ziliao/tytj/t858317.htm。

[33] 王路：《世界主要国家网络空间治理情况》，《中国信息安全》2013年第10期。

[34] 鲁传颖：《发展中国家积极参与网络空间治理》，《中国社会科学报》2013年10月21日第1版。

[35] BBC，“US and UK Refuse to Sign UN’s Communications Treaty，” 14 December，2012，http：//www.bbc.co.uk/news/technology-20717774.

[36] 杨剑：《新兴大国与国际数字鸿沟的消弭——以中非信息技术合作为例》，《世界经济研究》2013年第4 期。

第二章

国家主权在网络空间的适用性

纵观信息社会化进程，主权一直是一个“进行中”的概念。互联网技术发展并非为主权概念敲响丧钟，而是更加丰富了主权概念的内涵和外延，是国家主权在网络空间的延伸、映射和特殊逻辑。

16世纪法国政治思想家让·博丹第一次系统地提出主权理论。17世纪中叶形成的威斯特伐利亚体系进一步完善了近代意义的国家主权概念。国家主权包括对内最高权和对外独立权，具有对内和对外的双重性。人民、土地、政府、主权是构成国家概念的四个基本要素。[1]从国家的四个基本构成要素可见，威斯特伐利亚体系中的主权概念与现实世界的地理空间具有一定关联。然而，随着互联网技术的发展，网络空间得以构建。这一空间是全新的虚拟空间，与地理空间相对疏离，甚至有人发出《网络空间独立宣言》[2]，认为网络空间是“一个独立于国家之外的新空间”[3]，宣称“传统的基于地理边界的法律和治理在网络空间中不适用”[4]。

穿梭于现实空间和网络空间的是同一群人，究竟他们要遵守完全独立的两套规则体系还是现实空间“照亮”网络空间，规则被延伸或映射？与领土要素密切相关的主权是否可以向无边界的网络空间传递？现实世界和虚拟世界的主权如何在互动中相互建构？在网络空间建立主权面临何种挑战？中国如何主张和建立国家的网络主权？这些都是值得学界当下思考的问题。

一 信息社会化对国家主权概念的影响

（一）经济全球化对国家主权概念的挑战

国家主权是特定历史条件下的产物，随着时空的变化而演进。全球化挑战国家主权的现实，引发了学者们对传统的国家主权概念的再思考。以英国政治思想家哈罗德·拉斯基（Harold Laski）为代表的学者们认为，国家主权不是绝对集中在政府手中，而是分散于国内各种政治力量中。[5]在全球化时代，国家主权通过“向上”或者“向下”的转移可以分割或让渡。[6]以英国社会学家安东尼·吉登斯（Anthony Giddens）和美国“新治理论”学者詹姆斯·罗西瑙（James Rosenau）为代表的学者们认为，国家主权虽然在国内政治生活和国际事务中依然处于核心地位，但因受到全球化的强烈冲击已被严重削弱。[7]以德国社会学家乌尔里希·贝克（Ulrich Beck）和德国思想家尤尔根·哈贝马斯（Jurgen Habermas）为代表的学者们更是认为，在全球化时代国家主权遇到了困境，已成为一个过时的概念。[8]

无论是“国家主权多元论”，还是“国家主权弱化论”，抑或是“国家主权过时论”，不可否认的是在经济全球化背景下，国家主权遭遇了一定程度的侵蚀、让渡和削弱。经济全球化进程中，国际组织、跨国公司、非政府组织等在世界经济和国际政治活动中的实践对国家主权产生侵蚀性影响。出于本国经济发展和实力积累的需要，国家行为体在调整国际压力和发展机会的矛盾时，主动在主权方面进行一定程度的让渡。在参与国际组织和履行国际义务时，国家主权会受到不同程度的削弱。

（二）信息社会化对国家主权概念的拓展

除了资本全球化、产品全球化，经济全球化的另一重要方面就是通信全球化。[9]通信全球化从信息流动的层面打破了传统的国家领土疆界的束缚，不断拓展国家主权的概念空间。信息技术对国家主权概念的影响，并非始于互联网技术的兴起。

1.纸质媒介

印刷媒体时期，纸媒通过信息传播方式在国家主权的对内面向产生影响。国家可以限制和禁止不利国家统一的信息通过纸媒被传播，因此，印刷媒体通过重塑国家人格和强化身份认同，使得国家被重新想

象，成为观念世界的“被想象的共同体”。[10]由于纸质媒介必须通过地理意义的边界才可进入另一国的领土范围，加之媒介输入国限制或阻止印刷媒体进入的成本较低，因此，印刷媒介对国家主权对外层面产生的负面影响十分有限。

2. 无线电通信和卫星技术

如果说印刷媒体对国家主权概念的影响总体上是正面的，那么与之相比，国际无线电通信和卫星技术对主权概念形成了较大冲击。无线电技术虚化了国家地理意义上的边界，国家控制不利信息进入的难度加大，主权受到对内和对外的侵蚀。与无线电技术的信息传播行为不同，利用卫星技术进行的信息传播不再受地理距离的限制，信息传递的范围更加宽泛。信息传递的方式亦不再局限于语言，可通过图像扩大受众范围。卫星技术不仅传播信息，还能收集信息。卫星技术更加虚化了领土边界概念，国家不仅需要控制不利信息进入，而且要防止自身信息泄露。主权在更大程度上受到对内和对外的侵蚀。[11]

3. 互联网技术

互联网技术对主权概念的挑战前所未有。互联网的去中心特征和阻隔信息输入的低廉成本，使得互联网平台的信息传播具有更强的渗透性。传统意义上的国家边界被强烈虚化。国家控制信息流动的难度，以及交互式和参与式的媒介信息传递方式最大程度地挑战了国家对内和对外的主权。具体表现在：第一，松散的非政府组织具有开放的活动空间，其发挥的作用日益重要，传统的国家主权概念趋于式微。第二，网络发达国家较强的信息输入能力和网络边缘国家较弱的信息接收控制能力都对国家的意识形态和政治权威构成挑战，从外部弱化了国家主权。第三，国家内部分裂势力、民间组织、私人企业通过互联网传播的“时空压缩”[12]特征对公民的政治认同形成威胁，造成了国家主权从内部的弱化。

纵观信息传播技术的发展历程，每一次的技术革新对主权概念都产生了不同程度的影响。主权概念不断被拓展，在受到信息技术数次冲击之后更加丰富。然而，进入互联网时代，网络一度被广泛视为国家和国家主权的挑战者甚至终结者。究竟如何理解网络主权的概念？虚拟世界的主权与现实世界的主权之间呈现何种关联？

二 国家主权在网络空间的延伸、映射和特殊逻辑

（一）网络主权的证成

1. 法理基础：对威斯特伐利亚体系主权概念的发展

在信息技术高速发展的时代，主权过时或主权终结的论调其实是将主权视为一个静态的概念。究竟如何理解主权概念？

自《威斯特伐利亚和约》签订以来，近代意义的国家主权概念形成，并逐步在国际交往中从不同侧面衍生其新的内涵。从威斯特伐利亚时代到20世纪中期可谓“政治主权”时期，各国在国际交往中政治霸权凸显，西方国家与殖民地国家、落后国家之间的交往强调国家独立和安全。20世纪中期以后，各国经济交往渐趋频繁，发达国家对发展中国家掠夺资源和抢占市场。国际经济领域霸权彰显，致使经济主权被关注。20世纪90年代后，文化的冲突和融合逐渐步入国际舞台并愈演愈烈。文化主权概念成型。[13]政治主权、经济主权、文化主权并不是新的主权概念，它们的代际演进恰恰说明主权是动态的概念，而非静止的概念。

《威斯特伐利亚和约》指涉的领土范围是以现实存在的、有形界线为依据的陆地上的边界。但是领海和领空如何界定？在17世纪和18世纪，先后有国家以枪和火炮的射击距离作为领海边界；直到现在，领空仍以航空器最大飞行高度为边界，地下以技术能达到的最大深度为边界。[14]从某种意义上讲，技术进步拓展了国家疆域，在各个空间延伸了主权管辖的“领土”。主权是一个开放的概念。网络主权也并非新一代的主权概念，而是对威斯特伐利亚体系主权概念的发展。

可见，主权概念随着国际格局演变和科学技术进步而不断衍生出新的内涵。主权既是一个政治概念，亦是一个法律概念。无论是前者抑或后者，都是一个反映关系的概念，是一个开放的、动态的、发展的概念。

2. 治理实践的现实基础：网络空间发展的必然趋势

网络空间“去主权化”现象在互联网发展初期显露端倪。在20世纪90年代美国“新治理论”学者罗西瑙主张网络空间自治论，将政府排除

在外，由互联网社群治理整个网络空间。[15]约翰·P.巴洛（John Perry Barlow）于1996年在达沃斯论坛发表著名的《网络空间独立宣言》，将网络空间视为一个独立于国家之外的、自我治理的新空间。[16]深受巴罗思想的影响，戴维·约翰逊（David Johnson）认为传统的基于地理边界的法律和治理在网络空间中不适用。[17]进入21世纪，劳伦斯·莱斯格（Larance Lessig）主张代码治理论，认为代码是网络空间的法律并主导着权力分配。[18]由于互联网的全球性和工程师团体在治理中发挥了关键作用，最开始的互联网治理被称作“没有政府治理”的一种全球治理实践。

多利益攸关方治理模式最早于2001年在信息社会世界峰会上作为一种新治理思路被提出，其内涵后来被重新定义。杰瑞米·马尔柯姆（Jeremy Malcolm）认为，多利益攸关方治理应是政府、市场和非政府团体各司其职、共同应对互联网治理中出现的问题。[19]该领域领军人物米尔顿·穆勒（Milton Mueller）进一步指出：国家与网络之间是一种控制与被控制的动态关系；互联网治理已经成为国际政治冲突的来源，必须建立一系列国际性的机制来规范国家参与治理。[20]由于网络空间全球治理的议程扩容、网络犯罪和战争等安全议题涉及国家间关系、云计算和大数据等技术，事关国家软实力，国家的治理中心地位和主权概念重新回归。

国家行为体对内通过建立和完善网络监管的法律体系，明确主权在网络空间的管辖范围和方式；对外通过制定网络安全战略，确立主权在网络安全中的主体地位。[21]国家主权的理念和实践占据网络空间治理主流话语体系。网络空间治理经历了从“去主权化”向“再主权化”的转变过程。

从法理基础和治理实践的现实基础可见，国家主权在网络空间的适用兼具合法性及合理性。

（二）网络主权的内涵和外延

网络空间与现实空间的基本形态和存在方式差异很大。网络空间由四个层面构成：（1）物理层面，物质可见部分的基础设施、硬件、卫星、电缆等；（2）社会层面：现实空间与网络空间通过人实现两个空间相互延展以及互动过程中的人、物和社会结果；（3）逻辑层面：管控网络中数据交换的协议、软件、版本等编码方案；（4）内容层面：

数字化内容的制作、储存、获得、复制、交换和分发等。网络主权的内涵和外延可理解为国家主权在这四个层面的适用。

1. 国家主权在网络空间的延伸

国家主权在物理层面和社会层面可得到有效延伸。存在于物理层面的有形的基础设施，比如计算机硬件、网络设备、电缆等，都是在主权明确划分的自然空间实际存在的，因此现实空间的主权原则可直接在物理层面得以适用。[22]

社会层面是指网络数字内容基于特定的逻辑关系，通过具有媒介作用的硬件（比如键盘、鼠标、显示器、扬声器、传感器、数据采集器、摄像录音设备等），与作为用户的人之间的直接或间接的互动，显示了现实空间与网络空间相互延展和互动的时空过程。用户通过终端的显示屏将镜像的数字内容跨越时间和地域与其他终端上的人进行互动。处于具体地域和司法管辖域中的人通过网络终端对其他司法管辖域中的人产生经济方面或社会方面的影响。这些影响可以事先具有给定的指向性，或不具有给定的指向性。在网络空间发生的每一次交易或互动，其边界都是有限的、可查的。上述两个层面的地域相关性，使得与主权司法管辖相关的属地原则、属人原则、保护原则和后果原则得以相应体现及应用。

国家主权在这两个层面的适用可具体包括：对境内相应的关键基础设施的管辖权；对关键基础设施中以及依托其自然领土空间而存在的电磁空间中的信息有序流动的治理权；面向网络空间中的技术活动、生产活动和社会活动的立法规范权，保护空间中的数据、设备、信息安全，预防和打击网络犯罪，明确非国家行为体的行为规范和相应的权益、责任、义务，保障本国网络空间的安全利益；承担国际网络空间有序运行的国际义务和参与国际合作的独立决策权。

但国家主权在这两个层面的应用会衍生一些新问题，比如关键基础设施的私人所属权与国家所属权之间的内部法律关系，国家主权与网络空间国际共享基础设施之间的关系和对外权利问题，网络空间司法管辖中经常出现的重叠管辖的问题。

2. 国家主权在网络空间的映射

网络空间的内容层面集中了与国家主权相关的虚拟空间资源和内容资源。它们在形态上不同于现实空间中基于地域的自然资源。现实空间存在着矿藏资源、森林资源、海洋资源，而网络空间存在着带宽资源、电缆容量资源、储存资源、运算资源、数据资源、无线电频谱资源等物化的资源，以及与用户密切相关的市场资源、内容资源和注意力资源等社会资源。内容层面的资源是网络空间中最重要的资源，它反映了一个民族的技术能力和信息化水平，反映了一个国家在网络空间中积累的资源和财富，同时也反映了一个民族文化遗产和价值观念数字化的程度，体现了一个民族在数字化时代的传承和文化软实力。它在形态上表现为在网络空间生产、加工、存储、流通的数字化的文字、数据、多媒体等内容。基于主权原则，国家可以宣布拥有对相应网络空间中数据和信息内容的产权和处置权。内容资源具有流动性，它与硬件之间具有可分离性。网络空间内容资源所具的独特性会导致一种特殊现象，即数字化的内容资源的主权极有可能依附主权归属于他国的基础设施。具备技术方面的获取能力不等同于具备获取内容和数据资源的合法性。一个信息技术公司因拥有巨大的用户群而掌握海量的用户信息，该公司具备技术能力获取这些用户数据并从中获利，但这些行为仍可能是违法的。同样，一个技术优势国家可在网络空间中获得全球各种内容、数据，如果这些内容的主权明确归属于他国，那么该国的获取和滥用的行为就可能侵犯了他国主权。

随着网络空间中数据、信息资源的战略意义日益显现，世界主要国家愈发重视对国家重要信息内容开发、储存和流动的监控。在大数据和云计算时代，各个国家行为体围绕全球内容资源的开发、占有、分析、运用开展了激烈的竞争。对网络空间的信息内容行使国家主权具有战略性意义。国家需要保留其对本国信息资源进行生产、开发、利用的权利，保留保护本国网络空间的信息内容不被外部势力非法占有和利用的权利。没有主权制度的保障，技术相对落后的发展中国家将再次失去对本国内容资源的处置权，网络空间的资源就会毫无限制地被拥有技术优势和处于网络管理结构顶端的国家行为体非法占用。

现实空间的主权制度在网络空间中的映射方式可从海洋空间中海洋权益问题的应对实践中得到启发。海洋把有领土边界和海岸线的陆地国家连接在一起，各国间海洋边界的模糊性以及海洋渔业资源的流动性与网络空间的许多特征相似。

《联合国海洋法公约》将国家主权原则和国家的国际义务原则相结

合，创立了现代海洋法制度。其中有两点特别值得借鉴，一是沿着国家主权域向全球海洋公域的趋向线进行阶梯式递减处理。这种处理方法既保证了主权明晰下的有效海域治理，又保证了人类共同遗产和公共利益免受或少受侵害。二是权利主张国应各自寻找并提供技术证据来证明自己的权利，通过联合国委托的技术专家委员会加以确认，而不是通过力量对比和国际斡旋来实现权益和权力的分配。[23]

根据《联合国海洋法公约》，沿着国家主权域向全球海洋公域的趋向线，分别为内水、领海、毗连区、专属经济区、大陆架延伸、公海和国际海底区域。从内水到公海和国际海底区域，国家的主权管辖和海洋权益是梯次递减，而其他国家在这些区域的权益逐渐上升。网络空间中的局域网、城域网、广域网和全球互联网之间也存在着管辖和权益的梯次变化的关系。与海洋主权边界和利益边界的认定相似，网络空间中的权益和边界认定同样具有较高技术含量。

3. 国家主权在网络空间的特殊逻辑

逻辑层面的特征是网络空间最独特的特征。自然空间是基于地缘关系而存在的，而网络空间是基于逻辑电路而形成的。地缘结构和存在于地缘结构的人以及包括森林、矿藏等自然资源构筑了现实社会上层建筑的物质基础；网络空间的有序运行是建立在所有跟编码相关的软件、协议、程序、版本、技术标准和规则之上。网络空间中的特殊数字资源和编码组成的逻辑电路构成了网络治理上层建筑的物质基础。

编码是网络空间的基本元素。它从技术层面构建了网络空间运营和互动的规则。编码是指建构互联网络的程序、协议和数字化的技术标准。编码逻辑的特征如现实空间中地缘的特征一样，是基础性和结构性的特征，是决定网络空间中权力和利益分配的重要依据，是网络治理的关键。编码决定了对网络空间行为规制的可能性和方式，它与法律的结合可以起到对网络行为的规制效果，影响网络空间的社会秩序、市场秩序和行为伦理价值。编码能够通过网络基本结构的改变，将某些规制性的要求暗含到协议之中，从而达成治理的目标。

编码方案不仅是技术符号，更是价值判断的体现。某些编码方案，比如互联网目前采用的TCP/IP协议，只是忠实地将数字信息传输到用数字IP地址标明的终端，对于传输的内容不予分辨。这种编码有利于网络使用者不受阻碍地进行信息传输和地址访问。从价值观来判断，这种技

术工具推进的是无限扩大个人自由的同时又轻易逃避社会责任的网络社会倾向。在使用者的人数有限且用途单一的情况下，如技术工程师群体之间在传输技术数据和分享数据时，这一编码方案只是一个技术工具。当无数的网民加入使用者的行列，甚至可以利用这个工具进行犯罪，比如实施金融诈骗、扩散色情音像、传播恐怖主义信息，此时这个编码方案就成为一个难以驾驭的、制造社会问题的工具，无法体现网络社会对规则和秩序建立的需求。由技术方案造成的网络社会混乱，须借助法律制度与技术方案的重新设定来重置网络社会。

编码在网络空间中实际发挥了资源控制边界的作用。网络空间有公共编码和私人编码。西方跨国公司通过知识产权制度，将网络空间最有价值的资源控制在自己的私有编码之内。网络核心国家也常常利用编码的这种功能来控制网络资源。编码程度越高，知识资源流动就越困难，而掌握编码的人在管控信息流动方面更具优势。掌握编码控制权的国家拥有保护本国信息资源并获得他国信息的工具，进而获得运用所有在其编码界限之内的信息资源的能力。具有编码制定权的国家及企业可在产业发展和产品发布上拥有巨大的技术优势和市场优势。因此，嵌入在软件和网络协议、技术标准中的编码问题，是建立网络主权不可忽略的重要方面。采用何种协议或技术标准以及如何采用这些编码方案，直接或间接地影响到经济主权。编码方案的采用，涉及国家的发展利益和安全利益。编码方案的漏洞和“后门”，将会使所有网络设备以及加载在网络设备上的内容和数据资源处于高度风险之中，对国家安全造成重大威胁，给全球网络的稳定性带来负面影响。[24]

从一个国家的角度看，一个主权国家应当拥有对网络中编码、协议、程序、技术标准、版本和技术规则的制定权（本国版本）和采用权（国外版本）。国家拥有对加载于其基础设施之上的软件编码、技术标准和网络协议版本的知情权和安全审计权。国家可根据自己的国家利益，对外来版本的编码方案采取或拒绝或采用或妥协的立场。他国如借用技术编码手段非法获取和使用别国信息资源，在法律上属于非法入侵和侵占。从全球网络角度看，国际互联网上通用的协议和技术标准应当体现公共产品的特点，反映网络空间分享、交流、和平、繁荣的共同愿景和价值。因此，应鼓励采用公共、安全、可审计的、责权清晰的编码方案，减少不开源的私有的技术标准和编码方案。

编码方案的选择权不应由对公共利益不负有责任的私营部门或只考虑技术进步的工程师来决定。无论在国内还是在国际层面，编码的选择

都应成为公共政策的重要内容。社会需要通过某种政治程序，根据技术先进性与社会责任平衡的原则、社会公共利益与个人自由平衡的原则、权利和义务平衡的原则选择网络空间的基础编码方案。方案的决定权属于社会的管理者——国家的合法政府。国家应成立对公共利益负责的编码管理局，编码方案的采用和通过可由一个国家的人民代表大会或议会来决定。

然而，国家主权在逻辑层面的划分和裁定须与技术发展同步。脱离了技术支撑的法律机制无法实现网络空间的有效治理。国际互联网中通用的编码方案，反映了世界的相互依赖和互联互通关系，因此它更像是国际组织的基本原则，它应当反映共同一致的利益。各国根据自己的权利保护和国际义务来决定是否加入和采纳，其中必定包含着主动的主权让渡，体现着主权的原则性和实践的模糊性。

三 建立网络主权面临的挑战

纵观信息社会化进程，主权一直是一个“进行中”的概念。互联网技术发展并非为主权概念敲响丧钟，而是更加丰富了主权概念的内涵和外延，是国家主权在网络空间的延伸、映射。建立网络主权主要面临来自三方面的挑战：一是国际社会对网络主权存在认识赤字；二是国家主权在网络空间适用模式受限；三是网络空间治理主体和客体的多样性。

（一）网络主权的“多种声音”

国际社会暂未统一采纳“网络主权”这一术语，但各治理行为体基本承认国家主体在网络空间的事实主权。国际社会对网络主权的认知仍存在差异，围绕其展开的争论仍不绝于耳，甚至存在以网络主权为线划分网络阵营的风险。

1. 中国及俄罗斯等新兴发展大国

中国是网络主权的发起国和倡导国。2010年6月发布的《中国互联网状况》白皮书中已明确指出：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。[25]2015年7月1日生效的《中华人民共和国国家安全法》首次以法律形式确定“网络空间主权”。[26]习近平总书记在第二届世界互联网大会开幕式上的讲话

中，明确了推进全球互联网治理体系变革的四项原则，其中首条便是尊重网络主权，“《联合国宪章》确立的主权平等原则是当代国际关系的基本准则，覆盖国与国交往各个领域，其原则和精神也应该适用于网络空间”。[27]中国网络领域的基础性法律《中华人民共和国网络安全法》于2016年11月7日颁布，该法首次明确了网络空间主权的原则。[28]此外，《网络空间国际合作战略》于2017年3月1日发布，就网络空间全球治理提出中国主张，倡导和平、主权、共治、普惠作为网络空间国际交流与合作的基本原则，“既体现各国政府依法管理网络空间的责任和权利，也有助于推动各国构建政府、企业和社会团体之间良性互动的平台，为信息技术的发展以及国际交流与合作营造一个健康的生态环境”。[29]该战略明确了网络空间的主权，在此基础上构建公正合理的网络空间国际秩序，并积极推动和巩固在此方面的国际共识。

从现状看，俄罗斯、巴西等新兴国家和上合组织积极拥护网络主权。新兴大国在网络空间具有战略利益，同时具备一定的经济和技术实力，它们将成为网络主权主张的积极推动者。俄罗斯已多次在国际上主张由国家对互联网实施监管。2012年12月，俄罗斯代表团在迪拜举行的国际电信联盟大会上提出“网络主权”等倡议。[30]在第二届世界互联网大会开幕式上，俄罗斯总理梅德韦杰夫在致辞中明确表示治理互联网的国际规则主要是尊重国家主权。巴西也在国际场合明确表达“支持各国管理各自互联网并保障其安全的主权”，积极主张网络主权。

2. 美国及欧盟发达国家

美国在网络主权问题上采取双重标准，一方面从全球霸权的角度主张“全球公域”和“互联网自由”，另一方面在实践行动中实施网络主权和保障网络安全。

尽管美国在言辞上不支持网络主权的表述，但它是最早在行动上践行网络主权的国家。美国率先对外颁布了《美国国家网络安全战略》（National Cybersecurity Strategy），又先后颁布了《网络安全国家行动计划》（Cybersecurity National Action Plan）、《网络威慑战略》（Cyber Deterrence Strategy）来保障国家网络安全。美国针对网络空间中的数据、设备、信息保护等方面积极进行国内立法，控制和规范网络空间中行为体的行为。如通过《爱国者法案》以加大对网络和通信的监听力度，美国情报部门对出入美国的信息以及美国ICT公司所掌握的各种信息进行监控。[31]

美国的各级法院所受理和裁定的网络空间纠纷案也是全球最多的。美国法院曾裁定加拿大iCraveTV播放加拿大电视台已经播放过的美国电视节目违法（但这并不违反加拿大法律）。[32]1999年法国法院裁定雅虎法国公司的拍卖网站发布纳粹纪念品出售的消息违法，而美国法院则加以否定。[33]美国的司法实践，特别是各个法院在裁定与网络相关的纠纷案时在要素采纳方面的实践，足以说明国家主权的经典原则仍然在指导司法裁定。

美国通过“网络自由”使其免受传统主权概念的束缚，目的在于有效推行美国整体战略，通过降低他国运用主权保护自己利益的能力，达到维持美国繁荣、确保安全、压制对手以及推广美国式价值观和影响力的目的，核心是美国在网络空间推行霸权主义，是一种网络空间的“圈地运动”。在经济领域，压低主权对各国经济资源保护的作用，有利于继续维持美国在知识经济中的既有优势，保护美国企业专有的知识产权；在打击网络犯罪方面，压低他国主权，有利于提高美国等西方强国司法部门的域外执行能力；在军事方面，压低他国主权可以保证美国军队越境对他国基础设施实施网络攻击的合法性，提高美国军队进行网络对抗的威慑力量；在网络国际治理方面，否定国家网络主权可以限制他国独立行使网络管理权，美国试图超越国家主权建立西方版的网络规范，同时用多利益攸关方模式阻止联合国在全球治理领域发挥主导作用，弱化发展中国家维护网络主权的努力；在价值观方面，将国家针对信息内容和信息流通行使管控权与违反《联合国宪章》所规定的言论自由画等号，以提倡网络上言论和集会自由为借口否认他国主权，达到削弱和孤立对手国政权的目的。

3. 国际组织及非政府组织

联合国目前虽然没有使用“网络主权”的术语，但承认网络空间的事实主权。2003年12月在瑞士举行的联合国信息社会世界峰会第一阶段会议通过了《日内瓦原则宣言》，其中第49段（a）款明确表述：“与互联网有关的公共政策问题的决策权是各国主权。”[34]2005年在突尼斯召开第二阶段会议，会议通过的《突尼斯议程》第35段（a）款指出：“我们重申互联网的管理包含技术和公共政策两个方面的问题，并应有所有利益相关方和相关政府间和国际组织的参与。”[35]

2013年6月24日，联合国大会发布了A/68/98文件，通过了“从国际安全角度看信息和通信领域发展政府专家组”所形成的决议。决议第20

条的内容是：“国家主权和源自主权的国际规范和原则适用于国家进行的信息通信技术活动，以及国家在其领土内对信息通信技术基础设施的管辖权”。[36]虽然决议条款并没有直接使用“网络主权”的术语，但此项条款的实质是承认“网络主权”。2015年7月22日，第四届联合国信息安全政府专家组发布报告A/70/174，重申各国在使用通信技术时必须尊重“主权平等”、“不干涉他国内政”等国际法原则。[37]

与之相反，以互联网名称与数字地址分配机构为代表的非政府组织始终限制政府在网络治理中的作用。在2016年3月召开的第55届ICANN公共会议上，虽然ICANN脱离了与美国政府的关系，逐渐过渡到独立的国际组织，但是大会通过决议，将各国政府参与互联网治理的平台——政府咨询委员会（GAC）的职能限定为“咨询”，防止其成为政府“干涉互联网治理的渠道”。[38]

（二）国家主权在网络空间适用模式面临的障碍

网络空间治理的“再主权化”让区隔于现实世界的虚拟世界自身形成主权概念的论调不攻自破。[39]然而，国家主权在现实世界的适用模式无法照搬至网络空间中，而需要根据虚拟世界的特殊性探寻国家主权在网络空间合理的适用模式。

1. 以个人为元点的跨境信息自由流动模式

这种模式将分析问题的元点定位于作为治理主体的个人，其特点是国家对信息流动的干预能力极低，个人作为通信主体的地位得到尊重。这并非宣布主权的死亡，而是在承认国家主权的前提下极有限度地行使主权。这种模式的践行需考虑以下因素：第一，各国是否已经将人类的共同利益置于本国国家利益之上；第二，国际关系是否已超越了霸权主义和强权政治，在此空间中人们之间的关系是否已建立在公正合理基础之上；第三，国际法是否对所有国家都具有强制性的约束力；第四，发展中国家是否不再面临强势国家对内部事务的干预；第五，国际机构或其他行为主体在此空间中是否已具备能力取代国家的作用。

从现实看，国际社会发生的“阿拉伯之春”、“占领华尔街”已让各国意识到信息不被管控、异议声音泛滥的灾难性后果。而2013年斯诺登披露的“棱镜门”事件，更是让美国推行互联网霸权的野心昭然若揭，各国都已明晰其对本国利益的潜在风险。考察网络空间的政治经济

和社会活动的特征，特别是美国政府在互联网领域的行为，反观近些年国际社会发生的事件，笔者认为以个人为元点的跨境信息自由流动模式的践行无法维持网络空间活动有序进行。

2. 以国家为元点的过度干预跨境信息流动模式

现实世界和虚拟世界无法区隔，相互关联。但是，在虚拟世界中过于强调传统的绝对主权会遇到巨大的技术障碍，也不符合全球化发展的趋势，亦不是解决问题的最佳选择。如果主权国家完全自主管制跨境信息流动，即未经主权国家同意的信息流出和流入都是侵犯主权，这种做法很大程度上会限制一个国家获取全球资源、实现发展的机会，有损一个国家的开放精神。长远而言，更会削弱国力，消耗维护主权的信心和能力。

从国际实践看，国家完全自主管制网络空间中跨境信息流动既不现实，亦不合理。20世纪70年代和80年代部分国家针对卫星广播提出“预先同意”原则，即须征得信息输入国同意后境外信息方可进入主权国家境内。该项原则最终没有被联合国采纳。虽然与“预先同意”原则类似的立场在《关于传送由人造卫星传播载有节目的信号的公约》中被采纳[40]，但面对互联网技术则完全无法付诸实践，因为互联网的域名不与特定的地理空间相关，服务商和主权国家无法得知信息是否已跨境流动。

在信息技术飞速发展的当下，坚守最传统的主权概念，不开放信息技术冲击的任何空间的做法完全行不通。一国因为坚持绝对的平等而放弃参与全球化和信息化的过程，理论难以圆融，实践也捉襟见肘。国家不能单纯地为维护主权而维护主权，需增强维护主权的能力。

3. 以关系为元点的共赢式管制跨境信息流动模式

主权是一个关系的概念，网络主权也是如此，它指向国际关系的具体实践。[41]主权在相互交往和关系互动中得以体现，并且是公平程序的结果。一个国家无论其规模大小、实力强弱，都应参与到国际社会的决断程序中，其利益都应当在国际会议或者国际谈判中被代表。[42]从实践角度出发，一个国家采取单边行动干预跨境信息流动，势必会影响其他国家，那么被影响的国家因其利益受到影响则会发出“抗议”。因此，该模式提倡经过公平的程序沟通，以信息流动的共赢为目标，由主

权国家进行适度干预。[43]

然而，这种模式的缺陷在于“公平”和“共赢”如何被定义。表面上看似公平，但因网络空间中各国信息技术强弱不同、经济资源分配不均，网络核心国家、网络化国家、网络边缘国家[44]的利益能否被公平实现，又能否达到共赢？即便各国之间经博弈和妥协后认定了某种“公平”的程序和“共赢”的利益，那么这种双边或多边的商定又通过何种制度得以实现并加以保障？

（三）来自治理主体和客体多样化的挑战

1. 信息流动和信息传播的方式

网络空间中无形资源的控制边界不像国界和军事控制线那样显而易见。信息和数据是一种流动性极强的权力资源。网络空间的互联性使技术优势国家得以运用网络获取流动的数据和信息，以及干涉他国内政的条件和渠道。优势国家可以运用这些技术对他国施加影响力，投射本国的软实力，影响他国社会价值观体系；投射武力，以更快速度和更高精确度从远距离对他国的信息基础设施实施破坏，以削弱对手；通过对他国重要人物的个人交往信息的侵犯，以达到削弱对方政府控制力的目的。

信息控制和传播对国家的内部治理十分重要，是国家权威的来源和维护权威的手段。国家通过三个方面影响信息环境。第一，作为创造信息环境的参与者，直接或通过各种代理者控制和发布信息，行使国家的权力；第二，作为一个规范制定者，建立一个信息发布和流动的法律秩序和管理体系；第三，作为权利保护者，国家有责任保护公民免受危害信息的侵扰。国家对信息流动的管控权主要是指对本国信息的输出、外国信息的输入和境内信息流动进行管理和监控的权力。

在互联网时代到来之前，信息传播是以大众媒体“一对多”的方式进行的。政府通过对信息交换系统所有权的控制实现对信息发布的控制。国家政府和主要政治派别大多控制着国家的主要媒体，比如报纸、杂志、广播、电视。网络时代的传播特点是分散化的，灵活迅捷的通信系统使得每一位用户都可以成为信息源和传播源。网络时代传播的“时空压缩”的特性导致传播的社会冲击力难以预估。信息交换系统的私有化和跨边界交换的自由化加剧了网络传播对政府管控能力的弱化。有效

结合法律的安排和对编码技术标准的控制，可增强政府管控信息的能力。互联网时代信息流动的方式和信息传播的方式，对国家政府在网络空间的治理权威形成挑战。

2. 网络社区的迅猛发展

网络社区最大的特点是摆脱地理边界的束缚，集结生活在不同领土范围内的人们。网络社区的出现使社会结构进一步多元化和扁平化，也使国际秩序更加复杂。网络社区等非国家行为体的发展对所有主权国家及其政府形成挑战。

信息技术的飞速发展，使得互联网成为网络社区等非国家行为体获得政治权力、经济权力和凝聚群体政治意识的重要平台。网络社区获得的工具性权力上升。规模较小的非政府组织可通过网络的组织功能、表达功能和“虚拟广场”与政府进行博弈。黑客、恐怖组织的网络破坏行为则更难以控制。不同文化背景的国家和处于不同发展阶段的国家网络社区发展的程度也不相同。一些优势国家利用这一差异，鼓动跨国网络社区对其他国家进行削弱性的攻击。这使得一些政局不稳的国家维护主权和社会稳定的难度加大。

3. 私有企业的技术控制

全球化时代，跨国公司在全球市场的经济活动已经打破了传统的国家“领土”边界。从事信息通信技术（ICT）的跨国公司则通过控制编码和技术的产权挑战国家的网络主权。

计算机网络技术中有一种“后台程序”。这样一种程序在终端使用者的视野范围内难以被发现，但它是一个始终在运行的更高层级的程序。换言之，后台程序就是一种潜藏起来并不出现在公众视野范围内的具有更大权力的程序。[45]从权力博弈的角度看，后台程序因处于公众认知以外，不受公众制衡与监督，成为权力拥有者的一种独占资源。如果拥有这样权力的企业是国内企业，那是对公权力的侵犯；如果是一个外国企业，则是对一个国家主权的部分侵蚀。

美国的ICT企业在全球信息化的过程中，把他们的产品作为信息化的技术设施出售给他国。美国政府帮助推行的电信产业的私有化，使美国的ICT跨国公司具备信息和通信产品的技术标准制定权，并且通过知

识产权体系将这些标准专利化。这些企业的产品已经成为各国重要基础设施的基本构成，而企业通过不开放的技术标准、编码和数据库控制着市场，也部分地拒绝了技术引进国政府对这些设备进行安全管理，对技术引进国的主权管理方式是一种挑战。

4. 信息文化

互联网在其实现全球化之前先后经历了公开化、私有化两个过程。公开化是指网络技术及其应用从军事领域向民用领域开放并扩展，私有化是指国家通信的经营权从政府手中向私营公司手中过渡。

互联网是作为一个去中心化和权力下放的系统而设计的。工程师按照他们的技术想象和价值观设计了互联网，便捷地将若干网络计算机设备联系在一起。用户可以匿名使用这一网络，信息可以被加密，能够隐蔽其来源，以数据包的方式进行传递。多年的应用使用户适应了现行的、由技术精英们制订的网络世界的规则，认同互联网“自由、隐蔽的可及性文化”。“维基解密”就是这种技术文化的产物。

自由、隐蔽、快速、创新的信息技术文化挑战一国主权的司法管辖权。从安全角度讲，网络技术的隐蔽性使网络袭击的来源难以追踪。司法取证能力在网络空间中严重滞后于网络技术发展。当针对网络犯罪的取证技术和技术痕迹认定标准刚刚确立，技术人员就针对“非法”需求而发展出无痕迹浏览技术，自动消除网络活动痕迹。司法管辖是有属地限制的，网络空间各服务器之间的多节点、多通路连接，使得司法实践难以在管辖地重叠的情况下寻找“始作俑者”。

5. 国家履行的国际义务

为了发展利益和提高国家实力或基于全球治理的需要，国家主权需要部分让渡或约束。欧盟和美国推动的《布达佩斯网络犯罪公约》，对于网络犯罪的司法管辖权和调查取证时的跨国合作等方面做出规定，要求条约签署国在不同程度上让渡国家主权。这在已经实行超主权的欧盟国家容易推行，而欧盟以外国家之间在犯罪认定和量刑上存在法律制度方面的较大差异，加入后对国家网络主权的影响很大。各国参加国际人权公约也会部分地限制国家在网络空间中信息管理权。

通过合理公正的谈判和国际契约让渡部分主权，或在实践中根据人类共同利益的指向认同相关国际行为规范，主动选择约束自身的主权行

为，也是当今时代处理国际关系的常见做法。但是让渡或约束部分主权不应是迫于压力，而是由主权国家共同参与和制定规则的国际组织来决定。

四 中国主张及确立网络主权的思考

（一）中国主张网络主权的对策

1. 主张网络主权应坚守伦理基础，体现道德高地

在主张网络主权时不过度强调网络空间的自卫权。网络空间的相互关联性和网络服务器被技术盗用的可能性，都使得自卫权的行使可能带来难以估量的社会后果。在边界模糊的网络空间中，网络自卫时使用“病毒”式的逻辑会殃及无辜网络区域，而且自卫中使用的病毒软件具有自我繁衍能力，清除工作会花费人类巨大的资源。网络自卫权如被不当使用，易造成其他行为体对臆测的威胁采取自卫行动。服务器很可能被黑客盗用，针对服务器所在的“网区”实施网络自卫行动将造成灾难性的后果。中国应明确主张反对网络空间军事化，反对网络战争，反对利用信息技术从事敌对和侵略活动；主张各国应遵守安全不分割原则，不应为了巩固自己的安全而损害他国的安全；主张各国应遵守主权不干涉原则，反对制定挑起网络相互威胁的计划，反对利用信息技术干涉他国内政；主张不过分强调网络空间的自卫权，和平利用网络空间。中国政府发布的《网络空间国际合作战略》强调：“应摈弃冷战思维、零和博弈和双重标准，在充分尊重别国安全的基础上，以合作谋和平，致力于在共同安全中实现自身安全。”[46]

网络空间是人类活动的全新的、虚拟的空间。人类的行为扩大到陆、海、空、太空、网络空间五维格局。在虚拟的网络空间，互联网突破了国家、地区、种族、民族、宗教、阶级等有形和无形的“疆界”，实现了全球范围的人类交往。中国主张网络主权的基础是人类在网络空间相互依存的共同利益，目的是建设多边国家的利益共同体，构建网络空间命运共同体。

2. 主张网络主权应体现中国担当

中国并非只在受到侵害时才对外主张国家网络主权。中国对网络主

权的主张和阐述是网络空间全球治理中国智慧的重要贡献。强调网络主权对全球网络稳定的服务性功能，呼应了全球对网络空间互联共享平台的稳定性的需求。中国主张网络空间全球治理应坚持多边参与和多方参与。国家不分大小、强弱、贫富，都应当通过国际网络治理机制和平台，平等参与网络空间的国际秩序与规则建设，确保网络空间的未来发展由各国人民共同掌控。同时，充分发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各主体的作用，构建全方位的治理平台。国际社会应共同管理和公平分享互联网基础资源，建立多边、民主、透明的全球互联网体系，实现互联网资源共享、责任共担、合作共治。[47]

中国呼应发展中国家对社会稳定和文化价值方面的关切，帮助发展中国家抓住数字机遇，跨越“数字鸿沟”。强调国家网络主权制度的建立，体现了网络空间中的平等权利和主权尊重，其目的是建立一个和平、安全、开放、合作的网络空间。

3. 主张网络主权应坚持相关表述的一致性和连续性

中国政府在2010年6月公布的《中国互联网状况》白皮书中指出：互联网是国家的重要基础设施，网络主权应当受到尊重和维护。外交部在国际场合也多次重申：互联网不是一个处于国家主权之外的全球公域，一国境内的互联网属于国家主权范围，各国的互联网主权应当受到尊重和保护，各国有权根据本国信息技术发展水平、历史传统、文化语言、道德习俗，自主选择网络空间建设的发展路径、制定网络空间政策法规；有权采取必要措施保护本国信息基础设施和正当信息活动免受威胁、干扰和破坏。反对一些国家以网络自由为名，在网络空间对别国进行干扰渗透，推行其价值观，对别国社会稳定和政治安全造成威胁。这一立场反映了我国在网络空间中的核心利益。关于网络主权的表述应当坚持相关表述的一致性和连续性，同时注意与中国主张的其他网络治理原则的兼容性和整体性。

（二）中国确立网络主权的对策

1. 以科学的手段维护网络主权

相对于现实空间国家主权范围的静态特征，网络空间中的主权具有动态发展的特点。至于在各国网络主权之外是否存在或应当存在网络公

域是一个开放的、可以讨论的问题，但应当是在承认国家的网络主权基础上加以讨论的问题。如果存在国家网络主权之外的网络公域，那么网络公域的管理就是一个国际社会共有、共管的问题，那么美国所掌控的根服务器以及互联网域名地址管理就应当通过某种方式交由相应的联合国下属的国际共管机构管理，建立一个不能由任何国家主导或滥用的真正国际化的互联网治理平台。

2. 以和平的方式维护网络主权

在全球化时代，维护网络主权更需要全面的国际合作，维护主权的手段也应更加科学，更强调以和平的方式维护网络主权。非和平地利用网络必将使已经成型的全球“互联网”变成全球“互裂网”（inter-severed net）。因此，主张网络主权是反对在网络空间中使用武力或以武力相威胁，反对将全球经济发展和人民相互沟通的网络平台用于战场，反对将恶意编码作为武器对他国利益进行侵犯，反对肆意扩大网络空间自卫权的使用。反对在网络空间中划分敌我集团。中国致力于推动各方切实遵守和平解决争端、不使用或威胁使用武力等国际关系基本准则，建立磋商与调停机制，预防和避免冲突。

3. 以发展的方式维护网络主权

一个国家在网络空间治理的话语权，取决于这个国家拥有对全球网络基础设施产权和控制权的份额，取决于其参与网络运用和网络管理的程度，取决于其经济水平、教育水平和网络应用水平。过去三十多年的现代化进程，为中国网络外交奠定了经济和政治基础。中国的综合实力以及在全球经济治理中的分量和政治影响力保证了中国在全球网络治理中拥有日益增长的发言权。中国拥有世界最多的网民，拥有最大的网络经济市场，不断成长中的我国内需市场很大程度上与网络销售相关，也吸引着全球贸易大国的注意力。如今，中国还是世界最大的信息技术产品的生产地，中国的技术产品在全球基础设施中的比例呈跃升状态，加强了我国在网络空间中的实质性存在，增加了维护网络主权的能力。

五 结语

网络主权观念是《联合国宪章》有关国际关系准则在网络空间中的延伸和体现，是网络空间国际制度和现实空间国际制度的一致性连接。

它体现的是网络空间中世界各民族、各国家的平等和相互尊重。它同时反映了当今世界通过网络维护和平、共同发展、分享技术进步的新观念。

网络主权是一个新观念，需要国际社会加以重视和充分讨论。但它不是一个全新事物，许多国家正在行使着各自的网络主权。以信息发达国家为先导，各国相继就网络空间中的数据、设备、信息保护、网络国家安全、防止网络犯罪进行国内立法，对网络空间中人和社会组织的各种行为进行规范，明确相关的权益、利益、责任和义务，保障本国安全利益和繁荣利益，保护公民的网上权利不受侵犯。这些国家行为本身就是履行网络主权的具体实践。

网络主权的具体内容包括国家对相应基础设施的管辖权、对信息流动的治理权、对数据和内容等数字资源的拥有权和处置权、对网络中编码和技术标准的制定权和采用权，以及面向国内的网络空间中人的技术活动、生产活动、社会活动的立法规范权和面向国际的国际义务承担和国际合作参与的独立决定权等。

网络空间是全球化时代技术发展的产物。网络主权观念要体现世界的相互依赖和共通互联的趋势，同时要体现对文化多样性的保护以及技术文化延展过程中全球社会的稳定。对于那些正在努力实现信息化的国家的人民和政府来说，对网络主权的尊重具有重大意义。技术也是一种文化，尊重网络主权可以保证这些国家在引进新技术文化的过程中社会的稳定与和平、人民的幸福与安宁，有利于保护和继承各民族优秀文化传统。尊重网络主权实际上是强化了各国政府对全球网络局部组成的管理责任，也有助于提升他们履行其相关国际义务的意愿和能力。

作为崛起中的大国，中国对网络主权问题的思考既要考虑对本国利益的维护，也要考虑网络空间治理的全球需要；既要考虑今日战略环境和维护国家安全利益和发展利益，也要顾及今后国家利益全球布局的需要，并着眼于信息技术发展和网络社会功能发展的未来趋势。

---

[1] 周鲠生：《国际法》，商务印书馆，1981，第74页。

[2] John Perry Barlow，A Declaration of the Independence of Cyberspace，http：//projects.eff.org/～barlow/Declaration-Final.html.

[3] See John Perry Barlow，A Declaration of the Independence of Cyberspace，http：//projects.eff.org/～barlow/Declaration-Final.html.

[4] David Johnson and David Post，“Law and Borders：The Rise of Law in Cyberspace”，Stanford Law Review，vol.48 （1996），no.5，p.1367.

[5] Harold Laski，Studies in the Problem of Sovereignty，Hardpress Publishing，2013，p.176.

[6] Paul Hirst and Grahame Thompson，“Globalization and the Future of the Nation State”，Economy and Society，vol. 24 （1995），no. 3，pp. 408-442.

[7] Anthony Giddens，The Third Way and Its Critics，Blackwell Publishers，2000，pp. 65-84；〔美〕詹姆斯·罗西瑙：《没有政府的治理：世界整治中的秩序与变革》，张胜军、刘小林译，江西人民出版社，2001，第326页。

[8] 参见〔德〕贝克《全球化时代民主怎样才是可行的？》，载〔德〕贝克、哈贝马斯《全球化与政治》，王学东、柴方国译，中央编译出版社，2000，第14页；〔德〕哈贝马斯《超越民族国家》，载贝克、哈贝马斯《全球化与政治》，王学东、柴方国译，中央编译出版社，2000，第78～79页。

[9] 俞可平：《论全球化与国家主权》，《马克思主义与现实》2004年第1期。

[10] 〔美〕本尼迪克特·安德森：《想象的共同体》，吴叡人译，上海人民出版社，2005，第6页。

[11] 刘连泰：《信息技术与主权概念》，《中外法学》2015年第2期。

[12] “时空压缩”指时间和空间的压缩。时间压缩意味着传播的及

时性取代迟滞性。空间压缩意味着主权的封闭性让位于主权的开放性。见杨泽伟《论国际法上的自然资源永久主权及其发展趋势》，《法商研究》2003年第4期。

[13] 杨泽伟：《主权论：国际法上的主权问题及其发展趋势研究》，北京大学出版社，2006，第112页。

[14] 刘文富：《网络政治——网络社会与国家治理》，商务印书馆，2002，第184页。

[15]〔美〕詹姆斯·罗西瑙：《没有政府的治理：世界整治中的秩序与变革》，张胜军、刘小林译，江西人民出版社，2001，第3～13页。

[16] John Perry Barlow，A Declaration of the Independence of Cyberspace，http：//projects.eff.org/～barlow/Declaration-Final.html.

[17] David Johnson and David Post，“Law and Borders：The Rise of Law in Cyberspace”，Stanford Law Review，vol.48（1996），no.5，p.1367.

[18]〔美〕劳伦斯·莱斯格：《代码：塑造网络空间的法律》，李旭等译，中信出版社，2004，第6页。

[19] Jeremy Malcolm，Multi-stakeholder Governance and the Internet Governance Forum，Terminus Press，p. 319.

[20] Milton L. Mueller，Networks and States：The Global Politics of Internet Governance，The MIT Press，2010，pp. 48-49.

[21] 刘杨钺、杨一心：《网络空间“再主权化”与国际网络治理的未来》，《国际论坛》2013年第6期。

[22] Michael Schmitt（ed.），Tallinn Manual on the International Law Applicable to Cyber Warfare，Cambridge University Press，2013，p.6.

[23] United Nations，United Nations Convention on the Law of the Sea of 10 December 1982，
http：//www.un.org/depts/los/convention_agreements/texts/unclos/UNCLOTOC.htm.

[24] 杨剑：《数字边疆的权力与财富》，上海人民出版社，2012，第271～274页。

[25] 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，第24页。

[26]《中华人民共和国国家安全法》，法律出版社，2015，第7页。

[27]《习近平在第二届世界互联网大会开幕式上的讲话》（全文），新华网，http：//news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm。

[28]《中华人民共和国网络安全法》，中国人大网，
http：//www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm。

[29]《网络空间国际合作战略》，
http：//www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t14

[30]《综述：俄罗斯努力防范网络安全高风险》，新华网，
http：//news.xinhuanet.com/zgjx/2013-08/14/c_132627248.htm。

[31] The USA Patriot Act （H.R. 3162），Title Ⅶ and Title Ⅸ，
https：//epic.org/privacy/terrorism/hr3162.html.

[32] Twentieth Century Fox Film Corp. v. iCraveTV，2000 Copr. L. Dec. p. 28，p. 30，53 U.S.P.Q. 2d 1831.

[33] Yahoo！Inc.v.La Ligue Contre Le Racisme Et L’Antisemitisme，433 F 3d 1199 （2006）.

[34] WSIS，Declaration of Principles（WSIS-03/GENEVA/DOC/4-E），para.49（a），
http：//www.itu.int/net/wsis/docs/geneva/official/dop.html.

[35] WSIS，Tunis Agenda for the Information Society（WSIS-05/TUNIS/DOC/6（Rev.1）-E），para. 35（a），
http：//www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[36] United Nations General Assembly，Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security（A/68/98），para.20.

[37] See United Nations General Assembly，Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security（A/70/174）.

[38] ICANN，ICANN16，http：//icann2016.org.

[39] 参见〔美〕尼葛洛庞帝《数字化生存》，胡泳译，海南人民出版社，1996，第278页。See Lawrence Lessig，“The Path of Cyberlaw”，Yale Law Journal，vol.104（1995），p.1744；John T. Delacourt，“The International Impact of Internet Regulation”，Harvard International Law Journal，vol.38（1997），p.207.

[40] WIPO，Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted Satellite，
http：//www.wipo.int/treaties/en/ip/brussels.

[41] 胡泳、车乐格尔：《“网络主权”辨析》，《新闻与传播研究》2016年第1期。

[42] Iris Marion Young，“Activist Challenges to Deliberative Democracy，” Political Theory，vol.29（2001）. no. 5，pp. 670-690.

[43] 刘连泰：《信息技术与主权概念》，《中外法学》2015年第2期。

[44] 此种分类法参照杨剑《数字边疆的权力与财富》，上海人民出版社，2012，第216页。

[45] 杨剑：《数字边疆的权力与财富》，上海人民出版社，2012，第92页。

[46] 《网络空间国际合作战略》，http：//www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t14

[47] 《网络空间国际合作战略》，http：//www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t14

第三章

三视角理论框架下的网络主权

网络时代和全球化背景下的网络主权观，需要突破实体空间的局限和二元对立的误区，站在网络空间命运共同体的维度，以俯瞰全景的视角，科学把握排他性与让渡性的对立统一。

当今网络犯罪、网络恐怖主义盛行，网络安全问题丛生。如何进行全球网络空间治理、构建公平正义的国际规则，世界各国一直存在颇多争议，实质上反映的是国家、国民和国际三大网络空间行为体之间的利益诉求。行为体各自从自身利益出发，对另外两大行为体普遍忽视，从而形成了目前各执一词、难以调和的局面。网络空间新秩序的建立需要从三大行为体的视角审视全貌。三视角理论是从国家、国际、国民这“三点”出发，引出三个边界条件，在稳定的三角形共视区内将网络空间分成“三层”——物理层、应用层、核心层。不同层面区别对待，求同存异，从而跳出单点迷思和二元对立，站在网络空间命运共同体的维度，以俯瞰的视角，科学把握排他性与让渡性的对立统一。

一 国际社会对网络主权争议的三大焦点

网络安全问题已经成为全球性挑战，正在上升为主权国家第一层级的安全威胁。世界各国针对网络空间国际规则和全球治理体系变革展开热议，网络主权不可回避地成为争议的焦点。在这个问题上，虽然得到联合国信息安全政府专家组的较大认同，[1]但在国际社会，仍对网络主权存在深层分歧和质疑，主要集中在以下三方面。

一是将网络主权与互联网精神对立起来。有观点认为主权的排他性有悖于互联网精神的互联互通，认为强调网络主权会人为制造新的问题，导致互联网碎片化。例如，电子前线基金会（Electronic Frontier Foundation）发起人巴洛曾发表《网络空间独立宣言》，认为中、美、俄、法、德等各国政府都是工业时代的产物，均不拥有网络空间的主权，认为网络空间生来自由，民间力量自会明辨是非，形成网络空间新的社会契约，解决冲突和争议。[2]

二是将网络主权与人权对立起来。有观点认为互联网应该支持言论自由，主权的介入阻碍了信息自由流动，这一舆论矛头集中在中国设立防火墙上。例如，国际人权组织大赦国际（Amnesty International）认为中国的网络主权主张侵害了言论自由，并以此为由号召苹果、谷歌、脸书、领英等科技公司抵制中国。[3]

三是将网络主权与多利益攸关方对立起来。有观点认为网络主权引发互联网治理模式之争，政府主导的多边治理可能会挑战多利益攸关方治理模式。例如，美国商务部副部长施特里克林（Lawrence Strickling）表示对中国的立场感到困惑，认为中国一方面表示支持多利益攸关方治理模式，另一方面却在乌镇峰会提倡网络主权。[4]

由此可见，网络主权问题在网络空间国际规则中有着特殊的重要性，成为诸多问题树的树根，其他问题由此衍生。在这一问题上厘清分歧、达成共识，才有国际合作的基础。而“大道至简”，再复杂的问题回归到最简单的“道”上，道通则理明。如何才能让传统主权这个概念在网络空间全球化时代以更加科学的内涵和表达获得最大公约数和认同度？借助在中美、中俄、中欧国际二轨对话交流中得到的一些启发，本章试图构建一个理论框架，阐释一种整体的、互动的、分层的网络主权观，以便更客观、更辩证地理清问题、解决矛盾。

二 三视角是解决矛盾的重要突破

深入剖析上述三个主要矛盾，实质上反映的是国家、国民和国际三大网络空间行为体之间的利益诉求。这三大行为体各自从自身视角出发，对另外两大行为体普遍忽视，从而形成了目前各执一词、难以调和的局面。

网络主权和互联网精神这对矛盾，其背后的行为体是国家与国际；网络主权和人权这对矛盾，其背后行为体是国家与国民；而网络主权与多利益攸关方这一对矛盾，其背后又涉及国家、国际和国民三个行为体。

二元对立的零和博弈，或为僵局，或是一方胜利，但皆付出巨大代价。如今国际社会的舆论质疑，大多出自单一视角、单向思维、单边逻辑。站在一个点看问题，对另外两点普遍忽视，要么绝对，要么过激，结论是无解的，需要跳出单点迷思和二元对立，站在更高的全息维度，引入三个视角。

认清网络空间的三大行为体，如同混沌空间点亮的三盏灯，一盏灯只能看到一个点，两盏灯能看到一个面，而三盏灯可以让我们看清一个整体。从三视角出发，我们可以看到一个更真实的网络空间，其中各行为体的角色与诉求，以及相互间的关系影响，形成多元矛盾的对立统一。

三 三视角的理论框架

数学当中解多元方程总要设边界条件（n＞x＞0），在一个定义域里求解，变量既不是无穷大，也不是无穷小。三视角的意义就在于，由这三个行为体的视角出发，就能画出三个边界条件，更具包容性，形成一个稳定的三角形和共视区，进行有效对话，求同存异，可以让问题得到收敛和聚焦，避免单点思维，“发射后不管”。

传统的、实体空间的国家主权，存在天然的排他性。对内强调至高无上的权威性，对外强调不可侵犯的独立性。当人类进入了网络空间，开放性、全球性使另外两个行为体的体量增长，作用凸显。这个时候谈国家主权，一定要拓展国际和国民两个视角。如图3-1。

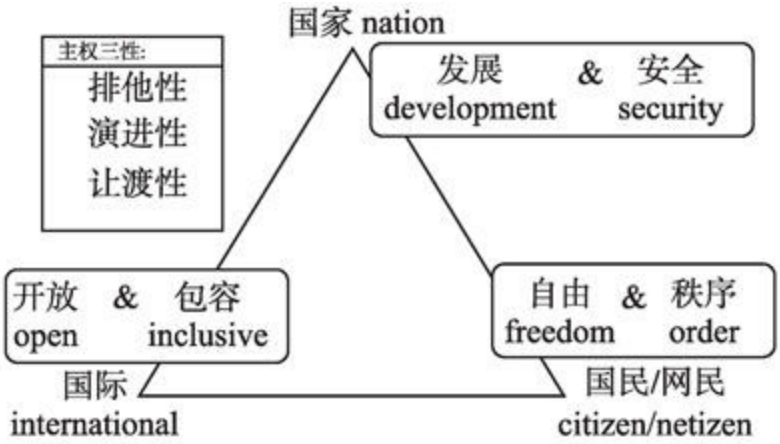

图3-1 国家、国际、国民/网民三视角共视区

国民视角：国民社群追求自由，具有更多的横向拓展的特征。今天全球网民达32亿，中国网民达7.1亿，这是个了不起的数字。一定程度上，可以说，网民就是公民、国民。国民社群内部具有家族、邻里、语言等方面的相似性，栖身于同一社会与文化语境当中，受深层文化心理结构的影响。但同时，在网络时代，国民社群更多地走出血缘和物理社区的绑定，实现横向水平拓展，以价值观认同为基础，追求温和渐进的社会变革。各国都市化人群的生活方式具有较大的相似性，并且因女权、人权、环保、反战、反全球化等共同价值观走到一起。1999年民间团体作为反全球化的力量在反WTO示威中崛起，并在新世纪作为一个崭新的利益攸关方成为网络空间政策的决策者。

国民社群虽然有追求自由的天性，然而事实证明，国民既拥有道义资源，也难免低级趣味；既具有一定程度的组织性，也存在紊乱、松散甚至引发冲突的可能；既拥有美好的价值观，也可能诉诸极端主义理念和民粹主义，最近的例子就是“伊斯兰国”等宗教极端主义组织通过网络招募战士，世界各地竟有年轻人趋之若鹜。在无序的环境下，完全靠网民治网，自律效果并不好，自由是不可能得到保障的。要维护每一个网民的自由，就必须要有秩序来平衡，这就注定网络不能是法外之地。秩序的建立和形成需要外力，需要国家、政府层面制定规则，依法治网，保障网民的合法权益。技术不是万能的，技术本身不会提供秩序和安全，需要主权来提供相应的法律保障。

国家视角：国家追求安全与发展，具有更多的纵向的垂直的特征。国家拥有征税的权力，还拥有军队、警察等暴力机器，按照等级鲜明的命令体系运作，这是17世纪中叶以后形成的威斯特伐利亚主权国家体系的特征。讨论网络空间的国家视角，需要将国家分成两类：发达的、北

方的、强势的上游国家和发展中的、南方的、弱势的中下游国家。网络主权对于后一类国家具有特殊意义。

对于发达国家、北方国家、强势国家来说，它们既可能利用自身所处的上游地位，引领建设和平美好创新的网络空间，也可能诉诸单边主义，肆无忌惮地利用自身技术优势监控全世界，甚至将网络空间军事化、武器化。在这些国家，最坏的趋势是网络空间对外政策上的好战主义。在国家和国民双边关系上，挪威和平学者加尔通（Johan Galtung）甚至得出了西方发达国家越民主越好战的结论。美国前总统小布什认为，在人类千万年的历史中，最珍贵的是驯服了统治者，将他们关进了笼子里，并号称自己站在笼子里向人们讲话。殊不知，在美国国内，可能真正做到了将统治者关进了笼子，但是在对外政策方面，他们仍然站在笼子以外。对这些国家来说，最要紧的事情是建立隔离带，不要将传统空间对外政策方面的好战主义延伸到网络空间。

对于发展中国家、南方国家、弱势国家来说，国家既可能以主权为国际法中唯一认可的法律武器来抵制霸权主义和好战主义，也可能滥用网络主权概念来隔绝自己国民的信息渠道。这些国家既要保安全又要谋发展，既要管网也要用网，利用网络空间建设符合自身国情的民主体系，避免失去与国民的联系和共鸣。国家与国民之间应是相互依存的关系。习主席在“4·19讲话”中讲得好：网民来自老百姓，老百姓上了网，民意也就上了网。群众在哪儿，我们的领导干部就要到哪儿去。各级党政机关和领导干部要学会通过网络走群众路线，积极回应网民关切，解疑释惑。[5]过去都说支部建在连上，现在看政权应该建在网上，在网上倾听民声，了解民意，集中民智，引导民主，更能体现执政党的智慧。这样互联网的自由活力也会给国家发展带来繁荣生机。

国际视角：国际社会追求开放与包容。国际互联网代表技术发展的主流，是人类文明的大势。国际社会要追求开放与包容，因为这里既有大国关系的角逐，又有东西方文化的碰撞，还需兼顾发达国家和发展中国家的利益平衡。国际社会的最大特征是经济全球化以及反经济全球化力量的全球化。按照德赫尔兰（Majid Tehranian）的观点，中国、印度以及一些东盟国家属于“北京全球化模式”。在这个模式下，中国是最典型的国家。中国经历了长达几十年高速经济增长，参与国际劳动分工和消费，拥有五千万海外华人，因而成为全球化过程的重要受益者。与此相反，伊朗、朝鲜、古巴以及非洲撒哈拉沙漠以南大部分国家，则游离于全球化体系之外。

“达沃斯全球化模式”属于另一种经济全球化的模式，向全球扩张资本主义的成本与利益，既普及了技术，也造就了消费主义的泛滥。世界经济论坛是该模式的代表，该论坛每年在瑞士达沃斯召开，代表几千家全球公司及其政治盟友的利益。与此相反，反对达沃斯模式的劳工、人权以及环保力量也实现了全球化，试图纠正经济全球化带来的负面影响。

以上是国民、国家以及国际三个视角的特征、逻辑以及优缺点。从国家视角看，国家要解放思想、转变观念，正确看待安全与发展的关系，可以将互联网为我所用，趋利避害。国家通过让渡一定的主权，融入国际体系，可以让国际的开放互通为国家带来更多发展机遇，促进文化交流、经济合作以及安全上携手应对。国家与国际之间有相互依赖、包容、让渡的关系，达成对立统一。习总书记说：“中国开放的大门不能关上也不会关上。”[6]

国际视角看，互联网在技术上实现了全球互联互通，但只要国家还存在，就不可能无视国界和国家主权。要防止过度追求开放，越过底线，导致一种强势文化格式化多元文化，网络强国更应主动协助填平数字鸿沟，积极让渡和分享网络资源和治理经验，克制使用不对称手段谋取短期利益的冲动。

在全球一网的基础上，创造更多的利益契合点，让世界各国都能够取得经济繁荣、文化昌盛、安全保障，这才与“互联互通，共享共治”的互联网精神本质相契合。中国《反恐怖主义法》删除或弱化了原本草案中规定的数据本地存储、提供接口等国际社会反映强烈的条款。[7]这说明中国在开放与安全之间正在做出必要的主权让渡。

国家追求安全与发展时，需要向国际开放；国民在追求自由时，需要国家提供秩序保障；国际追求开放时，需要包容不同国家的多元文化。这些多边关系看似对立，实则统一，看似矛盾，却相互依存。每个行为体不能总是一味追求自己利益的最大化和绝对化，而是需要一定的相互“让渡”，在三边所限定的共视区内达成最佳的平衡，也就是要在网络空间的地球村、一条船上，寻求守望相助。

综上所述，发展与安全、自由与秩序、开放与包容之间都是一组动与静的统一，阴和阳的平衡。其实这三个行为体本身的诉求并不是绝对冲突和对立，只不过放到不同的范畴，而表现出一定对立关系，但最终

我们追求的是大格局下的整体平衡，有让有合，对立统一。很多时候，通过观念的转变，视角的转化，就可将一些矛盾化解。

四 三视角下看网络主权特征

虽然传统主权天然排他，但在全球化时代的网络主权需要考虑合理让渡。具体什么时候排，什么时候让，让到什么份儿上，要有度。基于三视角模型，再进一步分析和把握这个度。如图3-2。

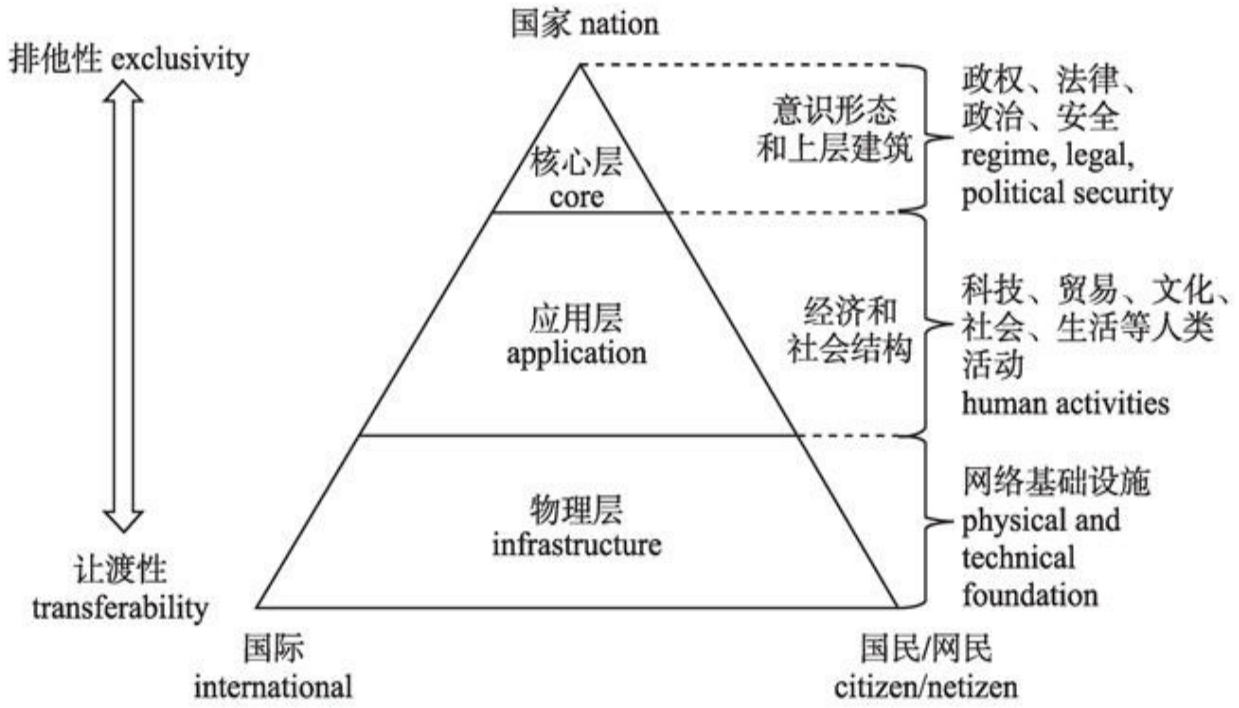

图3-2 三视角下的网络主权三层特征

过去习惯于把网络主权的争论焦点放在网络空间到底应不应该有主权，也就是放在主权的“演进性”或“延伸性”上，其实这根本就是一个无须争论的事实。认为网络空间没有边界，认为网络空间不适用国家主权，这些观点已不再成立。网络空间早就成为继陆海空天之后的第五疆域，美国前总统奥巴马的讲话中早就把它视为一个作战域，并组建了133支网络战部队。

各国不管在网络主权的提法上如何各执己见，在实践层面却无一例外对本国网络加以管治，防止受到外部干涉和侵害。这些都是承认网络

主权的实践彰显。分歧并不在于是否认同网络主权，而在于主权覆盖哪些区域，通俗地说，就是“脖子”以上还是以下的部分。这个问题反映了不同国家对网络安全的痛点是不一样的。国际社会应当尊重和理解各国的不同关切。

因此，我们认为研究的关键，是要用分层的方法来具体分析网络主权的可分性，进而找到主权“排他性”与“让渡性”的适用域。

底层：物理层，包含网络基础设施。这一层的关键是追求标准化，全球一网、互联互通。互联网，继粮食、水以及电之后，成为各国发展的必备基础设施和先决条件。这一层里，需要各国做出集体让渡，强势方更要向弱势方主动让渡，发达国家把成果向发展中国家输出，以填平数字鸿沟。在2005年信息社会世界峰会上，成立了全球数字团结基金，致力于弥补全球数字鸿沟，就属于这个范畴的事情。

中层：应用层，包含了互联网平台在现实中的广泛应用，互联网载体融入了人类在科技、文化、经济、贸易及日常生活等方面的各种活动。21世纪，技术的崛起延续了工业时代的势头，现实空间和网络空间光影交互，呈现多姿多彩的面貌。大英百科全书相对于维基百科，新华书店相对于亚马逊，中国移动相对于Skype，中国工商银行相对于余额宝，希尔顿酒店相对于民宿Airbnb，百货大楼相对于阿里巴巴，传统的出租车相对于滴滴优步。后者都具有一个相同的特点，即建立在网络或移动应用平台之上，更容易跨越主权国家的范畴。

网络主权在这一层次的影响应该因地制宜，动态平衡，多边与多方共治，自由与秩序平衡。在ICANN所管辖的域名体系中，各国都认可“.cn”（中国）、“.de”（德国）、“.ru”（俄罗斯）、“.jp”（日本）等国家代码顶级域的主权属性。同时，顶级域名的注册已经向省份和城市开放，“.Helsinki”（赫尔辛基）、“.London”（伦敦）、“.NYC”（纽约）等城市名称也都成为顶级域名，获得跟“.fi”（芬兰）、“.uk”（英国）、“.us”（美国）等国家级域名同样的待遇。它们都属于各国行政区划内的城市，完整携带主权属性。

同时，关于Whois域名注册信息查询，也可以较大程度上包容各国隐私法的差异。Whois是“Who is”（谁是）这两个单词的合并形式。“谁是这个域名的负责人？”Whois对这个问题进行解答。通过使用Whois数据库（https://whois.icann.org/en），任何人都可以查询

某个网站的注册信息，涉及包括域名所有人、注册商、注册地、创建和更新日期、联系电话、传真、邮箱等将近60行标准格式的信息。但是具体到各个国家层面，可根据本国隐私法的内容决定公开内容的完整程度。所以，从ICANN机制本身来看，虽然奉行的是多方原则，但是从更广的实践层面来看，ICANN却是多边和多方融合绽放的万花筒。

顶层：核心层，包含政权、法律、政治安全和意识形态，涉及执政根基，是一个国家的核心利益，不容挑战。因各国的国情、宗教、文化背景差异，分歧是客观存在的。文化的多样性是人类的生存常态，不能用一种文化强行格式化这个世界的所有文化，要尊重差异，包容多样。对于一个国家，你可以不认同它的制度和意识形态，但是必须尊重它的存在，包容它的差异，理解它的国情。

上层建筑和意识形态的土壤即是各国所处的历史、文化、文明语境。联合国教科文组织《世界文化多样性宣言》认为“尊重文化多样性、宽容、对话及合作是国际和平与安全的最佳保障之一”，希望“在承认文化多样性、认识到人类是一个统一的整体和发展文化间交流的基础上，开展更广泛的团结互助”，认为“尽管受到新的信息和传播技术的迅速发展积极推动的全球化进程对文化多样性是一种挑战，但也为各种文化和文明之间进行新的对话创造了条件”。[8]

网络空间应该避免重复各国在传统空间所走的弯路，不应以网络安全为借口复制传统空间中的敌我势力划分，应做到各文明、文化、国家之间的相互尊重、和平共处。2014年3月，在联合国教科文组织总部的讲话中，习近平主席阐述了中国对文明、文化以及宗教的基本观点，恰能回应当下全球网络空间领域存在的核心分歧。讲话指出：“文明交流互鉴不应该以独尊某一种文明或者贬损某一种文明为前提。”讲话认为：“要了解各种文明的真谛，必须秉持平等、谦虚的态度。如果居高临下对待一种文明，不仅不能参透这种文明的奥妙，而且会与之格格不入。历史和现实都表明，傲慢和偏见是文明交流互鉴的最大障碍。”[9]

可见，在三角形的中层和底层，网络主权可以进行一定程度的合理让渡，让更多的利益攸关方能够参与治理，形成多利益攸关方治理模式。而顶层重在体现政府的主导作用，“互联网的公共政策制定权是一国的主权，每个国家对境内信息基础设施承载的信息拥有天然的管辖权”，这是联合国信息安全政府专家组已经达成的共识。尊重各国自主选择网络发展道路和网络治理模式，是让各国政府承担国家责任、开展

国际合作的基本前提。

综合这三个分层可以进一步厘清多边与多方的分歧。两种模式其实并不冲突，而是在网络空间的不同区域、不同层级有不同的适用性。涉及意识形态、政策、法律、制度和政权安全问题，肯定要充分发挥国家政府的主导作用，充分体现多边治理的优势。

基于这个理论，我们可以回答前文提出的对网络主权的三个质疑：

第一，关于网络主权违背互联网精神的质疑。坚持网络主权绝不排斥互联网精神。“同一个世界，同一个网络”，不容置疑。承认网络主权是基础，是为了各国能够平等参与互联网的全球治理，不仅实现互联互通，而且还要共享共治。

第二，关于网络主权与网络自由的分歧。以防火墙为例，防火墙对中国来说是一种痛，是不得已而为之。面对网络空间日益恶化的安全态势、“颜色革命”的严峻挑战、上游强势资本的冲刷，网络对抗能力还不够强大的发展中国家，不能对政权和国家的安危无动于衷。就像让一个整日面对恐怖袭击威胁的国家，放下反恐的戒备，解散反恐的武装，那是不可能的。因此我们反对网络强国动用国力支持穿越他国防火墙的行为。但是随着安全形势的好转、互信的加深、民主的成熟和技术的发展，我们对有害信息的封堵也会更加精准、高效，将防火墙收窄。顶层所覆盖的范围实际上是面积很小的，过度扩大顶层区域的面积，不利于各方在网络主权上达成共识，这也是中国一直在努力研究、不断改进的。

第三，关于多边与多方对立的疑虑。提倡网络主权并非要取代多利益攸关方治理模式。各国政府也是多利益攸关方的一员，既要发挥政府在多方中的作用，同时也应当尊重、鼓励企业、社群、专家、智库发挥专业技术优势，参与治理。但要防止以多利益攸关方排斥政府的参与和在关键问题上的主导作用。在核心层和应用层，涉及意识形态、政策、法律、制度和金融安全问题，肯定要充分发挥国家政府的主导作用，充分体现多边治理的优势。

例如，美国和欧洲2016年发布的《欧美隐私盾协议》，最终取代了此前由于斯诺登泄密事件而废止的《安全港协议》。新协议较为妥善地协调了国民、国家以及国际社会之间的关系。由于欧盟是跨大西洋数据流通中相对弱势的一方，新的框架协议明确规定美国安全部门不可以大

规模、毫无鉴别地搜集欧洲用户的信息。欧洲公民在自身隐私受到侵害的时候，既可以向本国政府部门申诉，也可以越过本国政府直接向美国公司申诉。[10]新协议从实质上体现了网络空间的主权含义，也是政府主导下维护网络主权的法律实践，值得研究借鉴。政府在国际和国内重大事件当中扮演着举足轻重的角色，这是不争的事实。关键时刻，政府该出手时就出手，当放则放，当管必管，不容回避，也必须担当。

通过上述分析，三视角下看网络主权的对立统一，可概括为：在全球化向深度发展的网络时代，网络主权具有可分性。第一，核心层具有不可侵犯的排他性；第二，物理层、应用层具有开放共享的让渡性。既不允许滥用互联网的联通性来挑战主权国家的核心利益，也不能以传统主权的排他性动摇全球一网的基础平台。让渡与排他各自的比重具有弹性，因其网络主权能否得到国际规则的尊重而互动。

五 结论

第一，网络主权植根于现代法理，是国家权利和责任的综合体现。任何一个负责任、有良知的国家政府都不会漠视新空间的发展与安全，也不应排斥、阻挠其他国家的主权申张和全球共治的合理诉求。尊重网络主权是开展国际合作的前提，是构建良好秩序的基础。

第二，网络时代和全球化背景下的网络主权观，需要突破实体空间的局限和二元对立的误区，站在网络空间命运共同体的维度，以俯瞰全景的视角，科学把握排他性与让渡性的对立统一。中国坚持网络主权，也在合理让渡主权，中国重视国家安全，也在推进国际合作与开放发展。

第三，中国从不反对多方治理模式，但必须防止以此排斥政府在重大问题上的作用和责任。多边与多方是互补而不是互斥。政府和多利益攸关方可以在网络空间的不同层面发挥不同主导作用。

第四，网络时代，丛林法则应让渡于休戚与共、风雨同舟，画地为牢应让渡于开放共享，唯我独尊应让渡于共生共荣，以价值观画线应让渡于尊重差异、包容多样。

总体上来说，三视角的出发点和落脚点，就是能够让世界听懂中国声音。这样，才能真正赢得国际话语权，打造协同联动的新秩序。习近

平主席指出：“要理直气壮维护我国网络空间主权，明确宣示我们的主张。”[11]如何理直气壮地宣示和维护我国网络空间主权？先理直，才能气壮，我们要把“理”诠释清楚，自己要说得明白，让别人听得懂。听懂中国声音以后，让中国的互联网主张真正传得出、立得住、站得直，得到国际社会的广泛共鸣，赢得话语权，才能真正在国际规则制定上发挥我们的影响力。

---

[1] See United Nations General Assembly，Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security（A/70/174）.联合国信息安全政府专家组全称为“国际安全背景下信息和通信领域的发展政府专家组”，由中国、俄罗斯、美国、英国等主要国家的代表组成，具有广泛的国际代表性，并且在网络空间国际法规则的制定中发挥着越来越重要的作用。

[2] John Perry Barlow，A Declaration of the Independence of Cyberspace，http：//projects.eff.org/～barlow/Declaration-Final.html.

[3] https：//www.amnesty.org/en/latest/news/2015/12/tech-companies-must-reject-china-repressive-internet-rules/.

[4] US Department of Commerce，Remarks of Assistant Secretary Strickling at the Information Technology and Innovation Foundation，http：//www.ntia.doc.gov/speechtestimony/2016/remarks-assistant-secretary-strickling-information-technology-and-innovation-fo.

[5] 习近平：《在网络安全和信息化工作座谈会上的讲话（2016年4月19日）》，新华网，http：//news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm。

[6] 习近平：《在网络安全和信息化工作座谈会上的讲话（2016年4月19日）》，新华网，http：//news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm。

[7] 2015年2月25日，第十二届全国人大常委会第十三次会议审议的《反恐怖主义法》草案二审稿第15条规定：“电信业务经营者、互联网服务提供者应当在电信和互联网的设计、建设和运行中预设技术接口，将密码方案报密码主管部门审查。未预设技术接口，或者未报审密码方案的，相关产品或者技术不得投入使用。已经投入使用的，主管部门应当责令其立即停止使用。”该条被认为是规定了预留后门、提供源代码和密钥等法律义务，从而引发国内外的广泛关注。2015年12月27日第十二届全国人大常委会第十八次会议通过的《中华人民共和国反恐怖主义法》第18条则规定：“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等技术支持和协助。”

[8] 联合国教科文组织《世界文化多样性宣言》（2001年11月2日联合国教科文组织第三十一届大会通过），中国民族宗教网，http：//www.mzb.com.cn/html/report/28807-1.htm。

[9] 习近平：《在联合国教科文组织总部的演讲》（2014年3月27日，巴黎），新华网，http：//news.xinhuanet.com/politics/2014-03/28/c_119982831.htm。

[10] US Department of Commerce，EU-U.S.Privacy Shield，https：//www.commerce.gov/page/eu-us-privacy-shield.

[11] 《习近平：要理直气壮维护我国网络空间主权》，人民网，http：//media.people.com.cn/n1/2016/1010/c40606-28764045.html。

第四章

网络空间秩序构建中的网络主权

正如国家主权原则是现代国际秩序和国际法的基石，网络主权原则也将是网络空间国际秩序和国际法的基石。谁能够掌握网络主权问题的话语权和主导权，谁就能够在网络空间秩序构建和规则博弈中占据制高点。

随着传统国际关系向网络空间的延伸，当前，网络空间正处于秩序构建和规则博弈的关键时期。国家主权能否以及如何在网络空间适用，是其中最为复杂、最具根本性的问题之一。这一问题的走向，不仅直接关涉国家在网络空间的地位和作用，也与网络空间国际秩序和国际法制度的构建有着密切关联。

一 网络空间：从“去主权化”到“再主权化”

一般认为，“网络空间”（cyberspace）是指由互联网、电信网络、计算机系统和嵌入式处理器、控制器组成的相互依赖的信息技术基础设施。通常，这一术语还包括真实的信息环境和人们的相互交往。[1]

作为现代科学技术革命的结果，网络空间对人类生活的方方面面产生了深刻的影响，并已成为人类生活的一个新空间，即陆地、海洋、空气空间和外层空间之外的所谓“第五空间”（fifth domain）。在这一空间，人们依靠鼠标和屏幕进行着真实的、往往与现实世界无异的信息交流和相互交往。但另一方面，网络空间所具有的虚拟性和全球性，又使之与其他的传统空间有着显著的区别。那么，主权国家在网络空间治

理中能够发挥何种作用？国家主权在网络空间究竟能否和如何适用？

回顾网络空间形成和发展的历史，在较长一段时间内，主权国家发挥的作用十分有限，网络用户在各种技术标准和服务使用合同基础上的自律（而不是政府监管或“他律”），成为网络空间有序运行的基础。因此，网络空间被视为一个自由放任的“自主体系”，倡导网络空间“自我规制”、反对将现实空间的各种政府管制延伸到网络空间的观念曾经十分盛行。1996年美国著名网络活动家约翰·P. 巴洛发表的《网络空间独立宣言》就是这一观念的鲜明代表。在该宣言中，约翰·巴洛以网民代言人的姿态向世界各国政府宣称：“你们在我们居住的地方没有主权。……网络空间不存在于你们的边境之内。”[2]

上述排斥主权国家干预和规制网络空间的观念，在学界同样得到过广泛支持。美国学者戴维·约翰逊和戴维·波斯特在1996年发表的一篇著名文章中，对网络空间的独立性和独特性进行了这样的描述：

基于电脑的全球通信超越了领土边境，创建了人类活动的一个新领域并削弱了以地理边界为基础的法律的可行性和正当性。在这些电子通信打乱地理边界的同时，一种由屏幕和密码组成的新的边界出现了，这些屏幕和密码将一个事实上的世界同由原子组成的“真实世界”隔离开来。上述新的边界确立了一个独特的网络空间，它需要并能够创立它自己的法律和机构。[3]

不仅如此，反对国家主权适用于网络空间的态度似乎也体现在相关国家的政策和实践中。例如，以美国为代表的一些国家公开主张：网络空间是一个类似外层空间和公海的全球公域。在美国国防部出台的2005年《国土防御与公众支持战略》中，提出“全球公域包括国际水域、空气空间、外层空间和网络空间”。[4]时任美国国务卿的希拉里·克林顿在2010年发表的网络自由谈话中，也强调网络空间是一个“网络化的全球公域”，并以此对中国等国家的互联网管理政策横加指责。[5]

上述“去主权化”的观念，不仅符合网络空间早期发展相对独立于国家的现实，更重要的是，它与人们对网络空间特点和属性的认知密切相关：既然网络空间是一个全球性和无边界的空间，那么，以国家对特定领土的排他性控制为基础发展起来的主权原则，就不可能也不应当延伸适用到这一空间。

但事实上，为了应对各种不断增多的网络安全威胁，从1990年代后期起，各主权国家越来越多地参与到网络空间治理中，并在不同程度上、以不同形式在该空间行使主权，从而导致了网络空间所谓“国家的回归”态势。[6]例如，美国作为当今世界唯一的超级大国和互联网技术最为发达的国家，它一方面长期倡导“互联网自由”，另一方面也是网络安全立法方面最发达的国家之一，特别是“9·11”事件以来，美国先后通过了《爱国者法》、《国土安全法》、《保护美国法》等法案，对互联网加以更为严密的监控。[7]

事实上，由于网络空间的发展带来的网络安全等问题和挑战具有全球性，采取不同措施对网络空间进行规制和管理，是包括西方发达国家在内的各国普遍做法。除了美国外，英国、德国、俄罗斯、日本、韩国等国家也制定了国内法，对互联网信息安全加以监管。[8]换言之，与网络自由主义者的主张和期待相反，国家和政府行为体通过法律化、制度化途径，正重新确立其在网络空间的权威；与互联网发展初期缺乏有效的管制规则相比，近年来越来越多的国家开始制定和实行针对网络空间行为的法律规范，明确了网络使用者、服务和内容提供者、网络信息和行为所涉管理机构等各方之间的权利和责任分配，从而将互联网有效纳入国家权威的管辖之下。[9]

基于这一现实状况，国家主权在网络空间的适用得到了日益广泛的承认。例如，2003年联合国信息社会世界峰会通过的《日内瓦原则宣言》明确表示：“与互联网有关的公共政策问题的决策权是各国主权”。2013年6月联合国信息安全政府专家组达成的一份共识性文件指出：“国家主权和在主权基础上衍生的国际规范及原则适用于国家进行的信息通信技术活动，以及国家在其领土内对信息通信技术基础设施的管辖权。”[10]之后，在网络空间“伦敦进程”下召开的2013年首尔会议、2015年海牙会议等各种国际场合中，有关国家主权原则适用于网络空间的上述共识一再得到重申。由20名西方国家相关专家历时三年完成、2013年3月由英国剑桥大学出版社出版的《关于可适用于网络战的国际法的塔林手册》（简称《塔林手册》），在规则1（主权）指出：“一国有权对其领土内的网络基础设施和网络活动行使控制权。”[11]2017年2月出版的《塔林手册》2.0版，更是以一章的篇幅对网络主权相关问题进行了阐述。[12]尽管这些文件使用的措辞有所不同（如网络空间的国家主权、网络主权等），但国家主权原则在网络空间的适用已经在国际实践中得到普遍认可。

二 国家在网络空间行使主权的原因

曾经长期游离于主权国家规制范围之外、被认为是一个“自足体系”的网络空间，为什么会在近年来走向“再主权化”？对此，可以从以下两方面来加以阐释。

第一，主权国家“需要”在网络空间行使主权。

无可否认，开放和充满活力的互联网是经济增长和社会进步的巨大推动力，但随着互联网的普及，网络袭击、网络犯罪、网络间谍、网络军备竞赛等网络安全的问题日益引发关注。同时，网络作为一种全新的信息传播方式，对各国的政治稳定和社会发展也有着举足轻重的影响。例如，2010年底以来被称为“阿拉伯之春”的西亚北非动荡和政权更迭中，脸书（Facebook）、推特（Twitter）等网络社交媒体对于反政府力量的组织联络发挥了很大作用。2013年的“棱镜门”事件，更是对各国围绕信息安全问题的博弈产生了深远影响。根据2013年6月美国国家安全局承包商雇员爱德华·斯诺登叛逃后的大量爆料，美国依仗其互联网技术优势和对网络资源的垄断，长期对包括中国在内的众多国家进行持续和大规模的监听、窃密行为。

联合国信息社会世界峰会2005年通过的《突尼斯议程》指出：“如果信息通信技术的使用违背了维护国际稳定和安全的目标，并可能对各国基础设施的完整性造成负面影响而有损于国家安全，就必须以有效手段应对由此产生的挑战和威胁。”[13]网络安全问题引发的广泛关注，足以解释为何各国普遍把网络安全作为国家信息安全乃至战略安全的重要组成部分，并通过不同措施对网络空间加以管制。在2011年叙利亚骚乱开始后，叙利亚政府下令切断了该国境内所有的互联网服务；白俄罗斯屏蔽了各种社交网络；土耳其政府要求网络服务提供商进行信息屏蔽；许多国家推动使用具有政治疆域色彩的本国域名（.cn、.fr、.uk等），伊朗等国甚至在策划建立本国局域网。[14]

第二，主权国家“能够”在网络空间行使主权。

“网络空间”这一名称，最早出现在科幻小说中。[15]尽管从网络空间与现实世界的紧密关联来看，将网络空间理解为一个“空间”有其合理性，[16]但该空间绝非大多数“去主权化”论者所主张或暗示的那样，是一个远离现实世界的独立和独特的空间。事实上，网络空间的物

质基础、活动者都与现实世界有着复杂的重合和互动关系。一般认为，网络空间既包含有形的网络基础设施（计算机、服务器、电缆光纤等等），也包含虚拟的信息。[17]就各种网络基础设施而言，它们通常总是位于特定国家的领土范围内，并显然会受到各有关国家主权的支配。同样地，那些在网络空间从事网络活动（如收发电子邮件、撰写博文等）的人员（即所谓“网民”）也通常位于特定国家的领土范围内，并受到该国法律的管辖。显然，对于这些同时“穿越”于虚拟网络空间和现实世界之中的网络基础设施和人员，国家毫无争议地可以对之行使主权。

而且，即使是对于网络空间的虚拟信息，国家也可以行使主权。2000年4月，法国互联网用户在网上发现美国雅虎公司驻欧洲分支网站拍卖纳粹物品，而法国雅虎公司则为法国的用户提供了相关链接。巴黎国际反种族主义和反犹太人歧视联盟等团体在法国巴黎大审法院以美国雅虎公司为第一被告、法国雅虎公司为第二被告提起了诉讼，法院最终判决：美国雅虎公司应采取一切可能的技术手段阻止法国用户对其亲纳粹物品拍卖网站的访问，否则将处以每日10 万法郎的罚金。该案成为国家通过司法手段对网络信息内容进行审查和管理的一个经典案例。

还应看到，当代信息技术的发展，为各国明确其网络主权的边界提供了更大的可能性。中国政府通过“金盾工程”（Golden Shield）对国内外网站进行信息过滤或屏蔽，就是一个很好的例证。[18]尽管中国政府采取的这一互联网监管措施历来受到西方国家的批评和责难，但它至少表明，“由于对互联网的广泛使用依赖于相应的有形设施，一个国家只要控制了这些有形设施，就能够控制网络空间”。[19]

总之，“去主权化”只是网络空间发展进程中的一种阶段性和过渡性的观念，它体现着浓郁的乌托邦色彩。从根本上说，网络空间的“再主权化”，是由国家的现实需要和技术能力决定的。其实，网络空间的发展，自始至终都依赖于各主权国家领土内的网络基础设施，其“网民”自始至终都是各主权国家的公民，从这一意义上说，它自始至终都受到国家主权的支配和管辖。“去主权化”观念在很大程度上反映了网络空间早期发展相对独立于国家干预的实际状况，但十分偏颇地夸大了国家主权适用于网络空间的难度。其实，各国之所以在早期较少参与网络空间治理和规制，从根本上说是因为网络空间较为成功的自我规制使它们缺乏干预网络空间事务的“需要”。但随着各种不法行为以及安全威胁不断涌现，国家不可能继续对此采取听之任之的态度，网络空间

的“再主权化”就成为一种必然的趋势。

三 网络主权的法律内涵

网络空间的“再主权化”，并非意味着各国围绕国家主权在网络空间的行使已经不存在分歧和挑战。一位西方学者指出：国家能否在网络空间行使管辖权这个“第一代问题”已经得到解决，现在面临的是如何行使管辖权这个“第二代问题”。[20]就国家主权在网络空间的行使问题而言，同样地，目前关键的分歧也在于国家主权应当如何（而非能否）在网络空间行使。

网络空间存在和发展的时间相对较短，它本身也在随着现代信息技术的发展而迅猛发展。目前可以确定的是，与此前人类涉足的陆地、海洋、空气空间、外层空间等空间相比，网络空间的构成更为复杂和特殊。在此情况下，人类对于这一新空间的认识还在不断深化之中，国家主权在网络空间的行使也必将处于发展演进之中。从学界对于网络空间的基本认识和相关的国家或国际实践来看，笔者认为：网络空间的构成是多样化而不是单一的，因此，国家主权在网络空间的行使也不宜一概而论，而应加以具体分析和区别对待。

首先，关于网络空间的物理构成即网络基础设施。如前所述，网络空间作为一个人造的空间，是由现实世界的不同国家包括有关企业、个人通过电脑、路由器、服务器等各种基础设施创造的空间，这些基础设施是网络空间的物理基础或硬件基础。由于通常而言有关基础设施总是分布在不同主权国家领土范围之内，从原则上说，各国对这些网络基础设施可以行使完全和排他的主权。对此，各主要网络大国之间并不存在原则性的分歧。

当然，西方国家倾向于强调主权国家对该国境内网络基础设施承担的义务，如对从其境内发起的网络攻击的监控、防范义务（又称为“审慎义务”，due diligence）。在西方国家坚持和推动下，2015年7月联合国信息安全政府专家组通过的新的共识性文件（A/70/174），就包含了多项与此相关的“负责任的网络空间国家行为规范”，包括各国不应蓄意允许他人利用其领土使用信息通信技术实施国际不法行为；各国不应违反国际法规定的义务从事或故意支持蓄意破坏关键基础设施的信息通信技术活动；各国不得使用代理人利用信息通信技术做出国际不法行

为，并应力求不让非国家行为体利用其领土实施这类行为；等等。[21]

笔者认为，任何国家不能利用网络设施从事或指挥、控制私人从事违反本国义务的行为（如干涉他国内政、网络攻击和网络监控），这在国际法上久已得到确认。各国应对本国境内私人使用网络基础设施对他国从事违法行为加以监控，但这种监控义务应与其能力相当，而不应被过度强化。[22]

其次，关于网络空间的虚拟信息。互联网已经成为当代信息传播与交流最重要的载体之一，这也决定了海量信息的传输和储存是网络空间的一个核心功用。特别是随着计算机和互联网技术的广泛应用，人类已经从单纯相互联结的互联网时代步入对信息搜集和挖掘的大数据时代。[23]因此，国家能否对网络空间的数据行使主权，是一个十分复杂和关键的问题。

前文已经述及，基于对网络基础设施的控制，国家完全有能力对网络空间的虚拟信息和数据行使主权和相应的管辖权。不过，由于网络空间的全球性和数据的可复制性，数据的跨国存储和全球传输成为一种常见现象，这也对国家主权和管辖权的行使提出了挑战。笔者认为，可以考虑借鉴海洋法上船旗国制度来解决这一问题。具体而言：

——一国政府、企业和个人所有的信息和数据，原则上由该国（“所有国”）行使主权，如无下文所列例外情形，只能由该国行使管辖权；

——一国（包括企业、个人）存储在另一国（“所在国”）服务器上的信息和数据，可以参照船旗国制度接受所在国和所有国的双重管辖；

——一国在全球互联网传输的信息和数据，所有接入互联网的国家都有可能行使管辖权，但在具体个案中则将如2000年雅虎案所揭示的那样，由特定国家根据有关信息和数据是否违反该国国内法等标准来决定是否行使管辖权。

由此可见，国家的网络主权既包括对其境内有形网络基础设施的主权，也包括对无形网络信息和数据的主权（即所谓“信息主权”或“数据主权”），二者缺一不可。如果说网络基础设施是网络空间不可或缺的“躯壳”或“载体”，网络信息和数据就是网络空间的“灵魂”之所

在；离开了“信息主权”或“数据主权”的网络主权，只能是丧失“灵魂”、残缺不全的主权。在现实中，一些西方网络大国及其学者往往强调国家对有形网络基础设施的主权而淡化甚至否定信息主权或数据主权。[24]这种对网络主权加以狭义理解的倾向，是有其目的和用意的。如同海洋法上有关领海宽度的争论所表明的那样，大国往往力图推动对主权含义和适用范围的限制性解释，以便使本国获得更大的自由行动空间。但是，将网络主权限制于对网络基础设施的主权是片面和有害的，它实际上将使某些大国利用网络空间互联互通的特点获得更多干涉和侵犯他国网络主权的自由。

种种迹象表明，围绕着国家主权应当如何在网络空间行使这一问题，各国的分歧还将长期存在。值得注意的是，国际上有关网络主权的讨论正在走向条文化、具体化的态势，在2013年和2015年两份共识性文件的基础上，新一届联合国信息安全政府专家组正在就国际法（包括国家主权原则）适用于网络空间的有关问题加以进一步探讨，并有可能在新的专家组报告中对此做出具体阐述。2017年出版的《塔林手册》2.0版中，对网络主权以及与此密切相关的管辖权、审慎义务等问题都分别设有专章，详细阐述有关的各项规则。[25]对于上述发展，中国没有理由置身事外，而亟须积极谋划和应对。

四 网络主权的中国立场

中国高度关注和重视网络主权问题，近年来积极倡导尊重和维护各国的网络主权，并以此作为我国关于网络空间国际法和国际秩序的核心主张之一。

早在2010年谷歌退出中国事件后，中国政府就在《中国互联网状况》白皮书中提出：“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。”在《中华人民共和国网络安全法》2015年6月初次审议稿、2016年6月二次审议稿和2016年11月三次审议稿中，“维护网络空间主权和国家安全”都被明确为立法宗旨。习近平主席2015年12月在第二届世界互联网大会发表的主旨演讲中，将“尊重网络主权”列为推动全球互联网治理体系变革的四大原则之首，并将网络主权阐释为“尊重各国自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利，不搞网络霸权，不干涉他国内政，不从事、纵容或

支持危害他国国家安全的网络活动”。[26]

当然，围绕着国家主权的内涵和行使方式等问题，中国与主要西方国家之间还存在一些重要分歧。西方国家还常常以“威胁跨境数据流动”、“分割全球互联网”等说辞，对我国的有关主张加以“妖魔化”。以数据（信息）主权为例，习近平主席2014年7月在巴西国会发表的《弘扬传统友好 共谱合作新篇》演讲中，就强调了“信息主权”的重要性。我国的《网络安全法》第37条规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”其他法律法规中，也对数据监管包括本地存储等要求做出了相应规定。[27]但是，美国、欧盟等西方国家多次对我国的有关主张和立法加以反对，要求保障所谓“数据自由流动”，并谋求在《跨太平洋伙伴关系协定》（TPP）等国际条约中制定反映其主张的国际规则。[28]

互联网信息监管和内容审查，是关于网络主权的另一个重要争议问题。中国政府在多个国际场合一再提出：各国有权根据本国的网络发展水平、历史传统、文化语言和风俗习惯等，在充分考虑本国广大民众意愿和适当借鉴国际通行做法的基础上，制定本国的网络公共政策和法律，并依法管理互联网；中国与俄罗斯等六国共同向联合国大会提出的《信息安全国际行为准则》，也重申与互联网有关的公共政策问题的决策权是各国的主权，强调各国有责任和权利依法保护本国信息空间及关键信息基础设施免受威胁、干扰和攻击破坏。[29]但是，西方国家多年来（特别是2010年“谷歌事件”后）一直对我国的互联网监管措施加以指责，声称中国用以过滤网络信息和屏蔽特定网站的所谓“防火墙”将分割全球互联网。

必须看到，网络主权问题已经成为当前网络空间国际竞争的焦点问题。在网络时代，“没有网络安全就没有国家安全”的观念日益被接受。同样地，“没有网络主权就没有国家主权”的观念也必将得到接受。正如国家主权原则是现代国际秩序和国际法的基石，网络主权原则也将是网络空间国际秩序和国际法的基石。谁能够掌握网络主权问题的话语权和主导权，谁就能够在网络空间秩序构建和规则博弈中占据制高点。从这一意义上说，当前国际上的网络主权之争也就是网络领域的主导权之争。

当务之急，我国政府应当通过认真研究网络主权问题的发展态势和最新动向，更加深入地参与到网络空间国际对话和立法进程中，既充分反映自身的利益和主张，又着眼于网络空间命运共同体和人类共同利益，推动网络空间国际秩序和国际法制度的构建。笔者的主要对策建议包括：

第一，通过更加积极有为的网络外交，进一步树立中国作为负责任的网络大国的国际形象。一些西方国家政府和媒体出于意识形态上的敌对和树立“假想敌”的需要，多年来在互联网信息监管等问题上对中国妄加指责，肆意曲解、攻击中国有关网络主权的主张，不断炒作“中国网络威胁论”、抹黑中国的国际形象，对中国参与网络空间国际对话和规则制定产生了较为严重的消极影响。中国政府应当利用各种多边、区域和双边渠道，更加积极有为地对外开展网络外交，从法理和事实层面驳斥西方国家对中国网络主权观的无端指责。与此同时，我国也应当在国内继续大力奉行“依法治网”，加快改革和完善互联网管理体制。这些举措，将有助于我国在围绕网络主权的国际博弈中占据道义制高点，进一步树立中国作为负责任的网络大国的国际形象，从而增强我国的话语权和影响力，使我国有关网络主权的主张得到最大限度的宣扬和接受。

第二，“知己知彼”，大力加强对我国以及其他主要国家相关主张的理论研究。中国政府关于网络主权的系列主张，已经在国际上产生了很大影响。当然，在网络主权的具体内涵（特别是数据主权、互联网信息监管的理论依据和行使方式）、网络主权与网络空间命运共同体的关系以及网络主权和网络人权的关系等问题上，还有待于政府和学界共同开展深入、扎实的研究，通过坚实的理论支撑来加强我国有关主张的说服力和影响力。除此之外，我国还应积极跟踪美国、欧盟、俄罗斯等主要网络大国在网络主权问题上的最新政策和立法，这包括但不限于：（1）欧美国家数据保护和监控立法，以及美国与欧盟关于个人数据分享谈判的最新进展；（2）TPP电子商务和数据流动条款对数据主权的影响；（3）美国、德国、英国、俄罗斯等主要大国互联网监管的立法态势；（4）美国等西方国家在联合国信息安全政府专家组、“伦敦进程”以及“塔林2.0”项目等国际场合关于网络主权问题的政策倾向。只有这样，才能做到“知己知彼”，准确定位我国在网络主权问题上的核心利益所在。

毋庸讳言，与主要发达国家相比，我国现有网络空间法（包括国际

法）领域的研究力量较为分散、单薄，难以形成合力；在政学互动层面，除了有限的个例外，学者与政府部门的联系和协作较为有限，不利于二者优势互补，共同加强相关理论研究。为此，我国亟须加大智库建设力度，重点在网络空间法领域建设若干家有较强实力的专业化智库；同时，应当制度化、常态化地鼓励、吸收相关学者参与决策咨询和实际工作，通过政府与学界、企业等方面的资源整合和力量配置，形成优势互补、供需对接、高效协作、有序运转的理论研究机制体制。

第三，通过网络外交和法律外交，使正在酝酿和形成中的网络主权国际法规则、制度真正反映和维护本国利益。近年来，中国政府日益重视网络外交，国家网信办、外交部等部门都做了大量卓有成效的工作。在当今国际社会，国际法已经成为国家之间交往和博弈的通行话语，我国政府也应当更加重视网络领域的法律外交，善于运用法律的逻辑、法律的话语来表达、反映我国在网络主权问题上的利益和诉求，用法治的思维来传播中国话语，提出中国主张，形成中国方案。在国际上有关网络主权的讨论走向条文化、具体化的背景下，中国作为网络空间的核心利益攸关方之一，应当立足于通过实质性地引领国际议题、主导规则内容、影响相关国际规则的制定和形成，使正在酝酿和形成中的网络主权有关规则真正反映和维护本国利益。具体而言，我国应当着眼于推动数据主权、互联网信息监管等问题的谈判议题，充分发挥在乌镇世界互联网大会、上海合作组织、亚非法律协商组织以及联合国信息安全政府专家组、“伦敦进程”等机制内的话语权和影响力，以此引领谈判议题、引导规则内容。在有关网络安全的国际条约短期内难以制定的情况下，我国还应高度关注国际组织决议、非约束性行为准则、国际专家组报告等“软法”在网络主权问题上的重要影响。

总之，中国作为最早倡导网络主权的国家之一，应当立足于网络空间命运共同体理念，通过网络主权实现国家利益和人类共同利益的平衡，维护网络空间的互联互通、共享共治，有力地回击西方国家对我国网络主权主张的“妖魔化”。

五 结语

网络主权是国家主权在网络时代的自然延伸，它丰富和扩大了国家主权的内涵，并使网络空间的“威斯特伐利亚时代”开始渐具雏形。[30]同时，网络主权也是应对主权国家在网络空间正当安全关切的

必然产物。如两位美国著名学者所说：“对于互联网的未来，最大的危险不是来自政府的过度反应，而是来自政府根本不反应。”[31]

网络主权的确立有其必然性和合理性，是网络空间国际治理向正确方向迈出的重要一步。不过，网络主权并不意味着网络空间的分裂化和碎片化。近年来，许多国家网络“不安全”观念不断被强化，2013年“棱镜门”事件所曝光的美国政府从事的各种大规模网络监控和窃密，尤其影响深远。这一态势的发展，有可能促使各国越来越多地加强网络安全管制，甚至威胁网络空间的可持续发展。[32]面对这一新的挑战，主要网络大国应承担更大责任，避免滥用其在网络领域的优势威胁他国的网络安全。另一方面，各国还应加强对话与合作，增进网络空间的互信，维护网络空间的互联互通、共享共治。

---

[1] The White House，Cyberspace Policy Review：Assuring A Trusted and Resilient Information and Communications Infrastructure，http：//www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_f一种相近的定义认为，网络空间“是指基于全球计算机网络化，由人、机器、信息源之间相互联结而构成的一种新型的社会生活和交往的虚拟空间”。参见罗楚湘《网络空间的表达自由及其限制——兼论政府对互联网内容的管理》，《法学评论》2012年第4期。

[2] John Perry Barlow，A Declaration of the Independence of Cyberspace，http：//projects.eff.org/～barlow/Declaration-Final.html.

[3] David R. Johnson and David G. Post，“Law and Borders：The Rise of Law in Cyberspace”，Stanford Law Review，vol. 48 （1996），no.5，p.1367.

[4] US Department of Defense，The Strategy for Homeland Defense and Civil Support，https：//fas.org/irp/agency/dod/homeland.pdf.美国国防部2010年发布的《四年防务评估报告》也做出了基本相同的表述。See US Department of Defense，Quadrennial Defense Review Report，February 2010，p.8.

[5] Hillary Rodham Clinton，Remarks on Internet Freedom（Jan. 21，2010），
http：//www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[6] Ralf Bendrath & Jeanette Hofmann，The Return of the State in Cyberspace—Regulation and Legitimacy on the Internet：The Domain Name System and Privacy，
http：//kms2.isn.ethz.ch/serviceengine/Files/CRN/46735/ieventattachment_f 41C7-4461-BD32-556D7 FEA976B/en/BendrathHoffmann_The-Return-of-the-State-in-Cyberspace-final.pdf.

[7] 参见尹建国《美国网络信息安全治理机制及其对我国之启示》，《法商研究》2013年第2期。

[8] 参见顾华详、安娜《国外依法保障网络信息安全措施比较与启示》，《法治论丛》2011年第2期。

[9] 刘杨钺、杨一心：《网络空间“再主权化”与国际网络治理的未来》，《国际论坛》2013年第6期。

[10] See United Nations General Assembly，Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security（A/68/98），para.11，paras. 19-20.

[11] Michael Schmitt （ed.），Tallinn Manual on the International Law Applicable to Cyber Warfare，Cambridge University Press，2013，p.15.

[12] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp.11-29.另见本书中“对《塔林手册》2.0版网络主权观的初步评价”一节的相关讨论。

[13] WSIS，Tunis Agenda for the Information Society（WSIS-05/TUNIS/DOC/6（Rev.1）-E），para. 35（a），

http：//www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[14] See Stephen Gourley，“Cyber Sovereignty”，in Panayotis Yannakogeorgos & Adam Lowther （eds.），Conflict and Cooperation in Cyberspace：The Challenge to National Security，Taylor & Francis，2014，p.277.

[15] 1984年，移居加拿大的美国科幻作家威廉·吉布森（William Gibson）写下了一本书名为《神经漫游者》（Neuromancer）的长篇科幻小说。该小说描写了一名受雇于某跨国公司的反叛者兼网络独行侠凯斯，被派往全球电脑网络构成的空间里去执行一项极具冒险性的任务。进入这个巨大的空间（吉布森取名为“网络空间”，cyberspace），凯斯并不需要乘坐飞船或火箭，只需在大脑神经中植入插座，然后接通电极，电脑网络便被他感知。当网络与人的思想意识合为一体后，人即可遨游其中。在这个广袤的空间里，看不到高山荒野，也看不到城镇乡村，只有庞大的三维信息库和各种信息在高速流动。小说出版后，好评如潮并获得多项大奖，“网络空间”的名称也由此开始被广泛使用。参见百度百科“网络空间”条目：http：//baike.baidu.com/link?url=1Jp2wQNsrWU_BnZzA5i72q_XdpZAea564xSCWuMdVDt7X6U7vRbTIETGdbpjazUvS1NjerijPNZCsku760K。

[16] See Julie Cohen，“Cyberspace as/and Space”，Columbia Law Review，vol.107 （2007），pp.213-215.

[17] See Joseph Nye，“Nuclear Lessons for Cyber Security? ”，Strategic Studies Quarterly，Winter 2011，p.19.

[18] 国外一般称为“中国防火长城”（the Great Firewall of China）。根据维基百科的解释，“防火长城主要指中国政府监控和过滤互联网内容的软硬件系统，由服务器和路由器等设备，加上相关的应用程序所构成。它的作用主要是监控网络上的通信，对认为不符合中国官方要求的传输内容，进行干扰、阻断、屏蔽。由于中国网络审查广泛，中国国内含有“不合适”内容的网站，会受到政府直接的行政干预，被要求自我审查、自我监管，乃至关闭，故防火长城主要作用在于

分析和过滤中国境内外网络的信息互相访问”。参见维基百科“防火长城”条目，
http：//zh.wikipedia.org/wiki/%E9%98%B2%E7%81%AB%E9%95%BF%E

[19] Timothy S. Wu，“Cyberspace Sovereignty? —The Internet and the International System”，Harvard Journal of Law & Technology，vol. 10（1997），no. 3，p.651.

[20] Benedikt Pirker，“Territorial Sovereignty and Integrity and the Challenges of Cyberspace”，in Katharina Ziolkowski（ed.），Peacetime Regime for State Activities in Cyberspace：International Law，International Relations and Diplomacy，CCDCOE，2014，p. 194.

[21] See United Nations General Assembly，Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security（A/70/170），para. 13.

[22] 例如，由于网络攻击的隐秘性等特点，在没有证据证明存在甲国政府对私人行为体的指挥或控制，或攻击来自甲国境内但攻击者身份难以查实的情况下，一些西方国家政府和学者极力主张，应当对网络攻击实行“转嫁的责任”（imputed responsibility），即如果一国未能采取必要的措施来预防从该国领土内发起的网络攻击，这些网络攻击将被转嫁于该国，并因此而产生该国的国家责任。但是，这一主张不适当地放宽了现有国际法上的归因标准、扩大了（疑似）攻击源头国的责任范围，有着很大的片面性和危险性。对这一问题更加详尽的讨论可参见黄志雄《论网络攻击在国际法上的归因》，《环球法律评论》2014年第5期。

[23] 参见梁亚滨《网络空间：大数据时代国家博弈的新领域》，《学习时报》2014年10月20日。

[24] See e.g. Michael Schmitt（ed.），Tallinn Manual on the International Law Applicable to Cyber Warfare，Cambridge University Press，

2013，pp.15-17；Wolff Heintschelvon Heinegg，“Legal Implications of Territorial Sovereignty in Cyberspace”，in C. Czosseck，R. Ottis，K. Ziolkowski （eds.），2012 4th International Conference on Cyber Conflict，NATO CCD COE，p.7.

[25] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp.11-78.

[26] 《习近平在第二届世界互联网大会开幕式上的讲话（全文）》，新华网，http：//news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm。

[27] 另见本书中第七章中的相关讨论。

[28] TPP第14章（电子商务）有关条文规定：“TPP缔约方承诺，将在确保保护个人信息等合法公共政策目标得到保障的前提下，确保全球信息和数据自由流动，以驱动互联网和数字经济。12个缔约方也同意，不将设立数据中心作为允许TPP缔约方企业进入市场的前提条件，也不要求转让或获取软件源代码。”

[29] 《信息安全国际行为准则》，http：//www.fmprc.gov.cn/mfa_chn/ziliao_611306/tytj_611312/zcwj_611316

[30] 关于网络空间“威斯特伐利亚时代”的名称和含义，可参见Chris Demchak & Peter Dombrowshi，“Rise of a Cybered Westphalian Age”，Strategic Studies Quarterly，Spring 2011，pp.32-61。

[31] See Jack Goldsmith & Timothy Wu，Who Controls the Internet? ： Illusions of A Borderless World，Oxford University Press，2008，p.145.

[32] 例如，巴西等多个国家在“棱镜门”事件后开始考虑数据本土化存储的要求。See Paulo Trevisani & Loretta Chao，“Brazil Retreats on Plan That Drew Google’s Fire”，Wall Street Journal，20 March，2014，

http：//online.wsj.com/news/articles/SB10001424052702304026304579449730185773.

第五章

网络空间主权的制度建构

网络空间重要性的凸显与中国法学理论的不足使得我们有必要对网络空间主权进行一番追根溯源的梳理，把握其流变，反思其现状，进而构造出既反映网络空间特征，又体现中国特色的网络空间主权法律理论和制度体系。

一 从“网络自身主权”到“网络空间主权”

2015年7月1日生效的《中华人民共和国国家安全法》，首次将“网络空间主权”以法律形式予以明确。时隔仅5日，《中华人民共和国网络安全法（草案）》发布，第一条便开宗明义地申明“维护网络空间主权”的立法主旨。2015年12月16日，国家主席习近平在第二届世界互联网大会的主旨演讲中，进一步将“尊重网络主权”列为全球互联网治理体系四项原则的核心。[1]

尽管网络空间主权理念已经成为中国处理网络事务的根本指针，但它的正当基础和法理意涵仍缺乏充分探究。中国的主流观点将网络空间主权简单视为国家主权在网络空间的自然延伸，[2]却回避了虚拟空间与真实领土之间的差异与矛盾，从而无法有效回应西方否定网络空间主权的种种主张。另一方面，从网络空间特性出发的“信息主权论”和“制网权论”又不恰当缩限了国家主权的范围：前者仅以网络信息的控制、管理和共享为内容，并未考虑更广泛的网络设施和网络行为；[3]后者把网络主权理解为国家对互联网根域名的控制权、网络地址的分配权、互

联网标准的制定权、网上舆论的话语权等国家能力层面，缺失了国家主权制度应有的规范性，亦无法建构出以国际合作为基础的全球治理新框架。[4]网络空间重要性的凸显与中国法学理论的不足使得我们有必要对网络空间主权进行一番追根溯源的梳理，把握其流变，反思其现状，进而构造出既反映网络空间特征，又体现中国特色的网络空间主权法律理论和制度体系。

“网络空间主权”（Cyberspace Sovereignty）这一用语并非中国的独创，而是由美国著名网络法学者吴修铭（Timothy S. Wu）在1997年的《网络空间主权？——互联网与国际体系》一文中率先使用，[5]与之相关的学术讨论更可追寻到美国电子空间法律研究委员会主席戴维·约翰逊（David R. Johnson）和戴维·波斯特（David Post）教授的开创性文献《法律与边界——网络空间中法律的兴起》。[6]放宽时间的视野，不难发现在过去二十年间，西方理论界对网络空间主权经历了从抗拒到有条件接受的转变。1996年，约翰·P. 巴洛在《网络空间独立宣言》中慷慨陈词：工业世界的政府们，我来自网络世界——一个崭新的心灵家园，在我们这里，你们并不受欢迎，你们没有主权。[7]在电子前线基金会及其《连线》杂志的鼓吹下，“网络主权”展现出与惯常理解截然相反的含义，那就是“网络自身主权”（Cyberspace as Sovereignty）。然而，这种网络空间独立自足的乐观主义很快褪色了。人们日益发现，“网络自身主权”所依凭的信息技术并没有使政治和权力消失，反而在某种意义上强化了它：一种新型的权力——网络权力（cyberpower）出现了。通过基础设施、代码及人类技能，网络权力能够创造、控制和沟通相互联系的信息资源，从而在网络空间之内和之外达致期望的结果。[8]正因如此，哈佛大学国际法教授杰克·戈德史密斯（Jack L. Goldsmith）等人主张，鉴于构成互联网的硬件和软件都位于一国领土之内，基于领土的主权正当化了国家对其网络使用者的规制。[9]

历史不会简单地重复自身。网络空间再次找回的“国家”并未承担着和此前现实空间中一样的角色。从信息流动到政治忠诚，从国内组织到国际秩序，网络空间中国家形象的改变不可避免。对此，作为互联网发源地的美国抢占先机，将网络空间与海洋、国际空域、太空相提并论，划入单一主权国家无法企及的全球公域（global commons），进而呼吁建立网络空间的多利益攸关方治理模式（Multi-stakeholder Governance Model）。[10]显而易见，美国试图通过定义权的巧妙行

使，将网络技术和架构优势一举转变为政治和战略优势。尽管全球公域理论居于西方主流地位，但质疑的声音仍不断发出。[11]2013年“棱镜门”事件所曝光的网络监控和窃密行为进一步激起了网络空间主权和治理模式的世界论战，至今仍硝烟弥漫，远未止歇。[12]

透过国内外围绕网络空间主权所生发的纷纭聚讼，一系列核心问题得以浮现：（1）国家主权能否适用于网络空间？（2）网络空间中国家主权的行使是否遵循多利益攸关方治理模式？（3）如何建构逻辑清晰、体系严谨、富有特色的网络空间主权国内法体系？（4）如何以网络空间主权为基础，铸就多边、民主、透明的国际法制度？针对上述疑难，本章首先提出对国家主权的基本观点，以论证网络空间主权的正当性。进而，在揭示多利益攸关方治理模式和全球公域理论的缺陷之后，阐明“基于网络空间主权”治理模式的理据。从本章的第三部分开始，我们从政治上的网络空间主权转向法律上的网络空间主权性权力和权利，一方面梳理网络空间的国内立法权、行政权、司法管辖权，另一方面将中国网络空间主权的主张与国际法的制度相互融合，希冀为国际法框架下的网络空间主权及互联网全球治理体系的完善提供有益的参考。

二 国家空间主权的正当性

尽管国家主权和网络空间一古老一簇新，但时代的隔阂并没有成为两者融贯的壁垒。相反，正因为它们都处在网络社会的巨变之中，凭借着社会的网络化和网络的现实化，国家主权和网络空间同时演化、彼此交织，网络空间主权的正当性由此确立。

（一）国家主权：“变”与“不变”

1. 国家主权的传统与挑战

国家主权可能是最能主导我们认识国家自身及其与国际关系的概念，它的历史与现代国家的演变合若符契。[13]早在古希腊时期，柏拉图和亚里士多德就曾对城邦的最高权力（suremitas）有所论述，现代意义上的“国家主权”概念则源自法国学者让·博丹的《共和六书》，意即凌驾于公民和臣民之上的最高和绝对的权力。[14]通过主权与国家的永恒连接，不可分割、不可转让、不可消灭的主权不但成为国家的固有权力，更是国家权力统一的正当性渊源，现代主权国家的原型由此诞

生。之后，荷兰法学家格劳秀斯将主权从国内政治引入国际关系之中，他在《战争与和平法》一书里指出：凡行为不受其他人的权力的限制，从而不因其他人的意志的行使而使之无效的权力，就是主权。[15]1648年的《威斯特伐利亚和约》吸取了这一思想，从而确立了以国家为基本单位的国际体系。据此，主权一体两面，一面着眼国家权威与个体及组织之间的“纵向关系”，是主权概念的基础；一面指向国家与其他国家的“横向关系”，是主权概念的拓展。此即“内部主权”与“外部主权”的二元论。[16]

内部主权和外部主权有着不同的理论导向，前者以“主权归属”为鹄的，后者以“主权绝对”为中心。在时代变迁的背景下，内部主权依次呈现出君主主权、议会主权、国家主权、人民主权等各种样态。时至今日，人民主权已经成为各国普遍适用的基本准则，我国《宪法》第2条“中华人民共和国一切权力属于人民”亦属之。这意味着唯有人民才是国家权力的来源，也唯有来自人民授予的权威，国家权力才具有正当性。与国家内部主权归属的共识迥异，20世纪60年代以来，伴随着国际人道主义和人权观念的高涨、经济全球化的兴起以及地区的一体化，国家外部主权的绝对性备受挑战。[17]简言之，基于种族灭绝、人道灾难和国家崩溃的国际干涉动摇了国家主权的排他性，资本主义的跨地域发展和巨型企业的出现使得国家丧失了独立执行宏观经济政策的能力，最后，以欧盟为代表的欧洲议会、欧盟宪法、欧元等新的国际制度越过了民族国家的藩篱，标志着从国家主权主义向世界主义转变以及国家自主性的削弱。据此，形色各异的“主权过时论”开始涌现，以至于有人声称在当代全球化的背景下，主权已经消失了。[18]

2. 主权的坚守与调适

主权绝对性被侵蚀的事实，绝不意味着主权的瓦解。这首先因为，作为国家与非国家（个人、社团、法人、非政府组织和国际组织）区分的标志，“主权”与“国家”具有同质性，借用国际法院法官詹姆斯·理查德·克劳福德（James Richard Crawford）的表述，“主权国家”是一种有意味的同义反复。[19]因而，离开了“主权”概念，国家将无从定义。不仅如此，主权还在国家秩序的形成过程中发挥着核心作用。[20]在相互尊重主权的框架下，国家享有自由订立国际条约、磋商条约内容以及要求他方遵守条约的权利。在这一意义上，“主权”恰恰致力于“在一个混乱与失序的世界中确立秩序与条理”，从而给我们这

个缺乏共同价值观的危险的国际体系以唯一的安全网。[21]正因这样，建立在主权原则之上的《联合国宪章》才获得了实质的正当性。但不可否认的是，如联合国前秘书长加利所言，绝对和排他性的旧主权原则已经不再站得住脚，现在必须重新思考主权问题，承认它的更多形式，以发挥更多的作用。[22]有鉴于此，美国国际法学者路易斯·亨金（Louis Henkin）在海牙国际法学院做讲座时指出：我们必须将一些关于主权的比喻、假象剥离，令国家本质特征显露出来，那就是承认、尊重和促进一个国家在没有外来强迫和限制的情况下做出决定，据此，主权应祛除绝对性的神话，而代之以“主权独立”和“主权平等”。[23]

“主权就是独立，主权国家就是独立国家。”[24]前南斯拉夫问题国际刑事法庭法官李浩培先生的论断与国际法权威著作《奥本海国际法》高度一致：主权是国内的最高权威，但在国际法上并非意味着高于所有其他国家，而是含有全面独立的含义。[25]较诸主权绝对，主权独立更侧重于在消极层面制止他国干涉本质上属于国家国内管辖之事件，尤其是领土的完整和政治的独立（《联合国宪章》第2条第4款）。此外，“主权”还标志了独立国家之间的平等关系。[26]作为《联合国宪章》对主权的唯一直接表述，所有会员国主权平等原则（第2条第1款、第78条）被世界各国一致接受，从而构成了主权本质要求以及国际关系和国际法体系的基础。

然而，独立和平等并不是主权的全部内涵。如果说安全和经济是主权的功能性目标，[27]那么各国日益发现：为了达致这一目标，它们不得不更少地依赖单个的国家手段，而更多地依赖复杂的国际体制（international regime），意即“一系列围绕行为体预期所汇聚到的一个既定国际关系领域而形成的隐含的明确的原则、规范、规则和决策程序”。[28]军事技术的发展，特别是核武器的问世使得任何地理的防御屏障都不复存在，各国都不得不锁定在一个被动的相互影响格局中。与此同时，跨越国境的资本、商品、人员、知识和信息的流动促成了经济一体化，增进了各国在经济上的主动依存度。虽然安全和经济已经成为国家之间的共同利益，但这并不意味着世界和平；相反，相互依赖造成的冲突和摩擦加大了国际关系的敏感性和脆弱性。这令人们认识到：国际和平的维持以及随之而来的独立民族国家的维持，从长远来看，是以各国交出一部分主权为条件的。[29]就此而言，对主权的自愿让渡和自我限制并未贬损主权，相反，它通过广泛的国际义务恰恰提升了国家主权的行动能力。[30]这里的“义务”首先是建立国际体制——一套促

进国家间合作的正式和非正式规则——的合作义务。据此，国家不只是单纯的“自由施动者”（free agents），更是前南斯拉夫问题国际刑事法庭庭长安东尼奥·卡塞斯法官（Antonio Cassese）所称的“国际共同体成员”，[31]因而“被期望能够遵守共同体演进中的关于正当性的相关规范”，通过透明、互相公开和互赖的国际体制来实现“共同利益”。[32]故此，该等义务不但是普遍的，即适用于所有国家，还是基本的，即旨在保护安全、和平、人权等重要价值。

总之，那些关于“主权死亡”的说法显然夸大其词，事实上，国家不但可以自由地行使主权，而且其利益保护也需要它。[33]就内部而言，它仍意味着人们所赋予的一国领土之上的最高权威，可就外部而言，它已经改变了绝对不可侵犯的强硬面貌，而是体现为排除他国干涉、平等开展国际活动和承担国际共同体义务的国际资格。[34]

（二）网络空间主权：质疑与可能

“网络空间”（cyberspace）诞生于美国科幻作家威廉·吉布森1984年的小说《神经漫游者》，意指由计算机所创建的虚拟信息空间。但只有1989年万维网出现后，网络空间才走进现实。2003年，美国的《保护网络空间的国家安全战略》（National Strategy to Secure Cyberspace）首次正式阐释“网络空间”，即“它由无数相互关联的计算机、服务器、路由器、交换机和光缆组成，并支持着国家基础设施的运转”。[35]随着信息技术的发展，网络空间从以互联网设施为中心的界定向更宽泛的含义迈进。2011年，《英国网络安全战略》（The UK Cyber Security Strategy）把网络空间视为由多个数字网络组成的人际互动域（domain），它以存储、修改和交流信息为目的。此时的网络空间不但被实体化了，而且超越了计算机网络，囊括了各种通信网络、军事网络、工业网络和服务网络。[36]晚近，国际电信联盟（International Telecommunication Union）进一步将之拓展为：“由包括计算机、计算机系统、网络及其软件支持、计算机数据、内容数据、流量数据以及用户在内的所有要素或部分要素组成的物理或非物理领域。”[37]在网络空间内涵日渐丰富、外延不断扩张的背景下，本章将“网络空间”理解为“以信息通信设施及其使用者为基础，以数字化信息创造、存储、修改和流动为内容的互联互动空间”。

1. 网络空间的可规制性：国家主权介入的前提

网络空间之上的主权（sovereignty over cyberspace）所面临的首要挑战是“网络自身主权”论者的争辩：国家对网络空间的规制是不可能或徒劳无功的。[38]他们认为：作为塑造网络空间的核心力量，互联网基础架构（internet architecture）中的“端对端”（End to End）原则通过将更多的权力和创新交由“终端”，降低网络核心的复杂性，从而促成了网络的去中心化。[39]因此，与之前的电报电话网依循的等级原则不同，网络空间中没有一个集中控制的总开关，信息的传递不再依赖于单一通道，而是将信息流动的权利赋予每一个使用者。[40]多路径、分组交换机制以及TCP/IP协议组，使得数据的生产、传输和解读彼此分离，这一设计颇具深意，它不但是网络结构最优设计的反映，更是排斥政治控制理念的反映。[41]正因如此，“不可规制性”才成为网络空间的本质属性。

虽然“网络自身主权”论者言之凿凿，其实却混淆了应然与实然，将国家不应干预的规范性主张和不能干预的描述性说明等量齐观。网络空间的真相是：并没有特定的架构决定着互联网的本质，支撑互联网的可选择架构可以开放或者封闭，谁在使用网络、使用者从何处来、他能够发送何种信息均可以被代码控制，不同的代码进而产生了不同的网络和生活，故“可规制性”是架构设计的效力之一。[42]诚然，互联网的存在必须满足认证、兼容、互联等最低限度的架构要求，可与之相关的规制却进一步证明了网络空间规制的可行性。[43]首先，“认证”（identification）通过对每一个用户或计算机分配独一无二的网络地址，即域名系统来实现。作为全球互联网最重要的集中控制点，互联网名称与数字地址分配机构对域名注册享有绝对的权力，从而可以用来执行相关的非技术性政策。其次，“兼容”（compatibility）意味着交互操作中技术标准的统一。目前，国际互联网工程任务组（IETF）和万维网联盟（W3C）负责互联网标准的开发和推动，以解决不同平台、技术和开发者带来的不兼容问题。尽管这些标准只是推荐性的，可在网络效应下，一旦它们成为主流，就变为人们不得不遵守的强制规范。更重要的是，互联网标准并不纯粹是技术性的，它们的使用者将被有意无意地锁定在潜藏的商业利益、政治偏好和道德评价之中，[44]互联网协议第6版（IPv6）的发布和推广即是例证。最后，“互联”（interconnectivity）要求网络运营者在“认证”和“兼容”的条件下达致计算机、局域网、万维网之间的互联互通。近年来，围绕着网络互联还是分裂，美国和欧盟展开了“网络中立性”（network neutrality）的论辩，其核心在于“端对端”是否依然为宽频时代的最

佳架构。2010年，美国联邦通信委员会通过了“维护网络开放性”（Preserving the Open Internet）法令，以管制网络服务提供商的服务提供，借由透明度、禁止封锁、禁止不合理的差别待遇等三大规则防止其滥用市场控制权，以维护网络中立性。[45]对此，网络服务提供商反对说，禁止差别定价的管制将扼杀升级设备的投资意愿，反而限制产业创新的自由。[46]这场企业与政府之间的争讼目前仍无定论，[47]但它从根本上动摇了网络空间不可规制的观念。

2.真实的网络空间：国家主权介入的背景

网络空间“独立性”是国家主权的另一道屏障。“网络自身主权”论者从例外主义（exceptionalism）出发，将网络空间视为“自主之所”。简言之，计算机的跨界沟通打破了地域桎梏，动摇了基于领土的民族国家合法性，创造出人类活动的新领域。在该领域中，显示器、账号、网址、密码所组成的虚拟边界取代了地理边界，一个与原子世界不同的比特世界诞生了。[48]在该世界中，“网民”而非“公民”通过伦理道德、个人自律和对共同利益的驱动来达成“社会契约”，并经由自我规制守卫着网络空间的秩序。不过，这种将网络空间与日常空间区隔的观点固然正确认识到人们对网络的真切感受，即与现实空间迥然不同的“可经验空间”（experienced space），却忽视了虚拟与现实之间的密切关联。站在网络空间之外观察，“空间”不过是一种隐喻，一种学术浪漫主义。[49]因为并没有什么“空间”（space），有的只是计算机构成的，与信件、电话甚至古老的烽火一样的信息媒介网络。[50]

显然，无论是将网络空间视为独立空间的内部视角，还是将其视为现实空间延伸的外部视角，都有失偏颇。事实上，今天的人类存在空间已经成为物理-网络空间——一个原子和比特高度融合、不可分割的世界。就此而言，我们可以用“网络化的空间”（networked space）来将“空间”和“网络”这两面融为一体。[51]质言之，它是一个以信息技术为驱动的，由节点（node）、纽带（tie）和流量（flow）组成的流动性空间。[52]“节点”中既有分散的网络用户，也有庞大的网络服务提供者；节点之间的“纽带”既指电缆、交换器等物理设施，亦指如TCP/IP网络连接的核心协议；通过纽带传递的“流量”不但包括各种无体资源，也包括与人格相关的个人信息。因此，网络空间的特色不是虚拟的或现实的，而是虚拟空间和现实空间的“跨越”与“互动”。[53]它在象征意义上是虚拟的连接，在功能意义上却依赖于物理场所和国家

领地。就此而言，网络空间是一个脱胎于现实，可又区别于现实的他性空间，一个福柯意义上的“异托邦”（heterotopies）。[54]

如今，网络空间与现实世界的互动与日俱增，资源创造和分配的冲突越发激烈，网民之间的简单合意或自由联合再也不能应对纷繁芜杂的纷争，网络空间的自我规制无法持续，国家主权重新降临的契机已经到来。

3. 信息主权：国家主权的焦点

网络空间是人们数字化生存的空间，通过信息通信技术的运用，模拟化的现实空间被尽其所能地转化成海量的二进制代码，世界的一切都将被测量、记录、分析、分享和预测，这正是网络空间中最具决定性的力量。[55]与数据化信息相关的信息主权（information sovereignty）也由此成为网络与国家论战的主要舞台。[56]

在这一舞台上，首先上演的是信息自由和国家控制的“价值对抗”。西方学者将网络空间中的信息自由归入《世界人权宣言》、《公民权利与政治权利国际公约》项下的言论自由，进而将互联网视为前所未有的“解放科技”和“自由民主工具”，[57]主张国家放弃对网络信息的干预。然而，这种人为对立既误解了“网络”，也误解了“自由”。网络空间并非自在自为之物，而是由主权国家参与形成的“人为之物”，实际上，不论是互联网的诞生，还是其迅猛发展都是国家积极推动的结果。[58]时至今日，从信息的生产、搜集到信息的交换、传输和利用，国家已深深嵌入其中。[59]另一方面，作为一个由社会和政治建构的概念，信息自由并非技术的自然结果，它铭刻着文化和经济的烙印，受到政治和国家的塑造与保护。[60]所以并不奇怪，包括美国、法国、德国、加拿大、日本、韩国、印度在内的40余个国家已经对网络信息加以普遍审查，[61]其关注对象涉及个人隐私、知识产权、大众生产、电子商务以及色情、暴力、仇恨、危害国家安全等广泛事项。[62]就此而言，国家为网络信息流动的维系提供了必不可少的公共用品，在某种意义上，信息自由未来最大的威胁不是国家的反应过度，而是它根本没有反应。[63]

较诸抽象的价值之争，数据信息所有者、使用者、存储者在地理位置上的分离以及所引发的跨境流动、主体识别和权力行使是国家主权所

面临的具体困难。[64]一方面，鉴于网络空间依托于但不局限于领土的特质，国家难以判断在网络空间中传输的信息是否已跨越了国境。另一方面，网络信息的即时性和巨量性也让国家不可能完成监控有害信息进入和自身信息泄露的任务。无论是网络空间主权的反对者还是赞成者都同时观察到了这一现象，却又做出了迥异的推论：前者认为这恰恰说明了主权在网络空间的不适用性，后者则主张通过服务器的本地化，努力恢复国家对信息的掌控力。[65]实际上，一旦我们抛弃主权绝对的观念，就能看到另一番场景：网络空间中的主权并没有衰落，改变的是国家对主权不同向度的认识以及为获得国家利益而在这些向度间的权衡利弊。[66]质言之，跨境信息控制——这一“互赖主权”（interdependence sovereignty）的适当弱化，推动了网络经济和网络政务的发展，这反过来增强了“国内主权”（domestic sovereignty）；而当网络信息严重危及国家安全时，国家又通过国家合作与国际体制，令他国不得干涉的“威斯特伐利亚主权”（Westphalian Sovereignty）越过有形疆域，扩张到国家专属域名及其域内、核心网络系统等无形疆域。[67]

总之，网络空间因互通性和虚拟性而给人异于现实的“异域”感，但比特世界之下的电子设施——铜线、光纤、路由器、交换机、服务器——都真实地存在于物理世界中和特定主权国家的领土之上。因此，网络空间并非“风能进、雨能进、国家主权不能进”的“法外飞地”，而是扎根于大地、作用于现实的“第二人生”，真实世界一切可能的“恶”都以变形的方式映射其中，甚至凭借匿名性和跨地域的特征而膨胀。因而，关键并不在于主权国家能否在网络空间中现身，而在于其以何种方式行使其权力。[68]

三 基于网络空间主权的互联网治理模式

作为对“网络空间自身主权”的替代，多利益攸关方治理模式摆脱了网络自治的乌托邦，却又陷入了一切利益攸关方平等的幻象。面对多利益攸关方治理模式在正当性、有效性以及理论上的缺失，一种新的制度架构亟待出现，这就是基于网络空间主权的互联网治理模式。

（一）多利益攸关方治理模式及其困境

2005年，联合国在突尼斯举行的信息社会世界峰会上通过《突尼斯

议程》（Tunis Agenda），该议程首次提出了网络治理中的多利益攸关方主义（Multistakeholderim），意即政府、私营部门和民间团体通过发挥各自的作用秉承统一的原则、规范、规则、决策程序和计划，为互联网确定演进和使用形式。[69]2013年，国际互联网管治论坛（Internet Governance Forum）协调执行人Markus Kummer把多利益攸关方治理模式描述为“一种让所有利益攸关方在平等地位上，经由开放性、包容性和透明性的程序参与到政策对话之中的手段”。[70]与之类似，美国国家电信和信息管理局（National Telecommunications and Information Administration）部长Lawrence Strickling指出：多利益攸关方程序包括了所有利益攸关方的全面介入、基于同意的决策制定以及开放、透明和有责的方式。[71]基于此，多利益攸关方治理模式包含了若干要素：其一，该模式并不预设任何“中心权威”或“单一的领导者”；其二，该模式采取了包容性和平等性的原则，赋予了各参与方相应的权利、义务和责任；其三，该模式坚持去中心化的、由下至上（bottom-up）的进路，这要求所有的决策都应来自受其影响的团体的合作和同意。[72]

多利益攸关方治理模式看似为平衡各方利益的完美方案，实际上却窒碍难行。在此，我们可以从“正当性”（legitimacy）和“有效性”（effectiveness）两个维度予以分析。根据韦伯的阐释，“正当性”即“相信有权统治的信念”。[73]在自由主义的影响下，现代权力的正当性普遍诉诸个体自愿基础上的社会契约。就此而言，多利益攸关方治理模式从“参与式民主”（participatory democracy）中获得认同，主张人们自发自愿地亲自参与决定，强调以自我管理的方式实现公共目标和社会利益。由于统治者与被统治者的身份彼此重合，多利益攸关方治理模式意味着另一种形式的“自治”，正当性自然得以确立。不过，实践永远和理念存在着鸿沟。[74]首先，利益攸关方的外延是不精确的，正如学者所批评的，没人说得清他们是什么或者拥有什么权利，这种模糊性使得在决定由“谁”来代表不同社会部门时，代表权会被操纵或滥用；[75]其次，积极参与的利益攸关方多为专业化的技术团体和商业组织，网络空间的一般消费者和使用者普遍缺席了；再次，作为后加入者，广大的非西方主体对于现行秩序并没有表达同意与否的真正机会；最后，非政府组织和特定国家的密切联系削弱了自身的公正性，引发了其他国家的不满和疑虑。例如，互联网名称与数字地址分配机构与美国商务部的协议关系，使得其受制于美国国家电信和信息管理局，这背离了其声称的多利益攸关方治理原则。除了上述正当性的缺失，多利

益攸关方治理模式还饱受实施“有效性”的质疑。其一，它缺乏具体的行为指引，以至于有人批评说它只是主张了“包容性”，但对于包容的方式和限制未做考虑。事实上，迄今亦没有任何正式规则来保证其顺利运行。[76]其二，该模式试图回避或无视有关实质权利和权力的归属以及相关制度设计议题，落入了头脑简单的社群主义陷阱。其三，由下至上的决策方式固然摆脱了行政干预和官僚机构，但私人同样可能以更隐蔽的形式对网络施加控制，并可能带来不公平歧视、隐私保护不力以及资源分配不公的恶果。[77]其四，这一模式将权力分散给各方，可又缺乏事后的追责机制，最终陷入无人负责的尴尬局面。

（二）全球公域及其误用

多利益攸关方治理模式的困境不仅源自其正当性和有效性的不足，还在于作为其理据的全球公域与网络空间的凿枘不投。

全球公域即“不为任何一个国家所支配而所有国家的安全与繁荣所依赖的资源或领域”。[78]回顾历史，早在古希腊罗马时代，理性主宰的斯多葛主义哲学和万民法传统就使人们认识到“人类共有物”的存在，随着资本主义原始积累的海外扩张，海洋归属问题引发了艾尔弗雷德·赛耶·马汉（Alfred Thayer Mahan）等人对全球公域的初步思考。[79]20世纪下半叶，由英国经济学家哈丁所创立的“公地”（commons）理论逐渐被推广到全球政策领域，制度经济学由此成为法律上“共有物”之外的另一条进路。到了当代，理论研究的深化、国际依存度的提升和全球性问题的凸显，使得全球公域的规则设计日益受到重视。近年来，国际法已经先后确认四种全球公域，分别是公海、大气、南极洲和外层空间。[80]作为一个复杂系统，全球公域具有如下特征：[81]首先，它处在单一国家管辖之外，从而不为任一实体所拥有或控制；其次，它是所有国家都能进入的领域；再次，对于进入者而言，它具有重要的政治、经济、科学、文化或军事价值；最后，它的整体功用大于作为部分的功用。全球公域的提出超越以主权国家为基本单元的传统国际关系思维，体现了国际共同体的共同关切，蕴含了“公天下”的价值理性。但毋庸讳言，由于国家实力和话语权的失衡，某些国家能够凭借“巧霸权”，将自身私利转变成世界公利，将国内规则转变为国际规则，甚至将他国主权范围内的“私域”转变成“公域”，[82]最终导致全球公域的异化，网络空间便是一个最好的例证。

2005年，美国在其《国土安全和民事支援战略》中将网络空间归入全球公域，[83]并在《2010年四年防卫评估报告》中，进一步将网络空间明确为“信息环境中的全球领域”，从而成为美国安全的重要支柱之一。诚然，网络空间无所不在的普遍性和开放性给人带来一种“公域”的错觉，其实却不然。首先，网络空间不符合“超出各国管辖范围之外的地球自然资产”这一联合国关于全球公域的界定。这首先因为网络空间非自然造化，而系人力所为，从而不属于由全人类共同所有和共同利用的“共同财产”（common property）或共同遗产（common heritage or international patrimony）。[84]恰如美国信息技术与创新委员会前主席威廉·J.米切尔（William J. Mitchell）所言，网络空间由无数分布广泛的企业与管理机构共同创建，它们有着各自不同的权利和利害关系，并通过多种途径获利。[85]根据学者的统计，高达90%的全球网络空间都是私人拥有。[86]权利的既存性和主体的多元性使得互联网难以成为“共同之地”，而更类似于公私混合的“俱乐部产品”（club goods）。[87]由此，我们可以将网络空间理解为一系列网络化的“俱乐部”，它们在不同层次上有着差异化的开放性和规则。

其次，网络空间实际被网络中心国家所掌控。作为整个网络空间的底层框架，根服务器（root server）、根区文件（rootzone file）和根区文件系统（rootzone file system）构成了维系其正常运转的关键资源（critical internet resources）。其中，全球总计13 台根服务器中有10台位于美国本土，并实际处于美国的控制之下。[88]而就网络数据信息而言，美国也一直具备并在持续完善着对其实施有效监控的能力。美国国家安全局前员工斯诺登披露的“棱镜”项目显示：美国不仅可以记录通信人、时间、IP地址、通信时间长度等数据，还能实时监控特定对象在网络空间进行语音、视频通信内容。[89]在某一国家拥有压倒性优势的情形下，网络空间在事实上已经沦为其“私域”。

再次，全球公域的提出旨在防范因权属不明造成的过度开发，相关制度设计以化解“公地悲剧”为目的，而这与鼓励网络空间投资，从而发展化解风险的网络空间治理思路存在抵牾。因为理论上，网络空间可以通过新的网络建设引入更多的使用者，而不会导致其“租值耗散”。考虑到降低网络空间价值的主要是网络攻击和垃圾邮件等不良使用行为，困扰网络空间的并非“开发过度”，而是“反公地悲剧”（the tragedy of anti-commons）造成的“开发不足”。[90]质言之，由于网络主体复杂，任何人都在一定范围内排斥他人，但无法在更大空间内有

效行使权利，从而造成主体权利、义务、责任以及网络治理的碎片化，结果损及了网络空间的安全和创新。

最后，网络空间的虚拟主体同样是特定国家内的现实主体，他们的行动受制于且反作用于现实世界。在某种意义上，形色各异的网络空间只是线下商店、图书馆、公共广场的线上变形而已，它们所适用的法律规则并无二致。[91]故此，无论是依据国家管辖权的“领土原则”（the territoriality principle），还是效果原则（the effects principle），网络空间始终在国家主权所及的范围之内。

（三）以网络空间主权为基础的治理模式

面对多利益攸关方治理模式和网络空间全球公域说的缺陷，国际上出现改革的呼声。2011年，中国、俄罗斯等上合组织成员国向联合国提交《信息安全国际行为准则》，重申与互联网有关的公共政策问题的决策权是各国的主权。2012年12月，在国际电信世界大会（WCIT-12）上，发展中国家进一步祭起“网络主权”的大旗，要求重新塑造网络空间治理模式。在这一改进版的利益攸关方治理模式中，主权国家成为最重要的治理主体，政府、私营部门和民间团体之间理论上的平等被打破。然而，这一主张遭到美国和英国的强烈反对。正如有人所言：“迪拜过后，似乎只剩下两极的世界——大部分发展中国家（除印度外）已经选择了网络主权者的阵营。WCIT-12实际上变成了西方对抗其余所有国家的战场。”[92]以此观之，国家主权在网络空间的回归，首先源自网络霸权对网络空间的戕害。

网络霸权是地理霸权在网络空间的投射。依循传统国际政治中“中心—半边陲—边陲”的三分法，世界各国根据拥有资源和决策权力的多寡，可区分为网络中心国家、网络化国家和网络边缘国家。[93]以美国为代表的网络中心国家通过技术上的互联网管理权、网络规则的制定权和话语权以及军事上的制网权，获取了左右网络空间的强大力量。[94]相反，众多发展中国家不但在网络域名、根服务器、信息通信主干线方面受制于人，它们自身的经济、文化和安全亦面临着网络挑战。[95]详言之，在一个大部分由信息化交易和信息化产品构成的现代经济中，国家的税收管辖权和司法管辖权受到了极大侵蚀。同时，网络空间以“英语”为主要信息载体，这种单向的信息流动使得英语所附丽的观念、思维和意识形态主导着网络世界。最后，由于网络安全防护能力薄弱，发展中国家无法有效化解信息战、信息犯罪、非法访问等引发的风险。不

唯如是，在过去数年，网络中心国家和网络边缘国家的数字鸿沟非但没有弥合，还有逐步扩大的趋势。世界经济论坛发布的《2014年全球信息及技术报告》发现：大多数领先国家的“网络就绪指数”的排名均维持不变或上升，而中国、巴西、印度等很多新兴大国的排名则有所下降，从而展现出强者愈强的世界网络格局。[96]在此意义上，网络空间再主权化的实质系诉诸《联合国宪章》中的“主权平等原则”，主张不论一国的网络能力如何，其均享有和其他国家同等的权利，有权在其领域之上管理与维护网络空间。[97]

网络空间主权不仅通过平等原则落实了多利益攸关方治理模式的多方参与意旨，而且以更可行的方式化解了其正当性和有效性的痼疾。建立在“人民主权”之上的现代国家，秉持着“间接民主”的制度安排，即人民通过由自己的同意所选举出来的代表来负责制定法律和管理公共事务，而不是直接进行统治。约翰·穆勒对之进行了有力的辩护：“人民应该是主人，但他们必须聘用比他们更能干的仆人”。[98]在网络空间中，国家的立法、行政和司法机构既是网络治理的权力主体，又能通过代议制吸纳、代表网络使用者和消费者等普罗大众的利益，再以公开透明的立法、行政和司法程序赢得多利益攸关方的认可，最终获得了实质和形式上的正当性。[99]另一方面，因权威性的不足，组织上的分散性以及资金、技术的依赖性，民间团体无法实现共同的网络治理愿景，加之搭便车、责任回避和机会主义诱惑，私营部门彼此协作和通力合作困难重重，治理措施或者隔靴搔痒或者流于具文。[100]更重要的是，越来越多的网络私人纠纷向“私人—国家”争议和“国家—国家”争议演化，这集中凸显了多利益攸关方治理模式的有效性欠缺和主权国家的意义。最后，作为基本权利和法律秩序的维护者，国家通过界定市场结构与合作规则来降低网络主体的交往成本，通过公共产品供给的规模效应降低了执行成本，最终提升了网络治理的有效性。[101]凭借上述优势，“网络空间主权”的观念开始获得了国际认可。2015年7月，联合国在《从国际安全的角度来看信息和电信领域发展的政府专家组的报告》中将“国家主权原则”作为提升信息和电信安全的核心，该报告第27条进一步提出：国家主权和由国家主权衍生出来的国际准则与原则，适用于国家开展的信息通信技术相关活动，也适用于各国对本国领土上信息电信技术基础设施的司法管辖。[102]理论与实践的发展，为一种基于网络空间主权的新型全球治理模式锚定了目标。

四 网络空间主权的国内法建构

网络空间主权不仅属于政治范畴，更属于法律范畴。作为中国网络法的核心概念之一，如何从法律体系的观点探求其意蕴，厘清其外延，构造其制度，最终用网络空间主权建构法律制度，用法治框架落实网络空间主权，便是下文所要完成的任务。

（一）网络空间主权的法制化

1.从“政治性主权”到“法律性主权”

主权首先是一种先于法律的政治存在，一个政治范畴。[103]正如美国学者韦罗贝（Willoughby）所言：“国家的本质特征，即是它有别于其他人类组织而拥有的政治主权。政治主权意味着，一方面它有不受法律和其他权力控制的绝对自由；另一方面，对它的公民的法律权利与义务也加以绝对的控制。”[104]因此，如欲在实在法的体系内把握主权，我们就必须区分两种意义上的主权：“政治性主权”（political sovereign）与“法律性主权”（legal sovereign）。[105]该等主权两分法进一步丰富了内部主权和外部主权的二元论。详言之，就内部主权而言，政治性主权归属于国家中意志得到最终服从的君主或人民，法律性主权则归属于一个或数个国家组织；政治性主权因垄断了强制力而拥有要求他人服从的能力，它是一种事实（de facto）主权，而法律性主权则以法律权威为基础，它是一种规范（de jure）主权；政治性主权在根本上是制宪权，法律性主权主要指立法权、司法权与执法权；政治性主权者的命令只能通过选民或公共舆论来实现，法律性主权者的命令则由普通法院和行政机关强制执行。另一方面，就外部主权而言，政治性主权系由《威斯特伐利亚和约》产生的不干涉他国内政的“威斯特伐利亚主权”，法律性主权则指国家在国际体系中的合法地位，其表现为被国际社会承认的自主签订国际条约、参加国际组织、享有国际法权利及承担相应义务的“国际法理主权”（international legal sovereignty）；政治性主权立足于国家的拟人论（anthropomorphism of nations），倾向于国家主权的抽象性和绝对性，法律性主权则试图在国际体制内认识主权，因而主权是具体的、弹性的，在某种意义上，它由包括国际法在内的国际规范所建构和塑造。[106]

政治性主权和法律性主权的两分法契合了主权的双重性：既是抽象的，又是具体的；既是统一的，又是可分的；既是绝对的，又是相对的。[107]因此，政治性主权向法律性主权的转向，也就是抽象、统一和

绝对的“权威”（纵向）和“资格”（横向）向具体、可分和相对的“权力”（纵向）和“权利”（横向）转向，一言以蔽之，即从“主权”向“主权性权力/权利”转向。[108]事实上，早在博丹那里，两者的分离就已经出现。在《共和六书》中，他将“制定法律、媾和和宣战、设立国家的首要官员、终审权、定税和免税、赦免该受死刑惩罚之人、宣誓效忠、铸币和度量衡等”称为“主权特征的权力”。[109]当代的国际法律文件延续了这一思路，1979年的《月球协定》、1982年的《联合国海洋法公约》都运用了“主张或行使主权或主权权利（权力）”的字样以示区别。[110]由此，我们得以摆脱政治性主权的宏大叙事，而聚焦于规范性和灵活性兼备的主权性权力/权利之上。

2. 网络空间中的主权性权力/权利

主权性权力/权利纷繁多样，尽管在广义上可以把网络空间有关的所有主权性权力/权利统称为“网络空间主权”，但这种只是将网络空间作为主权自然延伸的做法，显然难以逃避类似于美国法学家弗拉克·伊斯特布鲁克（Frank H. Easterbrook）的批评：既然网络空间主权就是与之相关主权的集合的话，那它就与“马主权”（即针对马这一物种形成的主权）在本质上并无差异，并无必要建构一个独立法律概念和制度。[111]因此，只有立足于网络空间的特殊机理，并以此透视主权性权力/权利，作为法律概念的网络空间主权才可能获得真正独立的地位。而这一“特殊机理”的落脚点，便是“空间”。主权与空间密不可分。在传统的主权概念里，主权即对特定领陆和领空的绝对控制，这里的空间表现为稀缺（scarcity）、有限（finiteness）和自然（nature）的特质。[112]与之不同，网络空间系为人所造就的异托邦，它所拥有的不同于地理空间的特质对网络空间中的主权性权力/权利产生了微妙但重要的影响。

如前所述，网络空间以互联为特色。由互联网奠基人之一保罗·巴兰所提出的多个节点彼此连接的“分布式拓扑结构”，不但解决了依赖于中央组织的信息传输模式，还使得互联网能够像生物一样进化。网络空间演变的历史已经表明：它完全是由按需求的、本地化的、分散式的决策所决定。任何人在无需中央机构允许的情况下，都能为网络添加节点和纽带，从而使得网络空间从单一网络发展到多个独立和互联的网络共存。[113]据此，网络空间呈现出一个扁平化和多中心的场景。在这样的空间结构中，“由上至下”的“内部主权性权力”亦应适时而变，将

更多的权力交由不同类型的网络主体、公众及非政府组织分享，以期通过水平分权和协同治理达成国家目的。[114]就此而言，网络空间的主权性权力与其说是空间中的最高权力，毋宁说是时间中的“最先权力”和“最终权力”。前者意味着主权性权力应当退回到决策权的分配和界定上，即从决策的内容或结果中适度抽离，而集中在由谁、按照何种程序来做出决策的问题，换言之，其关注的是“关于决策的决策”。[115]后者意味着主权性权力的补充性和辅助性，只有其他主体无法独立实现关键目标之时，其才以适切方式介入。[116]

另一方面，网络空间还是一个“互动空间”。这里的“互动”首先指涉的是全球范围内网络主体之间的沟通与对话，其次表征了现实空间和虚拟空间、网络设施和网络信息之间的交错与转化。凭借信息通信技术的空间互动（spatial interaction），主权不但在一国领土之内加以落实，而且跨越领土边界在“非领土或由网络行为连接的零散区域中”得以施展。[117]显然，这大大拓展了内部主权性权力的范围，使得国家的管辖呈现无所不在的“普遍性”。但同时可以预见的是，这同时增大了与其他国家主权的横向摩擦。2000年的雅虎纳粹物品拍卖案便是绝佳的例证。[118]为此，外部主权性权利更加强化平等性的面向，经由国家之间的公平互动，建构和遵守国际准则，实现合作共赢。而这正印证了美国学者罗伯特·基欧汉和小约瑟夫·奈关于“信息革命极大地扩展了社会联系渠道，使国际体系更接近于复合相互依赖”的论断。[119]作为新型外部主权具体而微的反映，网络空间中的主权性权利固然包括传统上基于领土的“单边权利”，可更重要的却是与他国合作治理网络空间的“共治权利”。[120]

3. 网络空间主权的法律界定

主权概念需要法律化，为增进法律的操作性和明晰性，类似地，网络空间可以进一步简化为“网络设施、网络主体和网络行为”三要素。[121]这里的“网络设施”包括任何支持数字化生成和传输的技术工具，既指信息电缆、光纤、发射塔、卫星等基础设施，也包括了计算机、智能手机、服务器等日新月异的终端设施。网络主体包括了利用网络访问系统开展生产生活活动的网络用户、网络服务提供者、网络基础设施运营商和网络主管机构。网络行为则是网络主体利用网络设施在网络空间之内进行的活动。

综合主权的二元论以及网络空间要素的提炼，本章将法律框架下的网络空间主权定义为：（1）国家按其意志在领域内对网络设施、网络主体和网络行为所拥有的“最先权力”、“最终权力”、“普遍权力”；（2）国家向其他国家主张的、对网络设施、网络主体、网络行为享有的“单边权利”和“共治权利”以及相应的合作义务。从此出发，我们将首先从内部主权的层面建构网络空间主权国内法体系，然后在本章的第五部分尝试从外部主权的层面提出网络空间主权国际法体系。

（二）网络空间主权的国内法体系

1. 网络空间最先权力：网络基本法制定权

立法权是主权者的首要特权（the first prerogative），在网络空间亦是如此。不过，鉴于网络空间的互联性，其立法权的行使应以“分配网络空间规制权”为要务，以基本法的形式确立网络空间治理的权力架构和顶层设计。恰如美国法学家黑格所言：治理与其说是单一、连贯的单位，毋宁说是芜杂的团体和人们在不同领域开展支配行动的集合。[122]网络空间的治理须尽量包容不同层级的政府机构、私营部门和社会公众，同样，网络空间基本法也应在分权的基础上共治，在赋权的基础上追责，以此发挥国家管理、市场自律、社会监督多种途径的协同作用。对此，我们可以从程序和实体两个面向做进一步展开。

一方面，受限于人民主权原则，国家要促成受其立法权影响的个体或组织在审慎论辩基础上做出决定，通过将边缘化的非国家主体引入网络空间基本法制定过程之中，使网络空间主权的正当性得以增强。[123]质言之，国家不但为各种网络主体提供参与渠道，搭建公共推理与公私合作的制度平台，并且，考虑到尚未“触网”或无法发声的弱势群体在经济资源、政治机会和信息获取上的欠缺，国家还应进行倾斜性的“赋权”（empowerment），以实现真正意义上的审议和决定。另一方面，受限于网络空间的权力分散特性，国家不再是网络空间中的“中心行动者”，而应从平等参与及协同共治的理念出发，区分网络设施和网络信息，融汇政府主导、政府指导下行业和企业自律以及行业和企业主导不同模式的比较优势，推动网络空间治理从“碎片化”走向综合。[124]其中，在政府层面上，应有常设的网络主管部门专司其职，作为行政管理和执法机构，而非单纯协调机构。借此，国家不但能够消除多部门立法、政出多门的弊端，[125]而且有利于打破“谁主管谁负责”的固有思

维，避免将整体性和互联性的网络空间进行条块割裂。[126]在行业层面，虽然中国互联网协会也已在全国普遍成立，但在某种程度上独立性欠缺，无从发挥凝聚行业共识、树立行业准则、践行奖惩机制的作用。故而，国家应培育和发展多层次和多功能的网络自律组织，积极维护行业秩序和用户权益。在企业层面，网络服务提供者掌握着用户信息，创设了信息交互平台，提供了传递公众利益和意见的通道，国家应将其视为政治过程的参与者，在广泛授权的基础上严格限权，以达到行业利益、个人利益和国家利益的平衡。[127]不仅如此，由于网络信道的自然垄断性质，寥寥可数的网络运营商实际上已经成为去中心化网络中的“半中心”，它们自然承担着促进产业发展和经济创新的重任。[128]最后，在网络用户层面，其不仅要明了网络环境等同于现实生活，须为自己在网络空间中的行为负责，还有权采用建议、检举、申诉、控告等方式进行网络空间治理。对此，中国应借鉴英国“监督而非监控”的理念，建立受理、调查、处理、反馈、保障、不当举报制约等一系列监督辅助制度，最大限度地实现网络空间的“自我规制”。[129]

2. 网络空间最终权力：简约行政管理权

应对网络空间复杂性的有效手段就是国家的“简约管理”，[130]意即网络管理机构仅仅在尊重网络空间内在规律以及其他网络主体自主决定的前提下方能进行适度的介入，并且，其合理性应止于促进网络空间自我修复和自我完善必要性的范围之内。我们可以从如下方面进一步理解该等权力。

其一，在规则适用上，简约管理意味着国家优先依循由非政府网络主体共同制定或认可的并依靠成员以自律方式实施的“软法”，而非国家法。[131]这里的“软法”不但指由网络服务提供者为规范网络行为发布的一系列行为规则（如《淘宝规则》、《新浪微博社区公约》），也包括相关行业组织发布的行为规则指南、网络言论和行为标准以及自治性规范（如《中国互联网协会抵制网络谣言倡议书》、《互联网终端软件服务行业自律公约》）。其二，在执行手段上，简约管理要求以“非强制性措施”为主，以“强制性措施”为辅。后者即命令与服从关系中的许可、决定或处罚，前者意谓平等或对等关系中的登记、指导、协商以及各种非处罚性监管措施。[132]目前，中国对网站域名、IP地址以及非经营性网站已实行了登记备案制度，但对经营性网站则要求事前许可，若从事互联网新闻信息服务、网络视听、互联网文化经营和出版、

电子公告等特殊服务还需要相关部门的前置审批。[133]显然，芜杂的双重许可给网络服务提供者带来了不必要的合规成本以及广阔的寻租空间。其三，在行使对象上，简约管理体现为网络设施和网络信息的区隔，前者因有限性和固定性可采取传统的属地管理，后者则因流动性和复杂性而必须采取化繁为简的动态管理，否则，管理体制本身就可能因愈多的相互作用和随机性而解体。[134]据此，不管是网络信息的技术性控制（如IP地址或主干路由器阻断、域名过滤、软件监控、敏感词过滤）还是行政性控制（如人工删除、吊销许可），既需要有效且精确地瞄准目标，尽量适用规则而非原则界定被禁止内容的范围，也应保持制度的透明度，以公开方式执行，从而提高网络行为的可预期性。[135]

3. 网络空间普遍权力：类型化的司法管辖权

对人、事、物的司法管辖是主权性权力的基础。在网络设施相容相连、网络主体遍布世界、网络信息跨境流动的背景下，网络空间的管辖范围自然成为最核心和最具争议的问题之一。[136]对此，本章拟采取类型化的方法，因对象而异地确定管辖权的范围。

（1）网络设施：领土原则

一个国家的领土是其主权赖以体现的最基本空间，也是一个国家人民得以休养生息繁衍的物质基础，领土原则自然成为划定管辖权的首要原则。[137]如同其他物理存在，特定领陆、内河、领海和领空中存在的网络设施，无论由国家、组织还是个人所有，都应依循领土原则处于国家管辖之下。[138]不过，由于网络设施，特别是终端设备的可移动性，在使用中可能出现跨境移动，此时网络用户执行操作时所在的任何国家都具有管辖权。此外，根据领土原则衍生的“旗国主义”，位于国际空域、公海或外空的飞机、船舶或其他平台上的网络基础设施亦受船旗国或注册国管辖。需要说明的是，尽管船旗国或注册国对国外网络平台上的人或物具有管辖权，这些人或物也可能同时属于其他国家的管辖范围。例如，一个收发器所属的公司在甲国注册，它为该公司所使用，但该收发器却安装在注册为乙国的卫星上。那么甲、乙两国同时拥有对它的管辖权。[139]就此而言，管辖权是基本的，但非排他的主权性权力。

（2）网络主体：国籍原则

公民身份是权利和义务的统一，在某种意义上，该身份意味着自然人或组织对国家规制自身行为的授权。据此，无论一国的网络主体在境内还是境外，其利益、关系、资格和行为都将受所属国家的管辖。[140]由于网络空间的虚拟性，网络主体的地理位置往往难以判断，但其国籍通过信息技术和线下配合却容易获得，并由此成为确定管辖权的重要方式。[141]在美国United States v. Galaxy案中，被告Jay Cohen是一家在线赌博组织（WSE）的负责人，被诉通过网站接受美国公民的赌注。面对被告依据WSE设在安提瓜岛这一事实提出的管辖异议申请，法庭认为基于Jay Cohen的美国国籍，驳回其请求。[142]

（3）网络行为：效果原则

网络空间的交互式和参与式信息通信压缩了时间和空间，前者意味着网络信息传播的及时性取代迟滞性，后者意味着主权的封闭性让位于主权事实上的开放性。[143]借用量子力学的宏观表达，构成网络行为对象的电子可以在不同地方同时出现，廉价的存储器、便捷的访问和全球性的覆盖使得主权国家难以掌控网络信息的流动。因此，对网络行为的管辖便不得不舍弃固定化，而采用更灵活的方式，这就是“效果原则”。根据该原则，无论网络行为是否在一国领土之内，只要它在领土之内产生或意图产生不利影响，均在该国的管辖范围内。[144]为避免管辖权的过分扩张，这里的“影响”应做狭义理解，即仅限于“直接、可预见和实质性”的影响。尽管如此，由于网络空间的互动性，效果原则不可避免地对他国主权造成妨碍，为此，管辖权的行使至少应不违反相关国家的法律、不损及相关国家的国家利益。

五 基于网络空间主权的国际合作

在本章的最后部分，我们将从内部主权转向外部主权，从一国之内的立法权、行政权和司法管辖权转向国与国之间的权利主张。主权独立、平等、合作的国际法原则，和习近平主席关于“网络空间命运共同体”的倡导高度一致，丰富和塑造了网络空间主权的外部维度：网络安全、平等参与、共同利用、善意合作，奠定了国际合作的基础，并为未来的国际法准则和公约指明了方向。

（一）主权独立：网络空间单边权利

网络空间单边权利是主权独立及其所衍生的领土完整原则在网络空间的应用，其仅在消极意义上申明边界范围内网络主体、网络设施、网络信息权益的不可侵犯性。[145]而对于因域外网络主体、网络设施、网络行为所引发的政治、经济、社会、文化风险和争端，则必须依循网络空间共治的逻辑，由各方共同协商化解。在一系列单边权利束中，[146]网络安全权居于中心地位。这有着正反两方面原因。从正面观之，在发生学上，主权的出现使得国家成为国际安全的主要指涉对象，换言之，主权的意义在于透过国家互动形成安全复合体，[147]“安全”由此成为主权议题的关键所在；在实践中，恰如其他面临网络霸权威胁的网络边缘国家一样，中国网络空间的脆弱性和安全亦是主权性权利的首要关切。[148]从反面观之，网络空间独立权、防卫权等其他对网络空间主权

的表达或缺乏逻辑性，或缺乏后果考量。详言之，有论者将“独立权”界定为“本国网络可以独立运行，无需受制于别国”，[149]但该理解不但与“按照自己意志处理本国事务，而不受他国干涉”的国际法概念不符，[150]更违背了网络空间互联互通的基本架构，其实质是混淆了国家主权和国家能力。类似地，“防卫权”被视为“国家对外来网络攻击和威胁进行防卫的权利”，显然，这是自卫权——“在遭受外来武装攻击时采取相应武力措施进行反击的权利”——的网络空间翻版。[151]然而，这一对“武力制网”和“防卫权”的扩大解释可能正中网络霸权国家的下怀，帮助其实现通过单边军事手段来应对网络攻击的战略意图。[152]实际上，中国在2011年提出的《信息安全国际行为准则》中便已明确反对单边的防卫权，主张任何网络争端都应以和平方式解决，从而共同构建和谐的网络空间国际秩序。[153]总之，网络安全权反映了主权的政治意旨，同时具有包容性和广泛性，足以成为网络空间主权性权利中的重要组成。

所谓网络安全权，即一国所享有的、排除他国对其网络空间恶意侵入和攻击，维护网络信息保密性、完整性和可用性的权利，[154]其包含了对行为主体和行为类型的限定。一方面，它是国家间（inter-national）的权利，因而只能由一国向其他国家而非个人或私营部门主张。但是，由于网络的匿名性，将特定网络行为和特定主体联系起来的“归属”（attribution）认定成为最困难的问题。[155]目前，通过捕获他人电脑来展开其所有者并不知情的行动已习以为常，况且即使能把某种行为追溯到某一地点，要证明国家担当了主使者或包庇者的正式角色仍难上加难。对此，我们尝试援引国际法的“禁止损害”规则（No-harm Rule）加以解决。根据该规则，一国境内或一国管辖、控制下的活动不得对他国造成损害。[156]在1949年的“科孚海峡案”（Corfu Channel Case）中，国际法院明确指出：“每一个国家都有义务不得在明知的情况下允许其领土被用于损害他国权利的行为。”[157]这里的“明知”一般被理解为“对于某一活动可能导致的跨界损害已经或应当预见或知晓”。[158]正因如此，以“明知”为基础的禁止赔偿规则减轻了网络空间中国家对“归属”的证明负担。质言之，一旦国家能够证明危害网络安全的行为来自他国境内，且就该事实对他国发出正式通报，则该国就负有采取必要行动的义务，否则便构成对网络安全权的侵犯。另一方面，“网络安全权”指向的是任何损及网络设施和网络信息的网络行为。前者主要包括对传输光缆、服务器、路由器、工作站等物理设备的破坏，其中尤以有关公共通信、广播及电视传

输网络，重要行业网络，电、水、气、医疗卫生和社会保障网络，军事网络，政务网络，公众网络等关键信息基础设施的设备为重。后者主要指采取网络病毒、僵尸网络、拒绝服务攻击、高持续威胁攻击等手段对网络信息的窃取、拦截、修改和删除。[159]

（二）主权平等与主权合作：网络空间共治权利

1. 网络空间命运共同体：网络空间共治权利的理论基础

习近平主席在第二届世界互联网大会上旗帜鲜明地声明：网络空间是人类共同的活动空间，网络空间前途命运应由世界各国共同掌握，每一个国家都是网络空间命运共同体的一员。网络空间命运共同体的提出含义深远、意义重大，足以成为网络空间共治权利的理论基础。

首先，“共同体”一词反映了网络空间互联互通互动的特质。众所周知，网络空间依托于一个全球性的万维网，每个国家的网络空间都必然是全球性网络空间的组成部分。毫不奇怪，当一国针对其所拥有的网络空间行使主权性权利时，它必然面对他国的主权和利益，一系列的冲突与合作由此产生：我们可以在网络设施中根服务器的全球分布上以及域名设置、互联网技术规范的全球统一上发现它们，更能在网络信息的全球流动上感受到它们。事实上，网络空间的一体化是如此彻底，以至于离开了各国的共同参与，任何一国都不可能完成与网络空间重大议题相关的主权任务，包括但不限于：（1）关键性互联网资源（critical internet resources）的控制；（2）协议号、网页、通信等互联网标准的设定；（3）进入网络和互联的协调；（4）网络安全治理；（5）与隐私、数据、言论有关的信息媒介（information intermediation）规制；（6）基于网络架构的知识产权执行。[160]

其次，“命运”一词源自网络空间当前面临的重大挑战。根据对网络空间威胁程度的高低，这些挑战包括：（1）黑客攻击，即黑客破解或破坏某个程序、系统及网络安全。以2014年为例，就发生了OpenSSL的“心脏出血”（Heartbleed）式漏洞、Linux的Bash破壳、恶意软件Havex以及伊朗黑客“剁肉刀”（Cleaver）行动等重大安全事件，金融领域、能源行业屡受重创，关键基础设施面临严峻威胁。[161]（2）有组织的网络犯罪，不但指洗钱、贩毒、贩卖人口、走私等传统犯罪活动的虚拟化，而且涵盖了数据窃取、网络钓鱼等互联网所特有的犯罪行为。近年来，有组织犯罪转战互联网的数量激增，其高科技、隐蔽性和

跨国性给国家、公民和企业安全带来了前所未有的损害。据专家估计，仅在2010年，美国因网络犯罪造成的损失就高达1万亿美元。[162]（3）网络恐怖主义，系针对信息及计算机系统、程序和数据发起袭击，以动摇政府权威、制造民众恐慌，也包括恐怖组织借助网络空间进行的宣传、动员、招募、寻求资助等辅助性活动。[163]（4）网络间谍，意指利用互联网从特定目标或敌情信息库中监听、搜集和分析信息，如美国的棱镜计划。（5）网络战，即一国对敌国的网络空间进行的以干扰或破坏军事信息系统、武器装备和关键基础设施为目的武力攻击。[164]2008年格鲁吉亚遭受的网络打击和2010年伊朗“震网”蠕虫病毒均被视为网络战的典型案例。在层出不穷的全球性挑战面前，没有哪个国家能够置身事外、独善其身，维护网络空间秩序由此成为国际社会的共同责任。

最后，网络空间命运共同体贯彻了主权平等与合作原则，是对全球公域理论的扬弃和发展。虽然如前所述，全球公域与网络空间不可同日而语，但它充分证明了各国参与对解决争端的重要作用。不过，共同参与只赋予了国家影响最终决策的机会，特定国家并不必然是决策负责主体。[165]针对这一不足，网络空间命运共同体赋予了每一个国家以平等身份共同治理国际网络空间的权利，为多边、民主、透明的全球互联网治理体系的建立和维护奠定了基础。放宽视野看，网络空间命运共同体与国际环境法中“人类共同关切事项”（Common Concern of Humankind）的精神有着异曲同工之妙。[166]作为一个产生于1992年《联合国气候变化框架公约》和《生物多样性公约》的晚近概念，“人类共同关切事项”调整了以往属于个别国家主权管辖范围内但国际社会对其具有共同利益的活动或资源。基于对各国主权的尊重和对共同治理价值指引间的平衡，网络空间命运共同体的提出与“人类共同关切事项”具有同等重要性，足以成为网络空间主权国际法的根本理念。

2. 网络空间共治的既有努力与不足

国际社会很早就认识到网络空间共治的必要性。1998年，国际电信联盟全权代表大会提出了举办信息社会世界峰会的倡议。2002年，联合国大会第56/183号决议确立了峰会目标，同时决定分两个阶段召开。在2003年日内瓦会议和2005年突尼斯会议上，《原则宣言》、《行动计划》和《突尼斯议程》相继通过。2006年后，联合国根据上述成果，先后召开八次互联网治理论坛，逐渐形成了“应对网络安全、网络犯罪、

隐私和开放性问题，是所有利益攸关方的共同责任”的共识。[167]尽管如此，互联网治理论坛始终未能在具体问题上形成一致的、有效的解决方案，也未改变美国对互联网资源的垄断现状。[168]鉴于此，国际电信联盟试图对互联网治理机制进行彻底革新。在其举办的2012年国际电信世界大会（WCIT-12）上，各国以修改《国际电信规则》为契机展开交锋，由于对“成员国拥有接入国际电信业务的权力和国家对于信息内容的管理权”的严重分歧，最终规则无法完全生效。[169]而在2014年国际电信世界大会（PP-14）上，在美国的推动下，“网络安全和互联网治理事项不在国际电信联盟的强制事项内”的议案得以通过，国际电信联盟承担更积极角色的道路几乎被断绝。[170]另一方面，中国、俄罗斯、巴西、印度等发展中国家利用联合国平台发出的声音一直未获得重视。例如，2013年，金砖国家向联合国提出《加强国际合作，打击网络犯罪》的决议草案，美国、日本及部分欧洲国家在会场内外阻挠，致使会议进展相当有限。[171]再如，中国、俄罗斯等上合组织成员国两次提交的《信息安全国际行为准则》，也因美国的抵制而无果。当然，在相关国家的努力下，联合国还是通过了多份涉及网络恐怖主义的决议以及《从国际安全的角度来看信息和电信领域发展的政府专家组的报告》，但它们并不具有法律上的约束力。

较诸联合国框架下的正式多边机制，由主权国家发展的多边和双边关系在网络空间治理中发挥着更大作用。欧洲委员会于2001年牵头起草的《网络犯罪公约》作为迄今为止全球范围内针对网络犯罪达成的唯一多边公约，已获得39个国家的签署，被称为国际合作治理的里程碑。与此同时，欧盟还发起了国际磋商和对话的“伦敦进程”，成为第一个专门针对网络安全和网络空间治理的多边会议。2011年，在法国召开的G8峰会首次将“加强网络安全、保护个人信息和防止网络犯罪”列为核心议题，并启动相应的针对性措施。[172]中国亦在东南亚国家联盟、上海合作组织、金砖国家等国际组织框架内签署了《中国—东盟电信监管理事会关于网络安全问题的合作框架》（2009年）、《上合组织成员国保障国际信息安全政府间合作协定》（2009年）。[173]另一方面，中美、中俄、美俄之间已就网络安全事宜达成若干双边协定，[174]2015年9月中美两国就网络安全形成的共识尤其引人注目，同年12月通过的《打击网络犯罪及相关事项指导原则》便是落实上述共识中“中美打击网络犯罪及相关事项高级别联合对话”机制的重要成果。[175]

尽管非正式的多边和双边机制看似更有效率，但其不可避免地反映

了制定国的利益和偏好，[176]甚至存在利用优势地位强迫他国同意的情形，从而违反了主权平等原则。更重要的是，这一机制有悖于网络空间命运共同体的宗旨，无法容纳更多元的声音和诉求，对部分国家的排斥或无视，只能使网络空间的全球治理和共同规则有名无实，最终事倍功半。故此，中国一方面要坚持联合国作为最权威和最具代表性平台的地位，积极推动联合国框架下国际准则或公约的制定，另一方面也要正视当前联合国主导路径的挫折，利用世界互联网大会，倡导基于网络空间主权的共享共治理念，在复杂国际关系中“合纵连横”，寻找和促成各国在网络空间治理的利益共同点，早日成就符合大多数国家期待的国际法制度。

3. 网络空间共治的前景：网络共治权利的国际法准则

“一切有关合作的努力，都是在某种制度背景下发生的。”[177]网络空间主权的国际法不但影响着网络空间共治的方式，也决定了网络空间命运共同体能否形成。因此，如何为网络空间寻求共治权利的规范基础便成为克服集体行动悖论、化解意识形态分歧、建构网络空间秩序的当务之急。对此，美国学者多希望类推适用《联合国海洋法公约》、《国际民用航空公约》、《外层空间公约》等国际法规则，[178]但网络空间与全球公域的不兼容性令他们徒劳无功。故而，我们需要放开视野，从更基础和更广泛的国际法渊源中细化网络共治权利。

（1）平等参与

依托《联合国宪章》的主权平等原则，平等参与得以成为网络空间共治权利的出发点。这首先意指国家之间互不隶属，任何一国都不能通过胁迫等手段使他国接受或服从条约和国际规则。同时意味着国家之间互不歧视，每个国家，不论政治、经济和社会制度的任何差异，均有权进行网络空间合作，以维护网络空间安全、促进网络空间进步。此外，这还意味着网络空间相关国际会议上和国际组织中，各国应享有同等的代表权和投票权。[179]其次，网络空间共治权利对网络空间的价值原则上保持中立，并不预设特定选择。当前，中美两国对网络自由与网络秩序、网络开放与安全等议题持有不同立场，[180]这种实质性的价值之争只能通过公平决定程序才能求同存异、相互谅解。如果说国际法是持续地协调集体利益的法律结果，那么基于国际法的网络空间主权性权利亦应尽可能促成各国意志和利益的协调，以达致“交叠共识”。[181]

（2）共同利用

对网络空间的共同利用是各国平等参与的自然结果，也体现了习近平主席“共享共赢”思想。互联网的发展是全球的盛事，它引领了社会生产新变革，创造了人类生活新空间，拓展了国家治理新领域，极大提高了人类认识世界、改造世界的能力。“凡益之道，与时偕行”。所有国家都有权从网络空间的繁荣中受益。然而，在不同主体同时利用网络空间这一共享资源的场合中，冲突不可避免，亟待公平合理地确定各国权利的边界。实际上，国际法院已经在1969年“北海大陆架案”、1974年“渔业管辖权案”、1993年“格陵兰—扬马延海洋化划界案”等案件中运用公平原则化解共享资源争端。[182]国际法协会的《国际河流利用规则》和联合国的《国际水道非航行使用公约》亦针对国际河流——这一跨两个或两个以上国家的水资源——特别明确了公平合理利用原则。[183]尽管该原则因标准模糊而受到批评，但它毕竟在赋予各国利用权的同时，科以不剥夺他国利用权以及保护资源的义务，从而为各国间的持续利用建立了弹性框架。以此为参照，网络空间的公平合理利用首先要求任一国家不得在网络空间中从事或指挥、控制私人从事有损他国利用权的行为；其次，网络中心国家不得凭借自身在核心技术、信息通信技术产品和服务、信息通信网络等方面的优势，不公平分配国家顶级域名（ccTLD）、通用顶级域名（gTLD）等重要网络资源，不维护或破坏光纤电缆等关键性基础设施的稳定运行；最后，公平合理利用还要求相关国家对网络空间保护和发展的努力应当与其网络能力及可能造成的威胁或可能获得的利益成比例，从而实现权利义务平衡。总之，公平合理利用的原则表明了远未定型的网络空间国际法争议的基本态度，即遏制网络霸权、弥合网络中心国家和边缘国家的巨大鸿沟、促进实质平等。

（3）善意合作

各国善意合作是网络空间共治的落脚点，也是主权合作的题中之义。在国际法上，合作解决问题的一般义务，已得到了普遍接受和《联合国宪章》第1条第3款和1970年联合国大会《关于各国依联合国宪章建立友好关系及合作之国际法原则之宣言》的支持。此外，针对多国共享自然资源和跨境污染事件的合作义务，联合国在1973年《关于在由两国或多国共享自然资源的环境领域进行合作的决议》和1992年《里约宣言》中专门予以重申。

根据上述国际法原则并充分考量网络空间的特性，其一，这里的“善意合作义务”首先意味着“安全合作”。质言之，由于网络所面临的全球危机及其对国家的重要意义，网络空间已经成为全球安全和国家安全的交汇点。而各国网络空间的密切关联，又使它们必须整体考虑，不可分开，一种虚拟的“安全复合体”由此诞生。[184]在这一复合体中，尽管冲突、竞争与合作并存，但在共同问题的压力下，合作打击网络犯罪、网络恐怖，抵制网络间谍和网络战始终居于主导地位。其二，有效的合作依赖于信息，一国对关系自身利益且在他国控制下的网络信息有权主张共享。[185]其三，在一国的措施对他国网络空间造成不利影响或在其领土内发生的事件造成跨界损害时，应及时通知他国，以便后者做好评估、预防和应急工作。同时，在一国行为严重影响他国利益时，还应提前协商。其四，各国应致力于建立正式的磋商平台和机制，定期举办国际会议，逐步建立联合国及其安理会下的“以国家为主体、多利益攸关方参与、公私合作”的国际网络空间组织，[186]全面协调和管理网络空间事务。其五，作为网络空间全球治理的最终解决之道，各国应秉承坦诚和善意，尽可能促成网络空间国际准则和公约的订立，并采取一切必要措施保证相关准则或公约的严格执行，特别是建立网络空间的争端解决机制，以实现国际规则的长效约束力。[187]

六 结语

“尊重网络主权，维护和平安全，促进开放合作，构建良好秩序”是建立多边、民主、透明的全球互联网治理体系的四项基本原则。网络空间主权的首要位置充分说明了它在网络空间治理中的前提性作用：没有内部主权，国家就不能制定网络基本法、不能确立网络管理模式、不能管辖网络纠纷；没有外部主权，国家就不能保障网络设施、网络主体和网络信息的安全，不能在国际层面上平等参与、共同利用和进行有效合作。一言以蔽之，没有网络空间主权，就不可能有网络空间真正的自由、秩序、发展和繁荣。

网络空间主权并没有损及网络自由，因为网络自由主义者所称的信息自由从未诞生过。[188]网络空间主权亦没有损及法治。网络空间立法权、行政权和司法权贯穿了权力有限性和内容明确性的法治原则，而网络空间单边权利和共治权利不但契合了国际法，还为未来国际准则和公约的制定搭建了架构。这恰恰印证了英国人的历史经验：法治是主权的基本原则。[189]面对历久弥新的主权观念和日新月异的网络空间，包容

了自由、法治、民主的网络空间主权是中国给予世界的又一贡献。我们应不懈坚持之，努力践行之。“立志在坚不在锐，成功在久不在速。”我们深信，网络空间主权必将大行天下，最终铸成和平、安全、开放、合作的全球网络空间。

---

[1] 参见徐隽《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》，《人民日报》2015年12月17日第1版。

[2] 参见若英《什么是网络主权？》，《红旗文稿》2014年第13期；支振锋：《网络主权指引国际治理新格局》，《人民日报》2016年1月5日第5版。

[3] 参见任明艳《互联网背景下国家信息主权问题研究》，《河北法学》2007年第6期。

[4] 参见余丽《论制网权：互联网作用于国际政治的新型国家权利》，《郑州大学学报》（哲学社会科学版）2012年第4期。

[5] Timothy S. Wu，“Cyberspace Sovereignty? —The Internet and the International System”，Harvard Journal of Law & Technology，vol. 10（1997），no. 3，pp.647-666.

[6] 该文探讨了互联网对包括“信息主权”（information sovereignty）在内的传统领土主权的挑战，并建构出网络空间的自治模式。David R. Johnson and David G. Post，“Law and Borders：The Rise of Law in Cyberspace”，Stanford Law Review，vol. 48（1996），no 5，pp. 1367-1402.

[7] 参见约翰·P. 巴洛《网络空间独立宣言》，李旭、李小武译，高鸿钧校，载高鸿钧主编《清华法治论衡》（第四辑），清华大学出版社，2004，第10页。

[8] 参见〔美〕约瑟夫·奈《权力大未来》，王吉美译，中信出版社，2012，第171页。

[9] Jack L. Goldsmith，“The Internet and the Abiding Significance of Territorial Sovereignty”，Indiana Journal of Global Legal Studies，vol. 5（1998），no. 2，pp. 475-491.

[10] 相关官方的观点参见：Abraham M. Denmark & James Mulvenon（eds.），Contested Commons：The Future of American Power in a Multipolar World，Center for a New America Security，2010，http：//www.cnas.org/files/documents/publications/CNAS%20Contested%20
相关学者的观点参见Chris C. Demchak & Peter Dombrowski，“Rise of a Cybered Westphalian Age”，Strategic Studies Quarterly，vol. 5（2011），no. 1，p.32；Justyna Hofmokl，“The Internet Commons：Towards an Eclectic Theoretical Framework”，International Journal of the Commons，vol. 4（2010），no. 1，pp.226-250；Roger Hurwitz，“Depleted Trust in the Cyber Commons”，Strategic Studies Quarterly，vol. 6（2012），no. 3，pp.20-45。

[11] 例如，美国白宫网络政策评论起草人Sean Kanuck认为全球公域说缺乏国际法和政治经济学的理论支持。See Sean Kanuck，“Sovereign Discourse on Cyber Conflict Under International Law”，Texas Law Review，vol. 8（2010），pp.1571-1580.印第安纳大学Scott J. Shackelford助理教授直指网络空间是“虚伪公域”（pseudocommons）。See Scott J. Shackelford，“Toward Cyberpeace：Managing Cyberattacks Through Polycentric Governance”，American University Law Review，vol. 62（2013），no. 5，pp.1285-1296.美国战略司令部官员Patrick W. Franzese剖析了全球公域的五大特征，而网络空间无一具备。See Patrick W. Franzese，“Sovereignty in Cyberspace：Can it Exist？”，Air Force Law Review，vol. 64（2009），pp.14-17.

[12] Sarah Myers West，Globalizing Internet Governance：Negotiating Cyberspace Agreements in the Post-Snowden Era（TPRC Conference Paper），http：//ssrn.com/abstract=2418762.

[13] 参见〔澳〕约瑟夫·A. 凯米莱里、吉米·福尔克《主权的终结——日趋“缩小”和“碎片化”的世界政治》，李东燕译，浙江人民出

版社，2001，第13页。

[14] 参见王禹《主权的概念及其在中国政府收回香港和澳门过程中的运用》，《一国两制研究》2012年第2期。

[15] 参见〔荷〕格劳秀斯《战争与和平法》，何勤华等译，上海人民出版社，2005，第88页。

[16] Ivan Simonovi，“Relative Sovereignty of the Twenty First Century”，Hastings International & Comparative Law Review，vol.25（2002），no. 3，pp. 371-372.

[17] 参见朱毓朝《国家主权原则：国际关系的柱石还是“有规则的虚伪”》，《中大政治学评论》第3辑，中央编译出版社，2008。

[18] 参见俞可平等《全球化与国家主权》，社会科学文献出版社，2003，第13页。

[19] James Crawford and Martti Koskenniemi （eds.），The Cambridge Companion to International Law，Cambridge University Press，2012，p.118.

[20] James Crawford and Martti Koskenniemi （eds.），The Cambridge Companion to International Law，Cambridge University Press，2012，p.124.

[21] 杨泽伟：《主权论——国际法上的主权问题及其发展趋势研究》，北京大学出版社，2006，第266～267页。

[22] Boutros Boutros-Ghali，“Empowering the United Nations”，Foreign Affairs，vol.72 （1992/3），no.5，pp. 98-99.

[23] 参见〔美〕路易斯·亨金《国际法：政治与价值》，张乃根等译，中国政法大学出版社，2005，第13页。

[24] 李浩培：《国际法的概念和渊源》，贵州人民出版社，1994，第7页。

[25] 参见〔英〕詹宁斯、瓦茨修订《奥本海国际法》（第一卷第一分册），王铁崖等译，中国大百科全书出版社，1995，第92页。

[26] 参见王逸舟《当代国际政治背景下的国家主权》，《欧洲》1993年第6期。

[27] 参见〔美〕尼考劳斯·扎哈里亚迪斯主编《比较政治学：理论、案例与方法》，宁骚等译，北京大学出版社，2008，第158页。

[28] 〔美〕罗伯特·基欧汉、约瑟夫·奈：《权力与相互依赖》（第三版），门洪华译，北京大学出版社，2002，第9页。

[29] 参见〔英〕劳特派特修订《奥本海国际法》（上卷第一分册），王铁崖、陈体强译，商务印书馆，1989，第101页。

[30] 参见毛维准、卜永光《负责任主权：理论缘起、演化脉络与争议挑战》，《国际安全研究》2014年第2期。

[31] Antonio Cassese，International Law，Oxford University Press，2005，p.15.

[32] Amitai Etzioni，“Sovereignty as Responsibility”，Journal of World Affairs，vol. 50 （2006），no. 1，p.72.

[33] James Crawford and Martti Koskenniemi （eds.），The Cambridge Companion to International Law，Cambridge University Press，2012，p.132

[34] 参见联合国前国际法院特别法官伊恩·布朗利对主权的解说。〔英〕伊恩·布朗利：《国际公法原理》，曾令良等译，法律出版社，2007，第257页。

[35] 惠志斌：《全球网络空间信息安全战略研究》，世界图书出版公司，2013，第8页。

[36] The UK Cyber Security Strategy，

https：//www.gov.uk/government/uploads/system/uploads/attachment_data/cyber-security-strategy-final.pdf.

[37] ITU，ITU Toolkit For Cybercrime Legislation，https：//www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf.

[38] Timothy S. Wu，“Cyberspace Sovereignty? —The Internet and the International System”，Harvard Journal of Law & Technology，vol. 10（1997），no. 3，p.649.

[39] David D. Clark and Marjory S. Blumenthal，“Rethinking the Design of the Internet：The End to End Arguments vs. the Brave New World”，ACM Transactions on Internet Technology，vol.1（2001），no.1，pp.71-79.

[40] 吴修铭：《总开关：信息帝国的兴衰变迁》，顾佳译，中信出版社，2011，第170页。

[41] Lawrence Lessig，Code and Other Laws of Cyberspace，Harvard University Press，1999，p. 32.

[42]〔美〕劳伦斯·莱斯格：《代码2.0：网络空间中的法律》，李旭、沈伟伟译，清华大学出版社，2009，第36～39页。

[43] Robert Baldwin，Martin Cave and Martin Lodge（eds.），The Oxford Handbook of Regulation，Oxford University Press，2010，pp. 527-533.

[44] Raymund Werle and Eric J. Iversen，“Promoting Legitimacy in Technical Standardization”，Science，Technology & Innovation Studies，vol.2（2006），no.1，pp.19-39.

[45] Angele A. Gilroy，Access to Broadband Networks：The Net Neutrality Debate（Congressional Research Service），

http：//fas.org/sgp/crs/misc/R40616.pdf.

[46] Maureen K. Ohlhausen，The Open Internet：Regulating to Save the Unregulated Internet？，
http：//www.ftc.gov/speeches/ohlhausen/121026mannheim.pdf.

[47] 2014年1月14日，美国哥伦比亚特区巡回上诉法院就Verizon公司状告联邦通信委员会“网络中立条例”违法一案做出判决：“法律效力搁置，案件返回原审法院。”

[48] David R. Johnson and David G. Post，“The Rise of Law on the Global Network”，in Brian Kahin & Charles Nesson （eds.），Borders in Cyberspace：Information Policy and the Global Information Infrastructure，MIT Press，1997，p. 3.

[49] Julie E. Cohen，“Cyberspace As/And Space”，Columbia Law Review，vol. 107 （2007），no. 1，p. 211.

[50] Orin S. Kerr，“The Problem of Perspective in Internet Law”，Georgetown Law Journal，vol. 91 （2003），pp.360-361.

[51] Trotter Hardy，“The Proper Legal Regime for ‘Cyberspace’”，University of Pittsburgh Law Review，vol. 55 （1994），pp.993-995.

[52] Darin Barney：《网络社会的概念：科技、经济、政治与认同》，黄守义译，韦伯文化国际出版有限公司，2012，第31页。

[53] Julie E. Cohen，“Cyberspace As/And Space”，in Columbia Law Review，vol. 107 （2007），no. 1，pp. 237-243.

[54] 关于异托邦的详细阐释，参见〔法〕福柯《他性空间》，王喆译，《世界哲学》2006年第6期。

[55] 关于数字化信息的巨大潜力，参见〔英〕维克托·迈尔·舍恩

伯格《大数据时代》，周涛译，浙江人民出版社，2013，第98～126页。

[56] 基于数字化信息的界定，本章并不区分信息主权和数据主权（data sovereignty）。

[57] Larry Diamond，“Liberation Technology”，Journal of Democracy，vol. 21 （2010），no.3，p.70.

[58] 互联网的前身主要是1974年美国国防部国防高级研究计划署领头研发的阿帕网，具有高度的政治色彩。

[59] 参见张新宝《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015年第3期。

[60] Ronald Deibert & Rafal Rohozinski，“Liberation vs. Control：The Future of Cyberspace”，Journal of Democracy，vol. 21 （2010），no.4，p55.

[61] 王孔祥：《互联网治理中的国际法》，法律出版社，2015，第100～103页。

[62] Robert Baldwin，Martin Cave and Martin Lodge （eds.），The Oxford Handbook of Regulation，Oxford University Press，2010，pp.533-542.

[63] Jack Goldsmith and Tim Wu，Who Controls the Internet? Illusions of a Borderless World，Oxford University Press，2006，p145.

[64] Zachary Peterson，Mark Gondree and Robert Beverly，“A Position Paper on Data Sovereignty：The Importance of Geolocating Data in the Cloud”，in Proceedings of the 8th USENIX Conference on Networked Systems Design and Implementation，2011，https：//www.usenix.org/legacy/event/hotcloud11/tech/final_files/Peterson.p

[65] Jonah Force Hill，“The Growth of Data Localization Post-snowden：Analysis and Recommendations for U.S.Policymakers and Business Leaders”，in The Hague Institute for Global Justice，Conference on the Future of Cyber Governance，2014，http：//ssrn.com/abstract=2430275.

[66] Christopher Rudolph，“Sovereignty and Territorial Borders in a Global Age”，International Studies Review，vol. 7 （2005），no.1，pp.1-20.

[67] 关于主权的不同维度，请参见Stephen D. Krasnera，“Biding Sovereignty”，International Political Science Review，vol.22 （2001），no. 3，pp.229-251。

[68] Jeanette Hofmann，“Internet Governance：A Regulative Idea in Flux”，in Ravi Kumar & Jain Bandamutha （eds.），Internet Governance：An Introduction，Icfai University Press，2007，pp 74-108.

[69] WSIS，Tunis Agenda for the Information Society，http：//www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[70] Markus Kummer，Multistakeholder Cooperation：Reflections on the Emergence of a New Phraseology in International Cooperation，http：//www.internetsociety/org/blog/2013/05/multistakeholder-cooperation-reflections-emergence-newphraseology-international.

[71] Lawrence Strickling，Moving Together Beyond Dubai，http：//www.ntia.doc.gov/blog/2013/moving-together-beyond-dubai.

[72] Avri Doria，Use［and Abuse］of Multistakeholderism in the Internet，http：//psg.com/～avri/papers/Use%20and%20Abuse%20of%20MSism-130902.pdf.

[73]〔德〕马克斯·韦伯：《社会学的基本概念》，顾忠华译，广西师范大学出版社，2005，第34页。

[74] James A. Lewis，“Internet Governance：Inevitable Transitions”，The Centre for International Governance Innovation，https：//www.cigionline.org/sites/default/files/no4.pdf.

[75]〔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、鲁锐、夏雪、郑凯伦译，上海交通大学出版社，2015，第318页。

[76] John E. Savage & Bruce W. McConnell，Exploring Multi-Stakeholder Internet Governance（Breakthrough Group Working Paper），http：//www2.ewi.info/sites/default/files/Exploring%20Multi-Stakeholder%20Internet%20Governance_McConnell%20and%20Savage%20BC

[77] Neil Weinstock Netanel，“Cyberspace Self-Governance：A Sceptical View from Liberal Democratic Theory”，California Law Review，vol. 88（2000），no. 2，pp. 395-498.

[78] The National Military Strategy of United States 2011，http：//58.30.31.210：9999/www.defense.gov/Portals/1/Documents/pubs/2011-National-Military-Strategy.pdf.

[79] 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》，《中国社会科学》2014年第6期。

[80] Division of Environmental Law and Conventions，IEG of the Global Commons，http：//www.unep.org/delc/GlobalCommons/tabid/54404/.

[81] 参见张茗《全球公域：从“部分”治理到“全球”治理》，《世界经济与政治》2013年第11期。

[82] 参见王义桅《全球公域与美国巧霸权》，《同济大学学报》（社会科学版）2012年第4期。

[83] U.S. Department of Defense，The Strategy for Homeland Defense and Civil Support，http：//fas.org/man/eprint/homedefstrat.pdf.

[84] 参见孙灿、郑普建《国内学界全球公域研究综述》，《战略决策研究》2014年第3期。

[85] 参见〔美〕威廉·J.米切尔《伊托邦：数字时代的城市生活》，吴启迪等译，上海科技教育出版社，2005，第13页。

[86] Scott J. Shackelford，“Toward Cyberpeace：Managing Cyberattacks Through Polycentric Governance”，American University Law Review，vol. 62（2013），no. 5，p.1288.

[87] Mark Raymond，The Internet as a Global Commons?，https：//www.cigionline.org/publications/2012/10/internet-global-commons.

[88] 参见沈逸《全球网络空间治理原则之争与中国的战略选择》，《外交评论》2015年第2期。

[89] PRISM（surveillance program），https：//en.wikipedia.org/wiki/PRISM_（surveillance_program）.

[90] Michael A. Heller，“The Tragedy of the Anticommons：Property in the Transition from Marx to Markets”，Harvard Law Review，vol. 111（1998），no. 3，pp. 621-688.

[91] Timothy S. Wu，“Cyberspace Sovereignty? —The Internet and the International System”，Harvard Journal of Law & Technology，vol. 10（1997），no. 3，pp.647-665.

[92] Alexander Klimburg，The Internet Yalta（Center for a New American Security（CNAS）Commentary），http：//www.cnas.org/files/documents/publications/CNAS_WCIT_comment

[93] 参见杨剑《信息技术空间：权力、网络经济特征与财富分配》，上海社会科学院博士学位论文，2008，第77页。

[94] 参见刘建伟、余冬平《试论网络空间的世界政治化》，《国际

关系研究》2013年第6期。

[95] Panayotis A Yannakogeorgos & Adam B Lowther （eds.），Conflict and Cooperation in Cyberspace：The Challenge to National Security，CRC Press，2013，pp.283-287.

[96] 网络就绪指数（Networked Readiness Index）从三个方面衡量了各国有效利用信息通信技术的成熟度：信息通信技术在整体商业、监管和基础设施方面的环境；个人、企业和政府使用并获益于信息通信技术的准备就绪程度；实际使用最新信息通信技术的情况。参见临渊《2014年网络就绪指数排行榜解读》，http：//www.cnii.com.cn/internation/2014-04/30/content_1353346.htm。

[97] Jensen，Eric Talbot，“Cyber Sovereignty：The Way Ahead”，Texas International Law Journal，vol.50 （2015），no.2，pp.283-284.

[98] 参见刘军宁《直接民主与间接民主》，三联书店，1998，第37页。

[99] Ralf Bendrath，“The Return of the State in Cyberspace：The Hybrid Regulation of Global Data Protection”，in Myriam Dunn，Sai Felicia，Krishna-Hensel & Victor Mauer （eds.），The Resurgence of the State：Trends and Processes in Cyberspace Governance，Ashgate Publishing Ltd.，2007，pp.9-34.

[100] 参见蔡翠红《网络空间治理的大国责任刍议》，《当代世界与社会主义》2015年第1期。

[101] 参见〔美〕道格拉斯·C.诺思《经济史中的结构与变迁》，陈郁等译，上海三联书店、上海人民出版社，1994，第123页。

[102] See United Nations General Assembly，Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security（A/70/174）.

[103] 参见王铁崖、周忠海编《周鲠生国际法论文选》，海天出版社，1999，第395页。

[104] 陈序经：《现代主权论》，张世保译，清华大学出版社，2010，第157页。

[105] 政治性主权和法律性主权的区分由英国法学家戴雪所提出，参见〔英〕戴雪《英宪精义》，雷宾南译，中国法制出版社，2001，第148页。另参见〔英〕安德鲁·海伍德编《政治理论教程》（第三版），李智译，中国人民大学出版社，2009，第104～106页；〔美〕梅里亚姆：《卢梭以来的主权学说史》，毕洪海译，法律出版社，2006，第181～182页。

[106] 参见〔日〕篠田英朗《重新审视主权：从古典理论到全球时代》，戚渊译，商务印书馆，2005，第147～150页。

[107] 参见季卫东《宪政新论——全球化时代的法与社会变迁》，北京大学出版社，2002，第220页。

[108] 关于主权在权力（power）和权利（right）上的区分，参见Antonio Cassese，International Law（2nd edition），Oxford University Press，2005，pp.49-51。

[109] 参见〔法〕让·博丹《主权论》，李卫海、钱俊文译，北京大学出版社，2008，第102～145页。

[110] 参见喻锋《“主权权力让渡”新解》，《海南大学学报》2003年第3期。需要说明，海洋法中的主权和主权性权利并不一致，例如国家在专属经济区享有主权性权利，但并不享有主权。

[111] 这里借用了弗拉克·伊斯特布鲁克对“网络法”的批评，Frank H. Easterbrook，“Cyberspace and the Law of the Horse”，University of Chicago Legal Forum，vol. 1996 （1996），no.1，pp.207-216.

[112] 参见毛维准、卜永光《负责任主权：理论缘起、演化脉络与争

议挑战》，《国际安全研究》2014年第2期。

[113] 参见〔美〕巴拉巴西《链接：网络新科学》，徐彬译，湖南科技出版社，2001，第173页。

[114] 参见俞可平《治理与善治引论》，《马克思主义与现实》1999年第5期。

[115] 参见季卫东《法律程序的意义》，《中国社会科学》1993年第1期。

[116] 参见熊光清《从辅助原则看个人、社会、国家、超国家之间的关系》，《中国人民大学学报》2012年第5期。

[117] John Agnew，Globalization and Sovereignty，Rowman & Littlefield Publishers，2009.pp. 32-35.

[118] 在该案中，针对雅虎公司在网站上拍卖纳粹物的行为，法院认为法国用户接近、访问包含有纳粹物品的网站违犯了法国法律，因此判令雅虎关闭法国用户进入网页的途径。随后，雅虎将案件起诉到美国圣何塞（San Jose）的地区法院，要求撤消法国法院的判决。其理由是：它是一家基地在美国的互联网公司，其提供的服务完全符合美国法律，法国法院无权对发生在美国境内的案件进行审理，并且，其判决还违犯了美国宪法第一修正案的规定。这一案件充分凸显了网络空间中的主权冲突以及单边行动的困境。Stephen J. Kobrin，“Territoriality and the Governance of Cyberspace”，Journal of International Business Studies，vol. 32（2001），no. 4，pp.671-672.

[119] Robert O. Keohane & Joseph S.Nye Jr.，“Power and Interdependence in the Information Age”，Foreign Affairs，vol. 77（1998），no. 5，p.82.

[120] Adeno Addis，“Thin State in Thick Globalism：Sovereignty in the Information Age”，Vanderbilt Journal of Transnational Law，vol. 37（2004），no. 1，pp. 1-108.

[121] 这里综合了Stephen K. Gourley和劳伦斯·莱斯格对网络空间的定义，参见Panayotis A.Yannakogeorgos & Adam B.Lowther （eds.），Conflict and Cooperation in Cyberspace：The Challenge to National Security，CRC Press，2013，pp.278-279；〔美〕劳伦斯·莱斯格：《思想的未来》，李旭译，袁泳审校，中信出版社，2004，第23页。

[122] Neil Duxbury，“Robert Hale and the Economy of Legal Force”，The Modern Law Review，vol. 53 （1990），no.4，p.434.

[123] Julia Black，“Proceduralizing Regulation：Part II”，Oxford Journal of Legal Studies，vol.21 （2001），no.1，pp.33-58.

[124] 参见徐汉明《网络治理：安全优先 兼顾自由》，《中国社会科学报》2014年6月27日。

[125] 参见张新宝、林钟千《互联网有害信息的依法综合治理》，《现代法学》2015年第2期。

[126] 该原则最早是在2003年国家信息化领导小组《关于加强信息安全保障工作的意见》中提出的，后来扩充为“三谁原则”，即“谁主管谁负责、谁经营谁负责、谁接入谁负责”。

[127] 参见秦前红、李少文《网络公共空间治理的法治原理》，《现代法学》2014年第6期。

[128] 参见赵克锋编《中国防火长城——互联网审查的法律经济学》，中国经济出版社，2010，第145页。

[129] 参见张恒山《英国网络管制的内容及其手段探析》，《重庆工商大学学报》（社会科学版）2010年第3期。

[130] 参见任剑涛《国家治理的简约主义》，《开放时代》2010年第7期。

[131] 参见崔巍《网络社会管理须“软”“硬”法并举》，《光明日

报》2013年10月20日第7版。

[132] 参见余凌云《行政法讲义》，清华大学出版社，2014，第244页。

[133] 参见胡凌《网站治理：制度与模式》，《北大法律评论》2009年第2期。

[134] 参见莫兰《复杂性思想导论》，陈一壮译，华东师范大学出版社，2008，第5页。

[135] Derek E. Bambauer，“Cybersieves”，Duke Law Journal，vol.59（2009），no. 3，pp.390-409.

[136] Henry H. Perritt Jr.，“Jurisdiction in Cyberspace”，Villanova Law Review，vol.41（1996），no.1，pp.2-5.

[137] 参见马小军《“领土主权理论”的变化与中国领土安全再认识》，《领导者》2010年第4期。

[138] Wolff Heintschel von Heinegg，Legal Implication of Territorial Sovereignty，http：//insct.syr.edu/wp-content/uploads/2015/06/Heinegg_Sovereignty_In_Cyberspace.pdf.

[139] See Michael N. Schmitt（ed.），Tallinn Manual on the International Law Applicable to Cyber Warfare，Cambridge University Press，2013，p.19.

[140] Samuel F. Miller，“Prescriptive Jurisdiction over Internet Activity：The Need to Define and Establish the Boundaries of Cyberliberty”，Indiana Journal of Global Legal Studies，vol.10（2003），no.2，pp.227-254.

[141] 李智：《国际私法中互联网管辖权制度研究》，厦门大学出版社，2009，第122页。

[142] Ray August，“International Cyber-Jurisdiction：A Comparative Analysis”，American Business Law Journal，vol. 39 （2002），no. 4，p540.

[143] 刘连泰：《信息技术与主权概念》，《中外法学》2015年第2期。

[144] Wolff Heintschel von Heinegg，“Territorial Sovereignty and Neutrality in Cyberspace”，International Law Studies，vol.89 （2013），pp.133-134.

[145] 黄瑶：《后冷战时期的领土完整原则与人民自决原则》，《法学》2006年第6期。

[146] 关于主权权利束的说明，详见Michael Ross Fowler & Julie Marie Bunck，Law，Power，and the Sovereign State：The Evolution and Application of the Concept of Sovereignty，Pennsylvania State University Press，1995，p.71。

[147] 陈牧民：《当代国际安全理论中的主权意涵》，《全球政治评论》2008年第22期。

[148] 参见〔美〕斯蒂芬·克莱斯勒《结构冲突：第三世界对抗全球自由主义》，李小华译，浙江人民出版社，2001，第1页。

[149] 参见若英《什么是网络主权？》，《红旗文稿》2014年第13期。

[150] 关于独立权的界定，请参见李国民、欧斌主编《国际法》，清华大学出版社，2006，第38页。

[151] 王铁崖主编《国际法》，法律出版社，1995，第117页。

[152] 黄志雄：《国际法视角下的“网络战”及中国的对策——以诉诸武力权为中心》，《现代法学》2015年第5期。

[153] 《信息安全国际行为准则》，http：//www.fmprc.gov.cn/mfa_chn/ziliao_611306/tytj_611312/zcwj_611316

[154] 保密性是指未经授权无法访问系统或取得数据的特性，完整性是指未经授权无法改变数据内容的特性，可用性是指经授权可访问系统并在授权范围内使用数据的特性。

[155] Nathan A. Sales，“Regulating Cyber-security”，Northwestern University Law Review，vol. 107 （2013），no. 4，pp.1503-1568.

[156] 龚宇：《气候变化损害的国家责任：虚幻或现实》，《现代法学》2012年第4期。

[157] Corfu Channel（United Kingdom v. Albania），ICJ Reports，4，22，1949.

[158] 龚宇：《气候变化损害的国家责任：虚幻或现实》，《现代法学》2012年第4期。

[159] 参见杨义先《网络信息安全与保密》，北京邮电大学出版社，1999，第2页。

[160] Laura De Nardis and Mark Raymond，Thinking Clearly about Multistakeholder Internet Governance，http：//ssrn.com/abstract=2354377.

[161] 参见洪京一主编《世界网络安全发展报告（2014—2015）》，社会科学文献出版社，2015，第8～9页。

[162] U.S. Cybercrime Losses Double，Homeland SEC.News Wire，http：//www.homelandsecuritynewswire.com/us-cybercrime-losses-double.

[163] 郎平：《网络空间安全：一项新的全球议程》，《国家安全研究》2013年第1期。

[164] 参见李伯军《论网络战及战争法的适用问题》，《法学评论》

2013年第4期。

[165] 参见郭秋永《政治参与的意义：方法论上的分析》，《人文及社会科学集刊》1992年第5卷第1期。

[166] 共同参与和共同治理的区别，参见施文真《“人类共同遗产”原则与“共同资源”管理》，《科技法学评论》2010年第7卷第1期。

[167] 王孔祥：《国际化的“互联网治理论坛”》，《国外理论动态》2014年第3期。

[168] 参见刘杨钺《全球网络治理机制：演变、冲突与前景》，《国际论坛》2012年第1期。

[169] 参见鲁传颖《试析当前网络空间全球治理困境》，《现代国际关系》2013年第11期。

[170] U.S. Dep’t St.，Outcomes from the International Telecommunication Union 2014 Plenipotentiary Conference in Busan，Republic of Korea，
http：//www.state.gov/r/pa/prs/ps/2014/11/233914.htm.

[171] 于志刚：《缔结和参加网络犯罪国际公约的中国立场》，《政法论坛》2015年第5期。

[172] 王孔祥：《网络安全的国际合作机制探析》，《国际论坛》2013年第5期。

[173] 参见汪晓风《中美关系中的网络安全问题》，《美国研究》2013年第3期。

[174] Scott J. Shackelford，Enrique Oti，Jaclyn A. Kerr，Elaine Korzak & Andreas Kuehnvia，“Spotlight on Cyber V：Back to the Future of Internet Governance?”，Georgetown Journal of International Affairs，

http：//journal.georgetown.edu/back-to-the-future-of-internet-governance/.

[175] 《首次中美打击网络犯罪及相关事项高级别联合对话成果声明》，http：//www.mps.gov.cn/n16/n894593/n895609/4923384.html。

[176] 例如，《网络犯罪公约》对侵犯著作权的高度重视，不利于包括中国在内的发展中国家。

[177] Robert O. Keohane，“International Institutions：Two Approaches”，International Studies Quarterly，vol. 32 （1988），no. 4，pp. 379-396.

[178] Kristen Eichensehr，“The Cyber-law of Nations”，Georgetown Law Journal，vol. 317 （2015），no.2，pp.340-344.

[179] 参见杨泽伟《国家主权平等原则的法律效果》，《法商研究》2002年第5期。

[180] 参见汪晓风《中美关系中的网络安全问题》，《美国研究》2013年第3期。

[181] 参见秦天宝《国际法的新概念“人类共同关切事项”初探》，《法学评论》2006年第5期。

[182] 参见〔英〕欧文·麦克因泰里《国际法视野下国际水道的环境保护》，秦天宝译，知识产权出版社，2014，第148页。

[183] 参见曾彩琳《国际河流公平合理利用原则：回顾、反思与消解》，《世界地理研究》2012年第2期。

[184] 这里借鉴了布赞的区域安全复合体理论，参见王志坚《水霸权、安全秩序与制度构建：国际河流水政治复合体研究》，社会科学文献出版社，2015，第20页。

[185] 参见任明艳《互联网背景下国家信息主权问题研究》，《河北

法学》2007年第6期。

[186] 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》，《法学评论》2015年第4期。

[187] 参见张新宝《论网络信息安全合作的国际规则制定》，《中州学刊》2013年第10期。

[188] 参见〔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、鲁锐、夏雪、郑凯伦译，上海交通大学出版社，2015，第322页。

[189] Lord Hope of Craighead，“Is the Rule of Law now the Sovereign Principle?”，in Richard Rawlings，Peter Leyland and Alison Young（eds.），Sovereignty and the Law，Oxford University Press，2013，pp.89-97.

第六章

网络法上的网络空间主权原则[1]

《网络空间独立宣言》发表20年来的各国实践已经证明，互联网不是一个法外之地。巴洛幻想的一个免于政府介入的互联网早已被形形色色的网络入侵、网络攻击、网络犯罪等网络安全问题击得粉碎。

互联网是当今最为重要的全球性基础设施。在互联网发展初期，网络呈现的主要是其技术属性，人们将其作为更有效率的信息储存、传输和处理工具；随着互联网的普及和网络信息技术的发展，互联网的媒体属性逐渐显现，人们越来越多地从网络上获取新闻资讯；随着互联网的进一步普及和网络信息技术的进步，网络空间的社会属性凸显，网络已经成为人们生活必不可少的一部分。在这个网络变迁的过程中，网络空间经历了“去主权化”到“主权回归”的过程。越来越多的人认识到，网络空间主权（或称网络主权）是国家主权在网络空间的延伸，是国家主权不可分割的组成部分。

本章基于网络空间的构成要素分析了网络空间与国家主权的关联性，明确网络空间不属于全球公域，进而阐述了将网络空间主权原则确立为网络法基本原则的必要性，最后探讨了网络空间主权原则在网络法中的体现。

一 网络空间与国家主权相关联

对于网络的概念，目前学术界和实务界没有统一的定义。通常认

为，英文“network”所指的网络主要是指网络的物理形态。最早的计算机网络是指将计算机连接在一起所形成的用以交换数据的网络。现在连接在网络上的已经不仅仅限于普通的计算机了，还包括手机、电视等各种信息终端和设备，网络的功能也不仅仅限于交换数据，还包括信息的收集、储存、传输、处理等各项功能。我国《网络安全法》将网络定义为：“由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。”这也主要是从物理形态上对网络进行界定。

“网络空间（cyberspace）”的内涵比“网络”更宽泛，除了包括物理网络外，还包括人的活动等因素，特别是认可网络空间与现实空间一样，也是人们可以进行交往、互动的空间，即增加了网络的社会层。因此，网络空间是基于网络的可供人们交流互动的电子空间。

网络空间是否有主权，目前仍有一些争议。有人认为，网络无国界，网络空间是全球公域，不应受任何单个国家所管辖、支配，因而网络主权一说不成立。这以1996年美国网络活动家约翰·佩里·巴洛（John Perry Barlow）发表的《网络空间独立宣言》（A Declaration of Independence of Cyberspace）[2]为代表。他将网络空间视为一个自由放任的“自主体系”，倡导网络空间“自我规制”，反对将空间的各种政府管制延伸到网络空间，这是典型的网络空间“无主权论”，认为网络空间自然而然独立于国家的主权。巴洛乌托邦式的理想诞生于互联网发展的早期，《网络空间独立宣言》发表20年来的各国实践已经证明，互联网不是一个法外之地。巴洛幻想的一个免于政府介入的互联网早已被形形色色的网络入侵、网络攻击、网络犯罪等网络安全问题击得粉碎。

我们认为，要确定网络空间是否有国家主权，可以从网络空间的构成要素出发，先分析网络空间的构成要素与国家主权的关系，进而确定网络空间与国家主权的联系。

（一）网络空间的构成

网络空间的构成通常包括以下要素：

1. 网络设备

网络空间是由计算机、智能终端、路由器、交换机、缆线等硬件设备联网构成的电子空间，这些硬件设备是构成网络空间的物理层。随着移动互联网的发展和智能移动终端（如智能手机、平板电脑）的普及，一些看似孤立的设备也可以成为网络空间的一部分，只要它们能够通过移动互联网与互联的计算设备分享信息。从广义上讲，存放网络设备的设施和建筑也是网络空间的组成部分。

2.软件和协议

计算设备和传输设备必须借助软件和协议才能发挥处理和传输信息的功能；没有软件和协议的帮助，这些设备就不可能成为网络空间的一部分，也无法完成数据处理、传输或交换。

软件是一系列按照特定顺序组织的计算机数据和指令的集合。一般来讲，软件可以分为系统软件和应用软件。系统软件泛指那些为了有效地使用计算机系统，给应用软件开发与运行提供支持，或者能够为用户管理与使用计算机提供方便的一类软件。例如：基本输入/输出系统（BIOS）、操作系统（如Windows）、程序设计语言处理系统（如C语言编译器）等。应用软件泛指那些专门用于解决各种具体应用问题的软件。例如：文字处理软件、信息检索软件、游戏软件、媒体播放软件、网络通信软件等。软件并不只包括可以在计算机（这里的计算机是指广义的计算机）上运行的电脑程序，与这些电脑程序相关的文档一般也被认为是软件的一部分。

网络协议是为计算机网络中进行数据交换而建立的规则、标准或约定的集合。网络协议是由三个要素组成：①语义。语义是解释控制信息每个部分的意义。它规定了需要发出何种控制信息，以及完成的动作与做出什么样的响应。②语法。语法是用户数据与控制信息的结构与格式，以及数据出现的顺序。③时序。时序是对事件发生顺序的详细说明。这三个要素也可以形象地描述为：语义表示要做什么，语法表示要怎么做，时序表示做的顺序。

3.信息

从广义上讲，信息可以泛指人类社会传播的一切内容。人类通过获得、识别自然界和社会的不同信息来区别不同事物，得以认识和改造世界。信息论奠基人克劳德·香农（C.E.Shannon）认为，信息是“用来

消除随机不确定性的东西”。[3]原工信部副部长杨学山先生认为，信息是指所有客观存在的含义，它由载体、外壳、含义三要素构成。信息的载体和外壳是形，含义是义。承载信息的光、声、电、纸张、核苷酸[4]、神经元[5]是形，文字、语言、图表、概念是外壳。[6]对于计算机网络来讲，信息主要是指电子线路中传输的信号。网络的最重要意义在于处理、储存和传输信息，因此网络设备上生成、存储或传输的信息是网络空间的必备要素。网络上的信息主要表现为电子数据形态。

4. 网络主体

网络空间的主体非常广泛，包括网络建设者、运营者、服务提供者、监督管理者、用户等。其中最主要的是网络服务提供者和用户。网络服务提供者是提供各种软硬件或信息服务供他人使用的人，包括为网络用户提供信息通道或平台服务的狭义网络服务提供者和为用户提供信息内容服务的网络信息服务提供者。狭义的网络服务提供者又包括网络接入服务提供者、网络空间提供者（包括提供博客空间、BBS空间、服务器空间出租等）、搜索引擎服务提供者、传输通道服务提供者（如电信运营商）、云服务提供者等。网络用户则是指互联网服务的使用者。网络经济是“点击”经济、“注意力”经济，没有大量的用户，网络难以商业化发展。

5. 网络行为

网络空间是虚拟的电子空间，人们通过实施各种网络行为与其他网络主体发生社会关系，形成人与人、人与电脑的互动。网络行为主要包括网络信息行为和网络技术行为。网络信息行为以信息为行为对象，例如访问浏览网页信息、下载和上传信息、播放网络音视频、接收或发送电子邮件、入侵或破坏信息系统、窃取或篡改信息等。网络技术行为主要有网络技术开发、网络维护、程序的升级等。正是有人的活动，才使得网络社会得以形成。

（二）网络空间与国家主权的关联

网络空间的上述构成要素，均与国家主权有着关联：

首先，组成网络空间的物理设备设施是在各国主权管辖之下。网络空间是人造空间，非真正的物理空间，它是由大大小小的网络（局域

网）互联互通而成。这些组成网络空间的各个局域网络分别归属于私人、组织或政府所有。除了铺设在公海中的通信线缆或太空中的卫星外，组成网络的设备设施都以物理的方式存在于各国领土之上，置于由国家主权控制的地理空间中，相关主权国家当然对其具有管辖权。

其次，各国对在其境内运行、使用的网络软件、协议具有管辖权。在一国境内运行、使用的软件或协议通常需要符合该国认可的技术标准。对于提供、安装、传播损害国家利益、公共利益和他人合法权益的恶意软件、代码等行为，则属于国家法律打击的对象，许多国家都立法予以禁止和惩处。

第三，各国对在其境内的信息具有管辖权。当前学术界对信息或数据是否具有主权尚存争议，但争议焦点主要针对流经一国的数据以及流转到境外的数据是否有管辖权。对于储存于一国境内的信息，学者们认为是具有管辖权的。[7]在网络时代，以大数据形式存在的信息成为越来越重要的资源，信息的安全往往涉及个人利益、社会公共利益，甚至国家安全，因此，国家必须对信息行使管辖权。

第四，各国对本国网民及其网络行为，以及对本国实施特定危害行为的他国网民均具有管辖权。网络空间是一个由代码构成的电子空间，具有虚拟性的一面。但随着网络的普及和网络应用的深入开发，网络空间更具有现实性和社会性。随着网民数量的迅速增长，网络空间的社会性也越来越突出。每个上网者和网上的网站、网页都是互联网的节点；节点连接节点，交织成网，形成网络节点联系的体系，构成互联网上的社会交往体系，即网络社会。[8]在网络空间中，人们相互分享信息，彼此交往互动，成群结社。网络社会就是现实中的人在网络空间发生的各种社会关系的总和，它是现实社会在网络上的延伸，自然应属于现实社会的一部分。可见，网络空间是虚拟空间和现实社会的结合体。网络空间除了在物理三维上是虚拟的，在其他方面都具有现实性。网络空间的虚拟性是其表象，网络空间的现实性、社会性才是其本质。

在现实社会中，一国对于其公民、居住在其境内的他国公民和无国籍人、对该国实施特定危害行为的境外自然人均有权管辖。在网络社会也是一样，参与的网民也主要是各国公民。在这样一个有大量国民参与其中的网络社会，其中的各种行为和言论都可能关涉国家的安危和社会的稳定，影响经济的发展与人民的福祉，因此，各国都不可能完全放弃管辖权，事实上也没有国家放弃对网络空间的管辖。例如，2000年雅虎

的拍卖网站为纳粹纪念品提供销售服务，法国认为该类销售在法国造成损害，指控雅虎向法国公民提供“一页又一页的德国纳粹党党徽袖章、纳粹党卫军匕首、集中营照片，甚至齐克隆（Zyklon）毒气罐的复制品”。法官判决雅虎拍卖网站违反了法国法律，判令该公司采取所有必要措施劝阻，并使法国网民不能访问该非法的雅虎拍卖网站。雅虎最后同意根据法院命令删除有关物品。[9]该判决结果表明，网络空间不是无主权论者所说的无主权管辖领域。

二 网络空间不属于全球公域

在古代英国法上，所谓公地（commons），是指村民共享的一片地带，不属于任何个人；无论是用于放牧或作为村广场，均是为了所有人的利益而共有。全球公域是公地在全球层面的延伸，是指超越国家主权和管辖范围之外，为使一切人共同受益而存在的区域，对其保护关乎全人类的利益。全球公域在国际法上的共同特点是独立于主权国家，强调其为全人类共同所有，排斥或禁止任何国家以任何方式对其主张主权权利。目前，国际社会对全球公域概念的界定不尽一致。例如，根据世界自然保护联盟于1980年发布的《世界保护战略：保护生物资源，实现可持续发展》的界定，全球公域包括公海及其生物资源、大气及气候、南极及其水域。[10]当前人们普遍认为，全球公域主要指那些国家管辖范围之外的自然资产，包括公海及其上空、外层空间和南极洲。

（一）网络空间全球公域说是对网络空间主权的否定

近年来，不断有人将网络空间视为第四大全球公域。如新美国安全研究中心（Center for a New American Security）的研究员亚伯拉罕·德马克（Abraham M. Denmark）认为，美国的地缘政治优势依赖于海洋、天空、太空和网络这些全球公域的开放。[11]2011年4月，北约的一个研究报告《确保进入全球公域》（Assured Access to the Global Commons）中所指的全球公域包括海洋、天空、太空和网络。[12]该报告认为，公海、国际空域、外层空间和网络空间相互联系，对于盟国的繁荣和安全非常关键；在当今世界，进入这些领域具有军事上和经济上的必要性，丧失进入的能力，将影响北约执行集体防御、危机管理和合作安全等关键核心任务。

由于美国的国家安全战略与全球公域高度关联，美国一直以来都极

力鼓吹网络空间全球公域说。美国战略界和决策层不断提及将网络空间作为全球公域，并强调网络空间对美国安全和防务的重要性。[13]

2005年美国国防部出台的《国土防御与民间支持战略》就将网络空间视为全球公域。[14]2008年4月，时任国防部长罗伯特·盖茨（Robert Gates）在空军战争学院的一次演讲中声称，“保护21世纪的全球公域——特别是太空和网络空间——已经成为美国的一项关键任务”。[15]2010年2月，美国国防部发布的《四年防务评估报告》将网络空间、海洋、天空、太空并列为四大公域。国防部长盖茨再次指出，美国必须做好准备应对一系列更为广泛的安全挑战；这些挑战包括使用先进的新技术来阻止美国军事力量进入海洋、天空、太空和网络空间等全球公域，以及非国家组织以更为狡猾和更具毁灭性的手段来袭击美国和制造恐怖。[16]2015年的美国《国家安全战略》中提出，“应当采取集体行动，确保对共享空间（sharing space）——网络、太空、天空、海洋——的进入。”[17]

美国之所以主张网络空间为全球公域，其主要原因在于：

第一，将网络空间视为全球公域有利于美国最大程度上开发利用网络空间。虽然理论上各国都可以自由进入、开发、利用全球公域，但全球公域向来都是有利于技术强国，不利于技术落后国家。只有掌握了必要技术的国家，才能够为了政治、经济、科学、文化以及军事目的而出入其中并加以开发利用。因此，只有海洋技术强国才能更好地开发利用公海资源，只有科技强国才有能力到南极洲开展科研，只有航空航天大国才有能力开发利用太空；反之，技术弱国很难开发利用全球公域。互联网诞生于美国，美国拥有世界上最为先进的网络信息技术和最强大的网络企业，将网络空间视为全球公域当然有利于美国最大程度上开发利用网络空间。

第二，将网络空间视为全球公域是为了否定他国网络空间主权以维护美国网络霸权。在全球公域中的行动能力最能体现一国的真正实力。近年来，美国不断鼓吹海上航行自由，就是为其全世界最强大的海军提供最大活动空间。网络全球公域说也是为其全世界最强大的网络技术寻求最大的发挥空间，是为了将美国的技术优势转化为美国在全球公域的行动自由，是美国确保其全球霸主地位的重要战略。全球公域的范围越大，美国的霸主地位就越强。美国实际上已经把网络空间的优势作为其全球霸主地位的支撑点之一。在2012年10月11日召开的“工商业主管与

国家安全事务”会议上，新任国防部长莱昂·帕内塔（Leon E. Panetta）强调：“过去，我们在陆地、海洋、空中和太空采取行动。进入新世纪后，美国军队还必须在网络空间协同保卫国家。”[18]

第三，将网络空间视为全球公域有利于以“互联网自由”为名推销美国价值观。网络空间是处理和分享信息的空间。网络空间信息自由与美式的言论自由观高度吻合，非常有利于美国价值观的输出。美国主张网络全球公域说，目的之一就是为了推销美式价值观，确保美国价值观能够无阻碍地通达世界。希拉里·克林顿在2010年1月“互联网自由”演说中强调，人人都有权通过各种媒体不受疆界限制地寻求、接收和传播信息和思想，并提出要创制国家间行为规则，鼓励对全球网络公域的尊重。[19]这显然是在为美国价值观的推销创造条件，是为了让美国在全球信息空间免受传统主权概念的束缚，扩张美国主权的应用范围，在网络世界拓展美国的国家利益。[20]

（二）网络空间不是独立于国家主权的全球公域

网络空间完全不同于传统上的全球公域，不属于全球公域，理由在于：

第一，网络空间不是“世外桃源”，而是根基于各国领土之上。传统的全球公域如公海及其上空、太空、南极等，都是在地理上独立于各国领土，形成一个不受任何主权国家排他性占有的独立物理空间。而网络空间在物理上是一个虚拟空间，本身不具有排他属性，并且如前所述，组成网络空间的物理设备设施及其上的软件和信息等，除了在公海或太空外，基本上是在各国领土之上，从而自然而然地在各国主权管辖之下。

第二，网络空间中的信息自由不是因为它是一个全球公域，而是因为各国免除或放松了信息出入境管制。在网络空间发展初期，网络的巨大影响力还未呈现，网络空间被认为是现实世界之外的虚拟空间，各国政府对网络空间的信息几乎不予干涉，从而造成网络空间为完全自由空间的假象。随着信息通信技术的进步和网络的普及，网络空间不再被认为是完全的虚拟空间，而是现实世界的一部分，传统法律自然而然地延伸适用于网络空间，国家主权也自然而然地延伸适用于网络空间。我们不能根据互联网发展初期的片面认识而想当然地、一成不变地认为网络空间是天然的自由之地、法外之地，是新的全球公域。特别是伴随互联

网兴起的网络安全问题日益突出和紧迫，对网络信息的管制成为网络治理的核心问题之一，各国都不可能奉行没有任何管制的信息自由。

第三，网络空间与传统全球公域最大的不同是网络空间具有社会性。公海、太空和极地等传统的全球公域不适合于人类生活甚至生存，因而没有普通社会公众长期居住，形成不了一个社会。就算在公海上航行的船舶、在天空中飞行的飞行器中有许多普通社会公众的存在，但其也只是将船舶或飞行器作为交通工具使用，或作为暂时的娱乐场地（如游船），而不是作为日常生活场所，自然不能形成稳定的社会。[21]网络空间则不同，全球已有超过30亿的网民参与其中，人们在网络空间中交流互动，形成了一个真正的社区或社会，构成现实社会的一部分。在这样一个有海量国民参与的社会空间中，各国都不可能放弃管辖权。网络主体在网络空间中享有权利的同时也应履行相应的义务，承担相应的法律责任。

第四，网络的互联互通性或无国界性并不意味着网络空间就是一个全球公域。网络空间的互联互通性或无国界性只是意味着各国政府、组织和社会公众要加强合作，共同治理网络空间；意味着各国对打击其领土上的网络犯罪等违法行为负有一定的国际义务和责任。因此，各国基于对网络空间的共享共治，应对其领土范围内的网络空间中的人、信息和行为等行使必要的管辖权。

值得注意的是，2017年2月出版的《可适用于网络行动的国际法的塔林手册2.0版》（简称“《塔林手册》2.0版”，Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations）第1条“主权（一般原则）”明确否定了网络空间“全球公域”说，认为“尽管（全球公域）定性在法律之外的方面可能是有用的，国际专家组并不接受这一定性，原因是它忽视了网络空间和网络行动那些涉及主权原则的地域属性”。[22]

总之，网络空间的现实性和社会性，决定了网络空间不是法外之地，是受法律管辖的空间。网络空间是构建在各国主权之上的电子空间，不是排除国家主权管辖的全球公域，因此应该尊重各国自主选择网络发展道路、网络管理模式、互联网公共政策的权利。

网络空间虽然不是全球公域，但互联网是当今最重要的全球性基础设施。以互联网为主要特征的信息革命带来了生产力的又一次质的飞

跃，[23]任何国家都不可能脱离网络空间而谋求发展与繁荣。同时，与网络空间相伴生的网络安全问题威胁着世界各国的安全和发展，任何国家都难以独善其身。可以说，互联互通的网络空间已经将各国结成了“网络空间命运共同体”。人类只有一个地球，各国共处一个网络。国际社会应本着“人类命运共同体”意识[24]，通过积极有效的国际合作，共同探讨和构建国际互联网治理体系，同舟共济，权责共担，增进人类共同利益。

三 确立网络法网络空间主权原则的必要性

经历了互联网发展早期“去主权化”之后，现实迫使人们呼吁国家主权在网络空间的“回归”。现在多数学者认为，网络虽然无国界，但是网络基础设施是处于一国境内，网民、网络公司等网络主体都是有国籍的，网络数据逐渐成为所在国的重要资源，基于网络而形成的网络社会是现实社会不可分割的部分，因此网络理所应当受到所在国的管辖，而不应该是法外之地，故而明确网络主权是非常有必要的。值得注意的是，各国虽然在网络主权的提法上各执己见，但在实践层面却无一例外对本国网络加以管理和保障，防止受到外部入侵和干涉。[25]

（一）国际上有关网络主权的主张

国际上有许多重要文件、文献论及网络主权。早在2003年12月12日，信息社会世界峰会第一阶段会议通过的《日内瓦原则宣言》强调“致力于坚持所有国家主权平等的原则”，并明确“与互联网有关的公共政策问题的决策权是各国的主权”。[26]2005年信息社会世界峰会第二阶段会议通过的《突尼斯议程》再次重申，“就涉及互联网的公共政策问题的决策权属国家主权。各国有权利和责任处理与国际互联网相关的公共政策问题。”[27]

2013年6月24日，第六十八次联合国大会发布了A/68/98号文件，通过了联合国“从国际安全的角度来看信息和电信领域发展政府专家组”所形成的决议。决议第20条内容是：“国家主权和源自主权的国际规范和原则适用于国家进行的信息通信技术活动，以及国家在其领土内对信息通信技术基础设施的管辖权。”[28]2015年7月22日第七十次联合国大会发布的A/70/174号文再次重申了上述内容。在方滨兴院士看来，

这一条款的本质就是承认国家的“网络主权”。这说明“网络主权”理念已被联合国所认可和接受，国家主权在网络行为上是行之有效的。[29]

2013年，北约卓越网络合作防卫中心国际专家组编写出版的《关于可适用于网络战的国际法的塔林手册》（简称“《塔林手册》1.0版”，Tallinn Manual on the International Law Applicable to Cyber Warfare）[30]，第1条“主权”规定：“一国有权对其领土内的网络基础设施和网络活动实施控制。”第2条“管辖权”规定：“在不妨碍承担相关国际责任的情况下，一国可管辖：（一）在其领土内实施网络行动的人员；（二）位于其领土内的网络基础设施；（三）符合国际法的域外管辖情形。”[31]2017年国际专家组编写出版的《塔林手册》2.0版第1条“主权（一般原则）”更加明确指出“国家主权原则适用于网络空间”。第2条“对内主权”明确，在不妨碍履行国际法律义务的情况下，国家对其领土上的网络基础设施、人和网络活动享有主权。[32]参与《塔林手册》2.0版起草的黄志雄教授认为，“作为我国网络主张基石的网络主权概念现在已经被国际上普遍接受，中国政府有关主权适用于网络空间的立场已经形成国际共识。”[33]

2015年1月，中国与俄罗斯等六国共同向联合国大会提出的《信息安全国际行为准则》[34]，“重申与互联网有关的公共政策问题的决策权是各国的主权。对于与互联网有关的国际公共政策问题，各国拥有权利并负有责任”；要求“遵守《联合国宪章》和公认的国际关系基本准则，包括尊重各国主权，领土完整和政治独立，尊重人权和基本自由，尊重各国历史、文化、社会制度的多样性等”。

综上所述，网络主权作为国家主权在网络空间中的延伸，已经在国际上被广泛接受。

（二）中国有关网络主权的主张

中国历来强调网络空间主权。2010年6月，中国公布的《中国互联网状况》白皮书指出：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。[35]

2014年7月16日，中国国家主席习近平在巴西国会演讲指出，“虽

然互联网具有高度全球化的特征，但每一个国家在信息领域的主权权益都不应受到侵犯，互联网技术再发展也不能侵犯他国的信息主权。”[36]2014年11月19日，习近平主席向首届世界互联网大会致贺词中就表示，“中国愿意同世界各国携手努力，深化国际合作，尊重网络主权，维护网络安全，共同构建和平、安全、透明的网络空间。”[37]2015年12月16日，习近平主席在第二届世界互联网大会开幕式主旨演讲中提出，推进全球互联网治理体系变革要坚持尊重网络主权原则，“应该尊重各国自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利，不搞网络霸权，不干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。”[38]

2015年7月1日通过的《国家安全法》第25条规定：“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。”这是我国第一次在法律上上使用了“网络空间主权”概念。2016年11月通过的《网络安全法》再次明确要维护网络空间主权。该法第1条规定：“为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。”

2016年7月27日，中办、国办发布《国家信息化发展纲要》，明确提出，要维护网络主权和国家安全；依法管理我国主权范围内的网络活动，坚定捍卫我国网络主权。2016年12月公布的《国家网络安全战略》对我国所持的网络空间主权立场进行了完整、全面的阐述。该战略指出，国家主权拓展延伸到网络空间，网络空间主权成为国家主权的重要组成部分。应当坚持尊重维护网络空间主权的原则。网络空间主权不容侵犯，尊重各国自主选择发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利。各国主权范围内的网络事务由各国人民自己做主，各国有权根据本国国情，借鉴国际经验，制定有关网络空间的法律法规，依法采取必要措施，管理本国信息系统及本国疆域上的网络活动；保护本国信息系统和信息资源免受侵入、干扰、攻击和破坏，保障公民在网络空间的合法权益；防范、阻止和惩治危害国家安全和利益的有害信息在本国网络传播，维护网络空间秩序。任何国家都不搞网络霸权、不搞双重标准，不利用网络干涉他国内政，不从事、纵容

或支持危害他国国家安全的网络活动。

总体而言，中国一直在国际上积极倡导网络空间主权，并不断明晰网络空间主权的内涵，成为中国开展国内网络空间治理、参与国际网络空间治理的法理基础。

（三）网络空间主权原则作为网络法基本原则的必要性

法律原则是指法律的根本准则，是指在一定法律体系中作为法律规则的指导思想、立法基础或本源的、综合的、稳定的法律原理和准则。法律的基本原则体现了法律的基本精神和根本价值，反映了法律的本质。网络法的基本原则是贯穿于网络法之中的、为网络法所固有并对网络法的创制和实施具有最高指导意义的根本准则，体现了网络法的立法宗旨和基本精神，是全部网络法规范的价值主线和灵魂所在。

之所以要将网络空间主权原则作为网络法的基本原则，主要是因为：

第一，网络的发展没有改变以《联合国宪章》为核心的国际关系基本准则，尊重国家主权是当今国际关系的基本准则，其原则和精神也应该适用于网络空间。全球互联网实际上是各国国家局域网的互联互通，网络空间具有国际性，网络法也就具有一定的域外性，一国网络法的实施不可避免地会对境外的网民访问境内的网站信息造成一定影响。这些影响都会映射到网络空间主权问题上来，因此，网络法必须对网络空间主权问题有一个明确的立场，即要尊重各国网络空间主权。

第三，网络空间主权是一国网络立法、执法、司法的基石，也是一国实施网络治理的前提和基础。在现实世界中，各主权独立国家的立法、执法、司法都是基于一国主权而实施的，不容他国任意干涉。网络空间也是一样，各国基于国家主权对其领土上的网络设施、网民、网络活动、网络信息进行管理，是行使网络空间中的国家主权的体现。网络法应当对此予以确认。

第三，当前阶段，一些网络霸权国家在战略上把网络空间当作全球公域，强调网络空间中的行动自由，甚至利用技术优势肆意监视其他国家和政府领导人活动；一些国家基于自己的价值观和意识形态，推行所谓的“互联网自由”，利用网络手段进行意识形态渗透，甚至意图颠覆他国政府。因此，网络法尤其要强调网络空间主权原则，抵制他国利用

网络实施损害我国主权、政权的行为。

第四，从近年来的国家和国际实践来看，一些国家虽然没有明确承认网络空间主权，但无一例外地在法律上和实践中行使着网络空间主权。其实，明确网络空间的主权原则，既能体现各国政府依法管理网络空间的责任与权利，也有助于推动各国构建政府、企业和社会团体之间良性互动的平台，为信息技术的发展以及国际交流与合作营造一个健康的生态环境。[39]习近平主席在第三届世界互联网大会上的贺词再次强调，应“坚持网络主权理念，推动全球互联网治理朝着更加公正合理的方向迈进”。[40]

四 网络空间主权原则在网络法中的体现

所谓网络空间主权，简单来讲，就是一国国家主权在网络空间中的自然延伸和表现。[41]对内而言，网络空间主权指的是国家独立自主地选择本国网络发展道路、网络管理模式、互联网公共政策，不受外部干涉；对外而言，网络空间主权指的是一国平等地参与网络空间国际治理，防止本国互联网受到外部入侵和攻击。网络主权是一国国家主权不可分割的组成部分，是国家主权的应有之义，不是与传统国家主权并行的事物。

对于网络空间主权的内容，可以从传统国家主权的管辖权、独立权、防卫权、平等权等四个方面进行引申理解，但与传统国家主权的内涵相比，网络主权存在一些特殊之处。

（一）管辖权

管辖权是指国家对它领土内的一切人（享有外交豁免权的人除外）和事物以及领土外的本国人实行管辖的权力，同时有权按照自己的情况确定自己的政治制度和社会经济制度。对网络空间而言，管辖权指的是主权国家对本国境内的网民、网络设施、网络活动、网络信息和领土外的本国网民实行管辖的权力。基于网络主权，一国有权制定适用于本国的网络法律法规和政策，依法采取必要措施，管理本国信息系统及本国疆域上的网络活动；有权决定境内的网络是否接入国际互联网，境外的网站是否可以在境内被访问；可以禁止不服从本国法律法规的网站在境内提供服务；可以对网络空间的谣言、诈骗等非法信息传播进行必要的

管制；对网络违法犯罪行为有权行使行政、司法管辖权；等等。例如，我国《网络安全法》第2条明确规定：“在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。”这就是通过立法明确网络管辖权。《国家安全法》第25条也规定，要加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

在网络管辖权方面，对网络信息的管辖权争议较大。在互联网发展初期，各国对网络信息通常采取不管制或放松管制的政策，这让人们觉得网络信息绝对自由是天经地义的事情；随着互联网全面渗透到政治、经济、社会的方方面面，非法和不良网络信息也越来越多，使得对网络信息和网络舆情的治理成为各国政府的重要课题。我国基于本国法律对谷歌等不遵守我国有关网络信息法律的网站进行限制，正是行使网络空间管辖权的具体体现。一些西方国家主张的所谓“互联网自由”，就是要否定他国对网络信息的管辖权和治理权，让网络空间成为网络技术霸权国家畅通无阻的全球公域。

（二）独立权

独立权是指一国完全独立自主地行使权力，排除外来干涉，无须受制于别国。传统的国家主权“含有全面独立的意思，无论在国土以内或在国土以外都是独立的”。[42]由于互联网是全球性网络，各国的网络依赖互存，任何国家的网络都只是国际互联网的一部分；如果一国的网络不与他国的网络互联互通、完全独立运行，就只能是一国局域网了。因此，一国的网络要达到完全意义上的独立是不现实的，只能是相对的独立。但网络主权应当是独立的，即：一国网络除了应遵守该国认可的统一技术标准和国际规则外，不应受制于个别国家的支配。任何国家都不得搞网络霸权，不得利用网络干涉他国内政，不得从事、纵容或支持危害他国国家安全的网络活动。

目前，由于历史和技术原因，全球13台域名根服务器中美国境内有10台，只要美国在根服务器上屏蔽某一国家的域名，就能让这个国家的顶级域名网站在网络上瞬间“消失”。美国曾在战争的特殊时间里清除过伊拉克、利比亚的国家根域名，使得这两个国家的全部网站从国际互联网上消失。在这个意义上，美国具有全球独一无二的制网权，有能力威慑他国的网络主权。因此除了美国以外的其他各国的网络还无法实现

完全的独立存在。要实现各国网络的独立权，就要将互联网的根服务器交给一个像联合国一样的国际机构管理。

我国一直致力于推动由联合国来负责接管互联网名称与数字地址分配机构（ICANN）的职能，但美国极力反对。2016年10月1日，美国商务部下属机构国家电信和信息管理局（NTIA）被迫结束与互联网名称与数字地址分配机构之间的授权合同，把对互联网数字地址分配机构（IANA）的管理权完全移交给位于加利福尼亚州的互联网名称与数字地址分配机构（ICANN）。IANA管理权的移交客观上有助于各国网络摆脱美国的控制，走向更加独立。

（三）防卫权

防卫权是指国家为维护政治独立和领土完整而对外来侵略和威胁进行防卫的权力。网络领域的防卫权主要指的是主权国家具有对外来网络攻击和威胁进行防卫的权力。网络攻击造成的损害已经不亚于传统战争，甚至比传统战争造成的损害更大。2007年5月，爱沙尼亚受到大规模病毒攻击，导致整个政府网络几乎关闭。[43]2010年，“震网”病毒导致伊朗布什尔核电站无法正常工作。2010年5月，美国最先设立网络司令部，组建训练网军。这些事例已经警示人们网络战时代已经来临。2013年，美国棱镜门计划曝光，美国利用自身技术优势对他国民众、国家领导人实施监视、监听。此外，有的国家利用自身的信息优势和技术优势针对他国开展网络舆论攻势和意识形态输出，发动“颜色革命”，利用网络颠覆他国政权。总之，防卫权要求主权国家要设置网络疆界、网络边防，要有预防、监测、抵御和反击境外网络进攻的能力。

在网络防卫权方面，我国《网络安全法》第3条、第5条明确规定，国家坚持网络安全与信息化发展并重，建立健全网络安全保障体系，提高网络安全保护能力；国家采取措施，监测、防御、处置来源于中国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏。《国家安全法》第25条也明确规定国家要建设网络与信息安全保障体系，提升网络与信息安全保护能力，维护国家网络空间主权、安全和发展利益。

（四）平等权

平等权是指主权国家不论大小、强弱，也不论政治、经济、意识形

态和社会制度有何差异，在国际法上的地位一律平等。国际上，国家间关系的特征是平等和独立。[44]网络领域的平等权主要指的是各国的网络之间可以平等地进行互联互通，各国享有平等参与国际网络空间治理的权利。由于互联网是美国发明的，其他国家的网络都是后来接入到美国互联网上的，美国对互联网的掌控具有天然的绝对优势，其他国家则明显处于弱势地位，因而在能力上难以平等地参与国际网络空间治理。如何重构国际网络空间治理模式、保障各国平等参与网络治理，已经成为当前面临的重要任务。

我国《网络安全法》第7条规定，国家积极参与网络空间治理国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。上述国际网络空间治理体系的构建都应是建立在主权平等原则的基础上，否则不可能实现。

五 结语

我国《国家网络空间安全战略》指出，网络空间已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域，国家主权拓展延伸到网络空间，尊重网络空间主权正在成为国际社会共识。网络法贯彻网络主权原则，是实现网络空间依法有效治理的前提，是构建清朗网络空间的法律保障，有助于实现信息自由流动与维护国家安全、公共利益的有机统一。今后新出台的网络立法，都应当坚持网络空间主权原则。

---

[1] 本章系国家242项目“中美对全球网络治理规范的合作战略研究”（2016A153）的阶段性成果。

[2] John Perry Barlow，A Declaration of Independence of Cyberspace，https：//www.eff.org/cyberspace-independence.

[3] C.E.Shannon，“A Mathematical Theory of Communication”，The Bell System Technical Journal，vol.27 （1948），pp.379-423.

[4] 核苷酸（Nucleotide）是一类由嘌呤碱或嘧啶碱、核糖或脱氧核糖以及磷酸三种物质组成的化合物，它是核糖核酸及脱氧核糖核酸的基

本组成单位，是遗传信息的载体。含特定遗传信息的核苷酸序列，是遗传物质的最小功能单位。除某些病毒的基因由核糖核酸（RNA）构成以外，多数生物的基因由脱氧核糖核酸（DNA）构成，其中带有遗传信息的DNA片段称为基因。参见百度百科“核苷酸”、“核糖核酸”、“脱氧核糖核酸”词条。

[5] 神经元，又称神经元或神经细胞，是构成神经系统结构和功能的基本单位。神经元有接受、存储、整合和传递信息的功能。参见百度百科“神经元”词条。

[6] 杨学山：《科学揭示信息定义和发展规律》，《中国信息安全》2016年第4期。

[7] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，p.15.

[8] 郭玉锦、王欢：《网络社会学》，中国人民大学出版社，2010，第12页。

[9] Jack Goldsmith & Tim Wu，Who Controls the Internet? Illusions of a Borderless World，Oxford University Press，2006，pp.5-6.

[10] International Union for Conservation of Nature and Natural Resources，World Conservation Strategy：Living Resource Conservation for Sustainable Development，
https：//portals.iucn.org/library/efiles/documents/WCS-004.pdf.

[11] Abraham M. Denmark，Asia’s Security and the Contested Global Commons，Strategic Asia 2010-11：Asia’s Rising Power and America’s Continued Purpose，
http：//www.nbr.org/publications/strategic_asia/pdf/Preview/SA10/SA10_G

[12] Mark Barrett，Dick Bedford，Elizabeth Skinner，Eva Vergles，Assured Access to the Global Commons，3 Apr. 2011，

http：//www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf

[13] 马建英：《美国全球公域战略评析》，《现代国际关系》2013年第2期。

[14] US Department of Defense，Strategy for Homeland Defense and Civil Support，http：//digital.library.unt.edu/ark：/67531/metadc22361/m2/1/high_res_d/I2005_10389.pdf （“This active，layered defense is global，seamlessly integrating US capabilities in the forward regions of the world，the global commons of space and cyberspace，in the geographic approaches to US territory，and within the United States”）.

[15] Secretary of Defense Gates’Speech at Air War College，http：//www.cfr.org/world/secretary-defense-gates-speech-air-war-college/p16085.

[16] U. S. Department of Defense，DoD News Briefing with Secretary Gates and Adm.Mullen from the Pentagon，February 1，2010，http：//archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=4549.

[17] The White House，National Security Strategy，Feb. 2015，https：//www.whitehouse.gov/sites/default/files/docs/2015_national_security

[18] Leon E. Panetta，Defending the Nation from Cyber Attack（Business Executives for National Security，New York，October 11，2012），http：//www.bens.org/document.doc? id=188.

[19] Hillary Rodham Clinton，Remarks on Internet Freedom，http：//www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm，2015-11-24.

[20] 沈逸：《美国国家网络安全战略》，时事出版社，2013，第253页。

[21] 值得注意的是，这些船舶或航空器通常是有国籍的，国籍国对其有管辖权，不是国家主权之外的公域。

[22] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，p.12.

[23] 习近平：《在网络安全和信息化工作座谈会上的讲话（2016年4月19日）》，http：//news.xinhuanet.com/newmedia/2016-04/26/c_135312437.htm。

[24] 《胡锦涛在中国共产党第十八次全国代表大会上的报告》，中国政府网，http：//news.china.com.cn/politics/2012-11/20/content_27165856_8.htm。

[25] 若英：《什么是网络主权？》，http：//news.xinhuanet.com/politics/2014-07/10/c_126736910.htm。

[26] WSIS，Declaration of Principles（WSIS-03/GENEVA/DOC/4-E），para.49（a）（“Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues”），http：//www.itu.int/net/wsis/docs/geneva/official/dop.html.

[27] WSIS，Tunis Agenda for the Information Society（WSIS-05/TUNIS/DOC/6（Rev.1）-E），para. 35（a）（“Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues”），http：//www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[28] United Nations General Assembly，Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security（A/68/98），para.20 （“State sovereignty and international norms and principles that flow

from sovereignty apply to State conduct of ICT-related activities，and to their jurisdiction over ICT infrastructure within their territory”）.

[29] 方滨兴：《从“国家网络主权”谈基于国家联盟的自治根域名解析体系》，http：//blog.sina.com.cn/s/blog_7110463b0102v75z.html。

[30] Michael N. Schmitt （ed.），Tallinn Manual on the International Law Applicable to Cyber Warfare，Cambridge University Press，2013.国内有的翻译为《塔林网络战国际法手册》。

[31] 北约卓越网络合作防卫中心国际专家小组编《塔林网络战国际法手册》，朱莉欣等译，苏金远等审校，国防工业出版社，2016，第2～5页。

[32] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp.11，13.

[33] 刘璐：《塔林手册2.0第一次有了中国专家的声音，九个问题让你认识它》，http：//www.jfdaily.com/news/detail? id=45198。

[34] 2011年9月12日，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦常驻联合国代表联名致函联合国秘书长潘基文，请其将由上述国家共同起草的“信息安全国际行为准则”作为第六十六届联大正式文件散发。2015年1月9日，中国、哈萨克斯坦、吉尔吉斯斯坦、俄罗斯、塔吉克斯坦、乌兹别克斯坦常驻联合国代表联名致函联合国秘书长潘基文，请其将由上述国家共同提交的“信息安全国际行为准则”更新草案作为第六十九届联大正式文件散发。

[35] 《〈中国互联网状况〉白皮书》，新华网，http：//news.xinhuanet.com/politics/2010-06/08/c_12195221_6.htm。

[36] 《习近平在巴西国会的演讲》，新华网，http：//news.xinhuanet.com/world/2014-07/17/c_1111665403.htm。

[37]《习近平致首届世界互联网大会贺词》，新华网，http：//news.xinhuanet.com/live/2014-11/19/c_127228771.htm。

[38]《习近平在第二届世界互联网大会开幕式上的讲话》，新华网，http：//news.xinhuanet.com/world/2015-12/16/c_1117481089.htm。

[39]《外交部副部长李保东：维护网络空间应把握好四大原则》，人民网，http：//world.people.com.cn/n/2014/0606/c1002-25111773.html。

[40]《习近平在第三届世界互联网大会通过视频发表讲话》，正义网，http：//www.jcrb.com/xztpd/2017/201704/XJPJH_46291/419tpjj/201704/t2

[41] 若英：《什么是网络主权？》，http：//news.xinhuanet.com/politics/2014-07/10/c_126736910.htm。

[42]〔英〕詹宁斯、瓦茨修订《奥本海国际法》，王铁崖等译，中国大百科全书出版社，1995，第92页。

[43] 亨利·凯尼恩（Henry S.Kenyon）：《揭秘2007年爱沙尼亚遭大规模网络攻击事件始末》，http：//www.china.com.cn/military/txt/2009-11/20/content_18927324.htm。

[44]〔英〕詹宁斯、瓦茨修订《奥本海国际法》，王铁崖等译，中国大百科全书出版社，1995，第94页。

第七章

数据主权的必要谦抑：以《网络安全法》数据境内留存规定为例

中国提出网络主权观，遵循了其对自身与国际社会之间权责关系一贯的认识和定位。……如果说，中国不希望颠覆已有的世界秩序是国际共识的话，那对中国意图分裂互联网的担心，也就显得有些多余。

目前，网络主权已经得到各国的广泛接受，哪怕有些国家仅仅是“只做不说”。通说认为，网络主权同时具有对内和对外两个面向：在对内实施时，网络主权具有最高权威，任何其他国家不得干涉，在对外时，网络主权意味着国与国之间形式和实质上的平等。上述两个面向，用中国国家主席习近平的话来概括，即为“尊重各国自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利，不搞网络霸权，不干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动”[1]。

但对内的最高权威是否意味着网络主权不受任何限制？以数据为例，根据网络主权对内具备最高权威的题中之意，一国有权按照自我意志，自主、自由地规制境内收集和产生的数据，亦即通常所称的“数据主权”。而数据主权表现最为强烈的形式，即是要求在其境内收集和产生的数据只能存储在境内，不得流到境外。但在互联网时代，数据天然地跨国界流动，数据因流动而获得价值，数据流能引领技术流、资金流、人才流，已经成为基本共识。[2]数据本地化存储要求似乎与之背道而驰。反对数据本地化存储的人不仅将其看成贸易壁垒，甚至上升到破坏互联网全球互联互通的特性，进而推翻现有世界秩序的高度。[3]

因此，网络主权在对内享有最高权威的同时是否需要受一定限制的这个理论难题，我国政府和学者迄今为止多未触及。这也在一定程度上使得不少西方国家和学者认为，一旦中国强调网络主权，强调自主对境内的网络发展、网络管理、公共政策等作出规定，很有可能意味着中国正在将自身从全球统一的互联网中割裂开，而且还可能将对开放、自由、互联互通的互联网，以及对基于互联网的信息自由流动，造成严重威胁。[4]因此，在许多国际场合，批评中国网络主权的言论层出不穷。

为了使得我国高举的网络主权大旗具备理论上的自洽，本章拟探讨网络主权在对内行使时应具备的谦抑性。由于网络主权包罗万象，本章选取数据主权作为案例研究，以期做到深入。具体来说，本章提出应当从一个国家所处的历史和发展阶段，来充分认识包括数据主权在内的网络主权所应当发挥的作用。就我国而言，数据主权应当同时承担促进国家发展和国家安全的双重目的。以此为指导思想，本章聚焦《网络安全法》第37条规定的数据本地化存储要求，探讨如何通过制度设计，实现发展和安全之间的平衡。在探讨过程中，本章希望能厘清数据主权应当具备的必要谦抑，为解答网络主权行使过程中应当遵循的原则提供一定的基础。

一 网络主权在特定历史阶段的作用

首先，中国的网络主权观延续了中国对现实世界国际关系的立场。如果将习近平主席对网络主权的概括中“网络”两字删除，就可得到中国对国际关系中国家主权的基本看法。中国没有对网络主权做出任何超出传统主权概念的阐述。因此，中国提出网络主权观，遵循了其对自身与国际社会之间权责关系一贯的认识和定位。对中国领导人来说，将主权概念延伸至网络空间是一种逻辑上的必然。如果说，中国不希望颠覆已有的世界秩序是国际共识的话，那对中国意图分裂互联网的担心，也就显得有些多余。

其次，我们不应该忽视，中国政府领导层在强调网络主权的同时，对中国现在所处的发展阶段和政府的历史使命有着非常清醒的认识。在第二届世界互联网大会开幕式致辞时，习总书记首先强调的是，“我们的目标，就是要让互联网发展成果惠及13亿多中国人民，更好造福各国人民。”[5]在“4·19”讲话中，习总书记开宗明义地提出了中国互联网的发展必须坚持“以人民为中心”这样的理念。[6]

因此，应当认识到中国领导人将发展作为第一要务，网络主权是为了发展而服务。倡导网络主权，对内是为了保障中国能够自主地根据自己的情况制定发展互联网的政策和计划，对外是为了争取平等地参与互联网治理的权利和地位，以此让网络空间秩序朝着更加公平、公正的方向发展。

也就是说，就我国而言，包括数据主权在内的网络主权，应当同时承担促进国家发展和国家安全的双重目的。这也是为什么习近平总书记在“4·19”讲话中，是在论述“安全和发展”的关系时提到了网络主权。

二 数据主权最强烈的表现形式——数据的本地化存储

数据本地化存储（data localization），与数据跨境流动相对，指的是一国政府制定政策或规则，限制数据流出国境。[7]

在我国现行法律体系中，数据本地化存储要求并非没有先例。国务院2013年发布的《征信业管理条例》、国家卫生计生委2014年发布的《人口健康信息管理办法（试行）》、中国人民银行2011年发布的《关于银行业金融机构做好个人金融信息保护工作的通知》、国家新闻出版广电总局、工业和信息化部2016年发布的《网络出版服务管理规定》等，都对数据本地化提出了明确要求。[8]与上述限于具体部门或行业的规定不同，《网络安全法》因其“网络空间基本法”的地位，统筹性地对数据本地化做出了一般性规定，[9]受到国内外各界的广泛关注。

2016年8月11日英国《金融时报》报道，美、日、欧40余个行业组织发起“自2010年以来向中国领导层的最大交涉”，呼吁中国政府修订新的网络安全法等，“他们的担忧集中于中国新法规的某些内容，包括迫使境外公司将数据存储在中国境内”，并“警告这些法律法规对经济增长构成保护主义威胁，将进一步使中国孤立于全球数字经济以外”。[10]此外，2015年和2016年连续两年，美中贸易全国委员会对成员企业的调查和访谈均发现，中国政府的数据本地化存储要求是让在华经营的美国企业最为担忧的事项。[11]

实际上除中国外，国际上还有不少国家都或多或少地做出了数据本

地化的要求。[12]数据本地化一定是实现了什么价值，否则为何采取本地化措施的既有发达国家，也有发展中国家，且地域上遍布各个大洲？如果数据本地化确实起到了某些作用，又应该如何确保其不矫枉过正？换言之，数据本地化存储的合理界限在哪里？

为此，本章第三部分将归纳中外现有的数据本地化存储规定和实践。第四部分介绍国际上对数据本地化存储的主要反对意见。从第五部分开始将是本章的独创性贡献所在：第五部分将提出描述数据本地化存储的严苛度模型，以此作为度量各个国家本地化实践的标尺，由此指出数据本地化措施存在一种光谱式的渐进，严苛程度各不相同；第六部分将讨论数据本地化存储所实现的目的；第七部分将提出目的与手段之间在适当性和必要性上的应然关系；第八部分将从“数据本地化存储的合理界限理论”出发，检视《网络安全法》第37条的数据本地化存储规定，并给出基本评价；因第37条要求“国家网信部门会同国务院有关部门制定‘数据跨境安全评估’的办法”，本章最后一部分将以“数据本地化存储的合理界限理论”为主体，提出数据跨境安全评估办法的总体框架，为立法提供支撑或参考。[13]

三 数据本地化存储的中外实践

1. 中国现行规定和立法建议

我国现行主要的数据本地化存储的规定，主要分布在金融、卫生医疗、交通领域（见表7-1）。目前，金融行业中另外一项数据本地化立法草案是中国保险监督管理委员会2015年10月的《保险机构信息化监管规定（征求意见稿）》。其中第31条规定，“数据来源于中华人民共和国境内的，数据中心的物理位置应当位于境内。”第58条还规定，“外资保险机构信息系统所载数据移至中华人民共和国境外的，应当符合我国有关法律法规。”[14]

表7-1 中国关于数据本地化存储的现行规定

规定名称	具体要求
国务院2013年《征信业管理条例》②	第二十四条　征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。
国务院2015年《地图管理条例》③	第三十四条　互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并制定互联网地图数据安全管理制度和保障措施。
国家卫生计生委2014年《人口健康信息管理办法（试行）》④	第十条　不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。
中国人民银行2011年《关于银行业金融机构做好个人金融信息保护工作的通知》⑤	六、在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。

② 《征信业管理条例》，http://www.gov.cn/flfg/2013-01/29/content_2323780.htm。

③ 《地图管理条例》，http://www.gov.cn/zhengce/content/2015-12/14/content_10403.htm。

④ 国家卫生计生委：《人口健康信息管理办法（试行）》，http://www.nhfpc.gov.cn/guihuaxxs/s10741/201405/783ec8adebc6422bbebdf79db3868d0b.shtml。

⑤ 《关于银行业金融机构做好个人金融信息保护工作的通知》，http://www.gov.cn/gongbao/content/2011/content_1918924.htm。

表7-1 中国关于数据本地化存储的现行规定-续表

规定名称	具体要求
国家新闻出版广电总局，工业和信息化部2016年《网络出版服务管理规定》①	第八条　图书、音像、电子、报纸、期刊出版单位从事网络出版服务，应当具备以下条件：（三）有从事网络出版服务所需的必要的技术设备，相关服务器和存储设备必须存放在中华人民共和国境内。
中国保险监督管理委员会2011年《保险公司开业验收指引》②	“三、开业验收标准”中的“（九）信息化建设符合中国保监会要求”规定：“业务数据、财务数据等重要数据应存放在中国境内，具有独立的数据存储设备以及相应的安全防护和异地备份措施。”
交通部、工信部、公安部、商务部、工商总局、质检总局、国家网信办2016年《网络预约出租汽车经营服务管理暂行办法》③	第二十七条　网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于2年，除法律法规另有规定外，上述信息和数据不得外流。

① 工业和信息化部：《网络出版服务管理规定》，http://www.miit.gov.cn/n1146290/n4388791/c4638978/content.html。

② 中国保监会：《关于印发〈保险公司开业验收指引〉的通知》，http://www.circ.gov.cn/web/site0/tab5225/info163158.htm。

③ 交通运输部：《网络预约出租汽车经营服务管理暂行办法》，http://zizhan.mot.gov.cn/zfxxgk/bnssj/zcfgs/201607/t20160728_2068633.html。

在电信行业，据在华经营的外企反映，实践中申请ICP备案或许可，工信部门会要求组织机构在中国境内设置服务器，因此也在事实上构成数据本地化存储的要求。[15]

近期，最受关注的当属《网络安全法》对数据本地化存储的规定。第37条要求：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”这是我国第一次跨行业对数据本地化存储做出统一规定。

2. 域外数据本地化要求概述

据统计，目前全球有超过60个国家做出了数据本地化存储的要求。[16]如图7-1所示，这些国家遍布各个大洲，既有加拿大、澳大利亚、欧盟等发达国家和地区，也包括俄罗斯、尼日利亚、印度等发展中国家。[17]图中颜色越深，[18]则显示数据本地化存储的要求越严格。[19]

图7-1 数据本地化规定严苛程度

资料来源：Albright Stonebridge Group，“Data Localization：A Challenge to Global Commerce and the Free Flow of Information”，Sep. 2015，p.5.http：//www.albrightstoneb-ridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf.

现有的数据本地化存储规定，大多数是在2000年后做出的。[20]从图7-2可以发现很有趣的一点：数据本地化存储的兴起，恰恰与以互联网为代表的信息技术发展同步。在单PC机时代，数据直接存储在电脑的

硬盘上。在网络技术发展的早期，组织机构中的多个桌面终端连接一台服务器，数据统一存储在自有的服务器上。在这两个阶段，数据占有者能很好地控制数据的流向、存储地点、访问、处理等，对数据的控制能力最为完整。

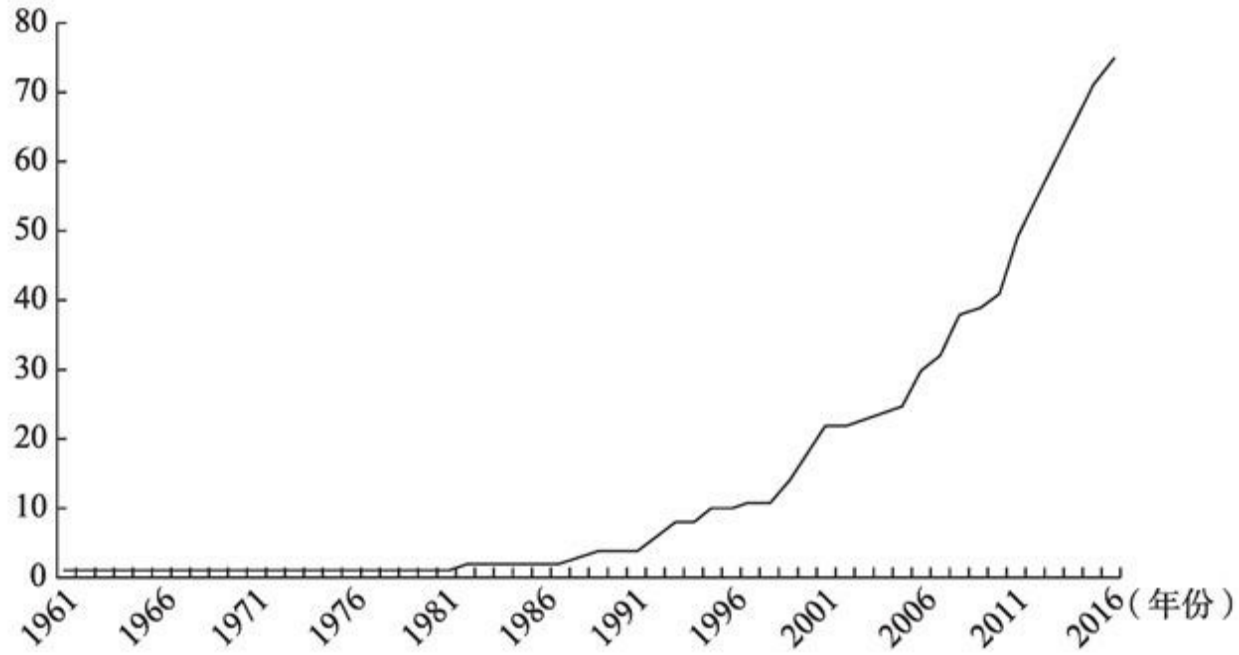

图7-2 数据本地化措施的演变发展*

资料来源：Martina Francesca Ferracane，Data Localization Trends，European Centre for International Political Economy，Presentation in Beijing，19 July 2016（内部研讨会）。

*该图的纵坐标代表采取数据本地化措施的国家数量。

云计算的普及，削弱了数据占有者的控制能力。一般来说，大型云服务商在不同国家和地区都设立了数据中心；组织机构租用云服务，虽然仍控制着对数据的访问和处理，但在通常情况下已经不能控制也无法得知数据的物理存储位置了。[21]与前两阶段相比，数据占有者与数据之间多出了一个“中间人”——云服务提供商。数据占有者要实现对数据的控制，取决于这位“中间人”是否忠实地承担自己代理人的角色。

大数据技术的发展，则在另外一个层面大大增强了数据占有者对数据控制的需求。一旦海量数据对外界披露，无论是主动的共享开放，还

是信息系统被攻破而导致的数据被动泄露，都可能被恶意使用。例如，敌对势力将海量数据与其他数据集组合，用各种算法进行数据挖掘等，可以分析掌握能威胁国家安全的信息。

可以看到，一方面，数据占有者控制数据的能力在削弱，中间环节在增多；另一方面，对数据加强控制的需求在不断增长。因此，在一定程度上，数据本地化存储体现了数据占有者面对上述两难时的一种反应。[22]

四 对数据本地化存储的反对意见

首先是在经济方面。有不少论者提出，数据本地化存储与现今全球经济中信息、资本、技术、人才高速流动的现实格格不入，将会严重影响效率，并减缓产业发展、技术进步等。欧洲国际政治经济研究中心（ECIPE）发布的一系列研究报告提出，采用数据本地化存储措施会对一国实际GDP（Real GDP）造成损失，如本地化将导致欧盟、印度、中国分别损失GDP的0.48%、0.25%和0.55%。[23]有学者对俄罗斯数据本地化存储措施进行专题研究后得出结论：俄罗斯的GDP将因此降低0.27%[24]。还有论者指出，一些国家采用数据本地化存储规定，目的在于打击美国IT巨头的竞争优势，扶持国内产业和企业，提高国内就业，[25]实际上构成了一种严重的数字贸易壁垒。[26]

其次是在互联网技术现实方面。有论者指出，强制数据存储于境内，违背互联网设计的初衷，进而可能破坏开放、互通的互联网架构。互联网治理全球委员会（Global Commission on Internet Governance）2016年6月发布的最终报告《统一的互联网》（One Internet）指出，数据在互联网上传输遵循效率原则，并不考虑国境因素，而人为施加地域限制，将会“动摇互联网基础架构的稳定性”。[27]还有论者指出，数据本地化存储的要求，本质上与信息技术发展的逻辑相冲突，例如云计算、大数据、物联网（the Internet of Things）。[28]以大数据为例，强制数据本地化存储，就意味着数据不能离开本地，而只能将所有域外的数据传输至本地，才能实现组合，同时如果其他国家或地区也设定了类似的数据本地化要求，则得以汇聚在一起的数据总量将会降低，大数据能发挥的效用也将随之减少。[29]

再次是在互联网治理乃至世界秩序方面。有论者指出，强制数据存

储在本地，是国家不顾技术现实和世界潮流，强行将数据纳入主权管控之下，这一点中国、俄罗斯等金砖国家表现得尤为积极。这些国家试图打造具有体现金砖国家特色的互联网，将会最终导致互联网的分裂，即巴尔干化。[30]还有很多论者进一步将数据本地化存储视为网络主权的具体表现形式之一，进而将网络主权与以多利益攸关方模式（multi-stakeholder model）为代表的全球互联网治理之间的冲突，当成中俄与美西方争夺世界秩序领导权的缩影之一。[31]

五 构建“数据本地化存储合理界限理论”之一——数据本地化存储严苛度模型

由前两个部分可知：一方面，随着信息技术的进步，数据本地化存储似乎正得到越来越多国家的青睐；另一方面，国际舆论和大量的学术研究却又极力反对本地化措施。正是在这种实践和认识之间巨大的错位之中，我国《网络安全法》的有关规定备受争议。

如何弥合现实中行为和认知之间的差距？本章提出以下建议：首先，无论是学者，还是决策者，都应当看到数据本地化存储措施是一个光谱式的存在，两端的本地化措施严苛程度截然不同；认识到这一点后，不仅学者在研究时能够避免泛泛而谈，决策者在选择政策工具时也能够更加准确、精细，而且双方在讨论时能够做到真正的聚焦。

其次，需要仔细探讨数据本地化存储能够实现哪些目标。就目的和手段之间的关系来说，这一点尤为重要。目的是判断手段适当性和必要性[32]的根本依据。目的一旦确定，就能据此选择严苛程度不同的数据本地化存储措施作为实现目的的手段。

换言之，本章希望通过讨论手段（数据本地化措施严苛程度）、目的（数据本地化措施能够实现的目标），以及目的和手段之间的适当性和必要性关联，为数据本地化存储提供一套具有合理性的评价标准，并以此标准检视现实中采用的本地化措施，最终实现依法治理数据化本地化存储，给其设定合理界限，在政府管制与信息自由之间，在多元价值碰撞时，实现一种平衡。这也是本章余下内容的主旨。

具体到本部分对手段的讨论，目前，已有文献大都未对数据本地化存储严苛程度进行准确描述。[33]本章从各国现行措施中抽象出四个维

度作为构建严苛度模型的指标：本地化存储的实施主体、本地存储彻底程度、本地化存储覆盖的数据范围、本地化存储的豁免条件。

之所以抽象出这四个指标，首先是因为从逻辑上来说，任何本地化措施都必然包含这四个维度。其次，不同国家在这四个维度做出不同的选择，就构成了不同严苛程度的数据本地化措施。本章将在第六部分详细分析我国《网络安全法》在这四个维度上做出的具体选择。

1. 本地化存储的实施主体

按照学者曹磊的看法，数据权利有两类主体——国家和公民。国家拥有数据主权，因此能“独立自主对本国数据进行管理和利用”。[34]而“数据权利的另一主体是公民，是相对应公民数据采集义务而形成的对数据利用的权利，这种对数据的利用又是建立在数据主权之下的。只有在数据主权法定框架下，公民才可自由行使数据权利”。[35]

现在对上述分析框架稍作修正：在宏观层面，国家依主权，划定其有权管辖的数据范围，并设定对数据管理和利用的法定框架。例如一国制定个人信息保护方面的法律，在法律中分别设定数据主体（亦即普通个人）、数据控制者（亦即收集、使用、披露个人信息的组织、机构、个人）及其他相关方的权利和义务。在微观层面，数据主体、数据控制者及其他相关方在国家设定的法定框架下，根据国家赋予的各自权利义务互动、协商，在不同场景中形成一项项具体的数据处理安排。聚焦到数据本地化存储，具体场景中，数据是否在本地存储或传输到境外，由数据主体、数据控制者及其他相关方自主协商决定，国家并不直接介入。如图7-3所示。

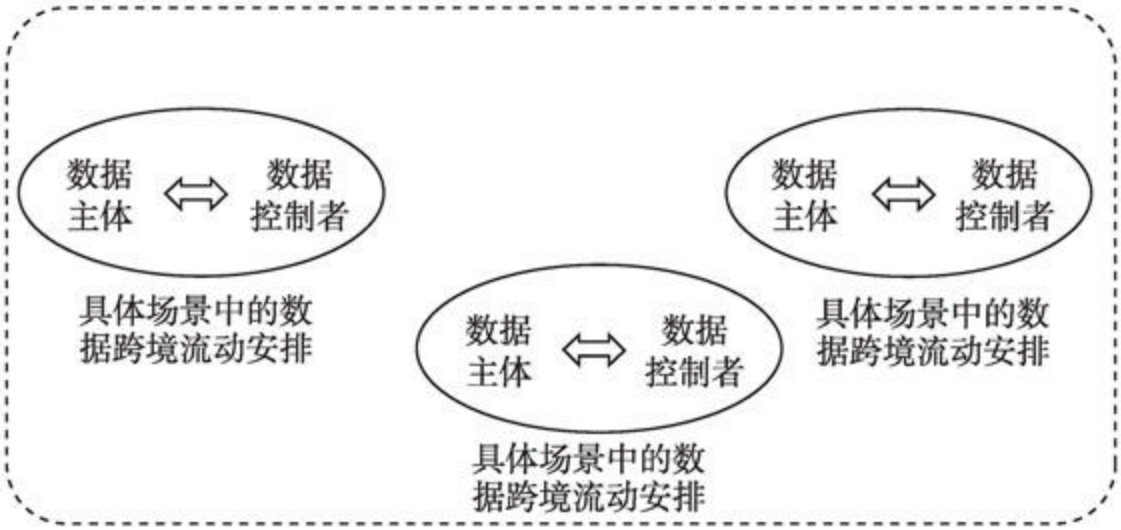

图7-3 国家行使数据主权设定的法定框架

举个例子，2011年生效的韩国《个人信息保护法》（The Personal Information Protection Act）在第17条第3款规定，“个人信息向境外第三方传输前，应取得数据主体的同意”。[36]在这个例子中，韩国行使数据主权的方式是制定《个人信息保护法案》；对数据是否本地化存储，韩国这个主权国家的基本态度是：数据流向境外不应与对数据的其他处理同等对待，所以数据控制者在向境外传输数据前要单独向数据主体告知，但数据是否只能留存于韩国境内应由数据主体自行决定；于是《个人信息保护法案》赋予数据主体自主控制其个人信息是否流向境外的权利，而数据控制者应遵照数据主体的意思表达。

换句话说，在数据本地化存储方面，韩国行使数据主权的方式是将数据跨境流动当成单独的风险点，同时尊重数据主体对此表达的意愿，并以个人权利的方式，赋予数据主体相对于数据控制者的优势地位。类似的还有印度通信技术部于2011年颁布的《信息技术法案》隐私方面实施细则。细则规定，如获得数据主体的同意，其个人信息可向境外传输。[37]

欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）关于数据跨境流动的制度设计，同样体现了数据主权不直接介入具体的数据处理安排这个特点。综合GDPR第五章“向第三国或国际组织传输个人数据”的规定可得出如下结论：欧盟这个数据主权主体对数据跨境流动的基本原则和前提是欧盟境外的数据接收方应提供与GDPR相同的数据保护水平。落实上述原则和前提的方式有两类：第

一，欧盟委员会（EU Commission）认定第三国的立法、数据保护制度等是否能够提供与GDPR相同的数据保护水平。第二，如欧盟委员会尚未做出上述认定，欧盟境外的数据接收方还可主动采取适当的保护措施，例如有约束力的公司内部规则（Binding Corporate Rules），确保在境外提供与GDPR相同的数据保护水平。[38]在此我们看到，欧盟委员会认定的是第三国整体的数据保护水平是否充分，此外GDPR还允许数据控制者主动采用充分的数据保护措施，为数据跨境流动扫清障碍。两类情况中，数据主权均不直接介入具体场景中的数据跨境。

类似的，加拿大在《跨境处理个人数据指南》（Guidelines for Processing Personal Data Across Borders）中要求，数据输出者应对跨境流通的数据安全负责，确保传输至境外第三方的个人数据得到充足保护。具体来说，数据输出者应当以契约或其他方式，确保：①防止第三方在处理数据过程中，出现未经授权使用或揭露的情形；②确认第三方具有完善的数据保护政策或流程；③定期稽核第三方处理或储存个人数据的安全性。[39]也就是说，加拿大通过立法对数据输出者施加了确保数据在境外安全的义务，以此体现国家对数据跨境流动的基本态度。

在数据本地化存储方面，国家在行使数据主权时还可突破上述的宏观和微观的界分，直接以公权力主体的身份介入到数据主体、数据控制者及其他相关方自主形成的数据处理安排之中。如图7-4所示。

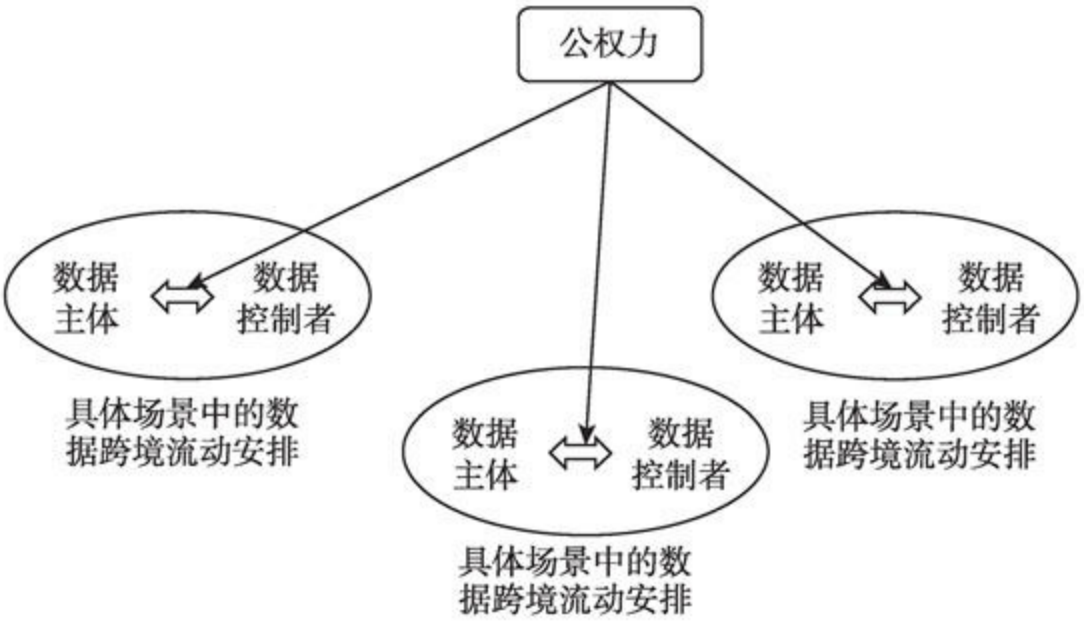

图7-4 国家以公权力主体的身份介入数据处理安排

例如，澳大利亚2012年生效的《个人控制电子健康记录法案》（Personally Controlled Electronic Health Records Act 2012）在第77条规定，涉及个人信息的健康记录只能留存于澳大利亚境内，否则将予以处罚。[40]与上述韩国“退居幕后”不同，澳大利亚这个主权国家直接“走到前台”，在具体的数据处理安排中与数据主体和数据控制者形成三方关系，强制要求数据在境内留存。

再如，我国台湾地区2012年生效的《个人资料保护法》第21条规定，“非公务机关为国际传输个人资料，而有下列情形之一者”，主管机关应予以限制：“一、涉及国家重大利益。二、国际条约或协议有特别规定。三、接受国对于个人资料之保护未有完善之法规，致有损当事人权益之虞。四、以迂回方法向第三国（地区）传输个人资料规避本法。”[41]可见在上述四种情形中，台湾地区的公权力机关将直接介入具体场景中数据跨境流动安排。[42]

如前文所述，在数据本地化存储实施主体方面存在两个模式。第一种模式，本章称之为“主权内化于私权”，国家淡入背景之中而不直接介入，而是将数据主权的意志通过明示数据流动基本原则、界定行为主体权利和义务等方式，使位于前台的数据主体、数据控制者及其他相关方以“戴着镣铐跳舞”的方式，自主达成具体场景中的数据跨境流动安排。这种模式中，由于数据主权意志已有体现，公权力往往只需在事中、事后，根据既定的数据流动基本原则对私人主体自主达成的数据跨境流动安排给予核验即可。

第二种模式中，本章称之为“主权直接参与”，国家数据主权以公权力的形式直接介入，与数据主体、数据控制者及其他相关方共同作为具体场景中的数据跨境流动安排的行为主体。此时，公权力作为国家数据主权的主要代言人，往往在事前要根据具体场景中的数据跨境流动给予审批或评估，做出个案裁量、深度参与最终达成的跨境流动安排。

可见，两种模式中，数据主权均不缺位，但实现其意志的方式不同，介入的深度和时间点不同，公权力拥有的裁量空间也有所不同。

2. 本地存储彻底程度

具体来说，本地化彻底程度包括以下三个层次：第一层，仅要求境内存储数据的副本（copy），与此同时数据可在境外存储、处理、访问。例如，印度尼西亚通信部要求组织机构应在境内建立数据灾备中心。[43]再如，俄罗斯2015年9月生效的第242-FZ号联邦法律，要求对俄罗斯“公民个人数据的收集、记录、整理、积累、存储、更新、修改和检索均应使用俄联邦境内的服务器”。[44]从字面上看，俄罗斯要求对俄公民个人数据的存储、处理、访问都应在俄罗斯境内进行，但在该法律生效前，俄罗斯通信和大众传媒部于2015年8月针对该法律发布了一个无约束力的澄清（clarification）。根据俄通信和大众传媒部对第242-FZ号联邦法律的解释，只要组织机构在俄境内存有数据副本（甚至于纸质副本即可），则个人数据可自由传输至境外。[45]在中国，前文所述的《网络出版服务管理规定》和《保险公司开业验收指引》中关于数据本地化存储的规定，也可解读允许境外存有境内留存数据的副本。

第二层，进一步要求数据只能在境内存储，此时对数据的处理也只能在境内进行，但允许从境外访问数据，例如允许从境外访问数据的部分字段而非整体。如我国《征信业管理条例》，要求“在中国境内采集的信息的整理、保存和加工，应当在中国境内进行”，对来自境外的访问并没有明令禁止。

第三层最为严格，要求数据的存储、处理、访问都必须在境内进行。前文提到的澳大利亚《个人控制电子健康记录法案》第77条规定：①不得在记录携带至澳大利亚境外，也不允许在澳大利亚境外持有记录；②不得在澳大利亚境外处理关于记录的各种信息。[46]其中，“不允许在澳大利亚境外持有记录”也就禁止来自境外的访问。另一个例子是中国人民银行《关于银行业金融机构做好个人金融信息保护工作的通知》要求“除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。”其中的“提供”包括来自境外的访问请求。[47]

3. 本地化存储覆盖的数据范围

就笔者掌握的资料来看，尚未有国家要求所有电子化数据都在本地化存储。多数国家选择在有限的范围内划定需本地化存储的数据，常见的有以下几类：

（1）个人数据（或个人信息）。这也是最常见的受到本地化存储

要求的数据类型。

（2）行业内的重要数据。如医疗健康行业（如澳大利亚）、银行业（如中国）、保险业（如中国）、征信业（如中国）、交通（如中国）、电子支付业（如土耳其[48]）、地图数据（如韩国[49]）、网络信息服务（如越南[50]）等。

4. 本地化存储的豁免条件

许多国家在要求数据本地化存储的同时，明确列出了豁免条件。因此，满足豁免条件的难易程度，也是数据本地化存储严苛度的一个重要指标。综合分析，豁免条件主要存在以下几种情形：

（1）数据主体明示同意即可。如前文所述的韩国、印度以及巴西[51]等国家。

（2）境外的数据接收方应能提供与本国相当的数据保护水平。此种情形最典型的例子是前文提到的欧盟的《通用数据保护条例》、加拿大的《跨境处理个人数据指导》等。这也是目前个人数据跨境传输方面最常见的豁免条件。据笔者不完全统计，目前至少有欧盟的28个成员、澳大利亚[52]、我国香港地区[53]、阿根廷[54]、以色列[55]、日本[56]、新西兰[57]、新加坡[58]等采用这样的豁免条件。

（3）公权力机关自由裁量。此种情形中，公权力机关的裁量对数据是否可跨境流动起决定性作用，甚至可超越既定基本原则的规定。例如，马来西亚2013年生效的《个人数据保护法》（Personal Data Protection Act）第129条规定，公民个人数据传输至境外的基本原则是数据接收方所在国家应能提供与本地相当的数据保护水平，但该法第46条规定，主管部门的部长可豁免某单个数据主体或某类数据主体受《个人数据保护法》规定的原则或条款的保护，还可在豁免的同时附加任何条件。[59]因此，主管部门的部长就特定数据境外传输享有非常大的自由裁量权。新加坡2014年生效的《个人数据保护法》（Personal Data Protection Act）也有类似规定，其第 26 条原则上要求境外数据接收方应提供与本地相当的数据保护水平，但同时赋予新加坡的“个人数据保护委员会”（Personal Data Protection Commission）广泛的自由裁量权。委员会可根据机构的申请，以书面的形式免除机构遵守数据跨境的合规义务，还可按其判断附加任何条件。[60]

我国也有类似赋予公权力机关自由裁量的例子。前文提到的中国人民银行2011年《关于银行业金融机构做好个人金融信息保护工作的通知》中规定“除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息”。而中国人民银行上海分行在其《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》（上海银发〔2011〕110号）中对上述规定做出了解释：“为客户办理业务所必需，且经客户书面授权或同意，境内银行业金融机构向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规。”[61]可见，对豁免情况的解释权，不仅在人民银行本身，也包括人民银行授权下的上海分行。

六 构建“数据本地化存储合理界限理论”之二——数据本地化存储所实现的目标

在详细描述了数据本地化存储手段后，本部分将主要分析数据本地化存储所能实现的目的，主要有三个层次。

1.数据安全（data security）

数据安全可以认同为传统所说的信息安全（information security）。信息安全主要追求三性，也就是所谓的CIA：保密性（confidentiality），指信息不被泄露给未经授权者的特性；完整性（integrity），指信息在存储或传输过程中保持未经授权不能改变的特性；可用性（availability），指信息可被授权者访问并使用的特性。[62]也就是说，数据安全保障的是信息或信息系统免受未经授权的访问、使用、披露、破坏、修改、销毁等。[63]

2.个人数据保护（data protection）

其一，数据保护与传统意义上的隐私（privacy）的区别。

A.欧洲

首先看法律规定。欧盟法中的数据保护和隐私是两个概念。最明显的是在《欧盟基本权利宪章》（Charter of Fundamental Rights of

the European Union）中，数据保护和隐私分属两个不同的权利，由两个不同的条文来规定（见表7-2）。

表7-2 《欧盟基本权利宪章》中的数据保护和隐私条款

第七条 尊重私人和家庭生活	每个人都有权获得对其私人和家庭生活、私人寓所、私人通信的尊重
第八条 个人数据保护	每个人都有保护其个人数据的权利。 对个人数据的处理，必须基于特定目的、以公平的方式进行，且需获得个人的同意或出于法律规定的其他正当事由。每个人有权访问或纠正其被收集的个人数据。 应由独立的权威机构来确保对上述规则的遵守

其次看学理上的解释。隐私权可理解为“别管我”（leave me alone），即个人私生活不被打扰的权利——“唯我独自享有的他人不得侵犯、干扰、触及的个人生活秘密、宁静的权利”。这是隐私权首次被提出时的经典理解。[64]可以看出，隐私权是个人用于抵抗外界对其私人领域、私密信息窥探、侵犯的一种防御性机制（defensive mechanism），是一种个人私域对内的保护。隐私权经典的理解符合《欧盟基本权利宪章》第7条的含义。

而个人数据保护权则主要建立在“个人信息自决理论”基础上。该理论认为，为保障人格的自由发展，个人应当能自由地决定以何种方式实现人格发展；人格的形成主要是在人与外界、特别是人与人的交往过程中实现，因此个体需要掌控对外自我披露或表现的程度，以便合理地维持自身与他人之间的人际关系，所以个人应当能自由、自主地决定如何使用个人信息。[65]也就是说，数据保护权赋予个人有权控制个人数据出于何种目的，面向何种对象范围，通过何种途径扩散和披露。换句话说，就是“个人依照法律控制自己的个人信息并决定是否被收集和利用的权利。”[66]

数据保护权与被动的防御性隐私权不同，其“将自身置于人际交往的互动场景之中，从而使得个人信息与个人私域的隐秘性脱钩，无论个人信息的具体内容是否涉及数据主体的个人隐秘，它都受到法律的保护，因为个人享有对其加以合理利用进而掌控自我表现的利益”。[67]

因此，数据保护是一种管理信息扩散和披露的机制，是一种面向外部的控制。《欧盟基本权利宪章》第8条规定的数据保护权，理论根基即在于保障“个人信息自决”的权利。[68]欧洲最新的《通用数据保护条例》（GDPR）正文中没有用到隐私（privacy）这个词，也是欧洲将隐私和数据保护做出区分的一个示例。

B. 美国和国际标准

隐私权概念起源于美国，因此在美国，隐私一开始是一种“别管我”的概念。但经过20世纪60～80年代的发展，美国的隐私概念现在已经包含了“个人信息自决”内涵。[69]

ISO/IECJTC1/SC27是国际标准化组织（ISO）和国际电工委员会（IEC）联合技术委员会（JTC1）下属专门负责信息安全领域标准化研究与制定工作的分技术委员会，SC27/WG5负责身份管理和隐私保护相关标准的研制和维护。目前在个人数据保护领域最具代表性和体系性的，当属ISO/IEC 29100系列标准，包括：ISO/IEC 29100《隐私保护框架》、ISO/IEC 29101《隐私体系架构》、ISO/IEC 29190《隐私能力评估模型》、ISO/IEC 29134《隐私影响评估》、ISO/IEC29151《个人可识别信息保护指南》等。在这套标准中，隐私也是包含了上述“别管我”和“个人信息自决”的内涵。[70]

因此，美国法律和国际标准中的隐私，不仅仅是传统意义上隐私的含义——即“别管我”（leave me alone）和个人私生活不被打扰的权利；相反，基本上可以认为，美国法律和国际标准中的隐私概念等价于欧洲的数据保护概念。

其二，数据安全和个人数据保护的区别

通过上面的讨论，可以明确数据保护主要在于“保护对个人信息的自主使用，要求他人不得以违反本人意愿的方式对个人信息进行处理”；这是因为，“非经本人同意的信息处理会在社会中造成超出本人预期的结果，并对本人的人格发展造成不可预料的影响，使得本人人格塑造的结果偏离原本的预期。”[71]

王利明教授用个人信息权的概念表述数据保护的基本要旨：“个人信息权主要是指对个人信息的支配和自主决定。个人信息权的内容包括

个人对信息被收集、利用等的知情权，以及自己利用或者授权他人利用的决定权等内容。即便对于可以公开且必须公开的个人信息，个人应当也有一定的控制权。例如，权利人有权知晓在多大程度上公开、向谁公开该信息以及他人会基于何种目的利用信息等等。”[72]

由此，数据安全和数据保护在概念上的区别应当就比较明显了。首先，没有数据安全，肯定没有数据保护，因为信息系统被攻破，数据遭到泄露，那数据保护要求的授权和控制扩散的机制就无从谈起了。其次，应当看到，即便实现了数据安全，并非就一定做到了数据保护，例如数据很安全地存储在组织机构的信息系统中，但是组织没有根据数据主体授权的范围来处理数据，那就违背了个人的数据权利。

这也是为什么在各国的个人数据保护立法中，数据安全部分的规定独立成章，但篇幅不大。以欧盟《通用数据保护条例》为例，立法的重心在于规定个人数据处理的基本原则[73]、数据主体的权利[74]、数据控制者和处理者的义务配置等。保障数据安全仅仅是数据控制者和处理者众多义务之一，其更重要的义务是在数据的收集、存储、使用、共享、公开、跨境传输等环节中提供各种机制，使得数据主体得以行使其“信息自决的权利”。例如，充满争议的被遗忘权，就是GDPR的一大创新。显然，被遗忘权无关数据安全，而是赋予个人在特定情况下删除与其相关的个人数据的权利。

数据保护与数据安全之间的关系可以用公式表达如下：

个人数据保护=数据安全+个人信息自决权利+数据控制者等相关方满足个人信息自决权利的义务。

3. 国家层面的数据保护

上一部分讲的数据保护主体主要是个人，正如前文所说，数据权利的另外一个主体是国家，因此本部分将主要讨论面向国家安全的数据保护，或国家作为主体的数据保护。先看下面三个例子：

阿里巴巴2016年11月2日公布的2016年9月底的季度业绩显示，淘宝中国平台活跃买家高达4.39亿户。[75]根据淘宝的隐私权政策，淘宝买家至少需要提交以下信息：姓名、性别、出生年月日、身份证号码、护照姓、护照名、护照号码、电话号码、电子邮箱、地址等。[76]结合上

述信息推知，阿里巴巴至少掌握了4亿我国公民的基础个人信息；而且借助于买家支付、收货等场景，其掌握的数据真实性甚至远超政府机关。单个公民的基础信息，无疑属于应当保护的个人信息。而一家私营企业汇聚了如此海量的公民个人信息库，其意义显然超出了保护个人权益的层面。

第二个例子，2016年11月，俄罗斯知名网络安全厂商卡巴斯基公开抗议微软挤压第三方杀毒软件在win10操作系统的生存空间。[77]表面上看来，该事件事关商业竞争。但更进一步考量，此事关乎国家安全。习近平总书记指出的，维护网络安全的关键在于“全天候全方位感知网络安全态势”[78]。因此，没有关于网络攻击、威胁来源、恶意地址等网络安全信息汇聚形成的安全大数据，也就根本无法做到“知己知彼”。微软排斥其他杀毒软件在其生态中的运作，客观上造成了独掌围绕其平台产生的安全大数据的结果。

第三个例子涉及住房空置率。据业内说法，空置率主要是指在统计时刻内没有被使用的住房除以全社会总住房所得出的空置率。而一旦“房屋空置率超过5%到10%，房地产市场就出现较大问题了：房屋闲置比较严重，严重的供过于求，租金、房价要开始回落了”。而且，“住房空置率反映了社会资源浪费的问题。空置率高企反映了近些年来住房的投资属性被无限放大、夸大，而住房的居住属性被淡化、弱化的现实，其背后则反映了中国社会贫富严重分化的现实”。[79]在我国，房价目前已是政府、百姓最关心的事情之一。因此，特别是在政府出台调控措施时，空置率很可能成为“对宏观经济调控政策、措施有较大影响的统计报告”，或者是“反映重大经济、社会问题的统计数据和统计报告”，属于国家机密的范畴。[80]这也从侧面说明了为何一些地方统计部门曾就当地住房空置情况做过调查，但对调查结果一直讳莫如深。[81]过去，学者或民间力量为了计算空置率，只能通过“数黑灯”或入户抽样调查，现如今，只需结合海量的快递订单、水电运行等数据，在某一区域甚至全国范围内得出准确的房屋空置率并非难事。

这三个例子均表明，大数据对国家发展、治理、安全等方面有着越来越重要的意义。首先，阿里巴巴掌握的人口信息，规模和颗粒度均可比拟公安机关的国家人口基础信息库，准确性甚至更胜一筹。对国家来说，人口基础数据一旦泄露，很可能对国家安全造成严重危害[82]，因此国家人口基础信息库是作为涉密系统来建设和管理的。所以，国家层面的数据保护首先应要求阿里保障其掌握的大数据的安全，也就是前文

讲到的保密性、完整性、可用性。

其次，除数据安全之外，由于某些特定大数据对国家来说具有基础性、战略性的作用，国家应当具有一定的支配权。例如阿里巴巴汇聚的我国人口大数据，如果不将其划成涉密系统的话，则国家至少应当有权要求其不得对外共享、交易，并且不得向境外的组织、个人提供。对于第二个例子中，鉴于微软操作系统在我国用户数量庞大，国家应当有权要求微软不得独占，乃至于要求其与主管部门共享win10平台产生于我国境内的网络安全大数据。这不仅是因为海量用户产生的安全大数据对维护国家网络安全至关重要，失去此数据很可能造成威胁情报上的盲区；另一原因是如果说安全大数据可以用于提升安全水平，反过来，安全大数据当然可以很轻易地被恶意分子用于分析系统和空间的漏洞和脆弱性，找到攻击的切入点，因此有必要严格管控。

第三个例子中，淘宝、顺丰等企业显然拥有了海量的快递订单数据，而目前，支付宝、微信等应用集成了生活缴费功能，获得越来越多家庭的青睐。上述两类数据并非属于国家秘密。但两者一结合，很容易综合分析得出受严格保护的国家机密数据。大数据的发展，事实上导致了国家秘密和非国家秘密之间的界限不断在模糊。对于“单独或者与其他信息相结合分析后，有可能对国家安全和公共利益造成不利影响的数据”，本章称之为敏感数据。显然，敏感数据比实践中认定的“国家秘密”范围要大得多。虽然将所有敏感数据都纳入“国家秘密”这样由公权力直接管控的强制机制内不是个现实的选项，但客观上确实存在强烈的需求来防范敏感数据被敌对国家或势力恶意使用（malicious use of big data），例如在关键时间节点恶意发布有关信息危害我国经济安全。

因此，国家层面的数据保护，除了数据安全及对数据一定的支配权外，还包括控制敏感数据可出于何种目的，面向何种对象范围，通过何种途径扩散和披露。综上，国家层面的数据保护=数据安全+数据支配权+防止敏感数据遭恶意使用对国家安全的威胁。

七 构建“数据本地化存储合理界限理论”之三——目的与手段的适当性和必要性关系

（一）比例原则之于数据化本地存储

本应由私人主体之间在具体场景下形成的数据跨境流动安排，因为国家数据主权的介入，需要留存在本地，或在满足国家数据主权设定的豁免条件后，数据才得以跨境流动。无疑，数据本地化存储是国家公权力的一种彰显。而比例原则是公权力在行使时必须首先遵守的“帝王条款”[83]，其对目的与手段必要性、适当性、均衡性的要求，对依法治理数据化本地存储、为其设定合理界限具有重要指导意义。

比例原则可分为适当性原则、必要性原则与均衡性原则三个子原则：适当性原则是指公权力行为的手段应当有助于或能够实现所追求的目的；必要性原则是指在能够“相同有效”地实现目的的众多手段中，公权力行为采用的手段造成的损害应当最小；均衡性原则要求公权力行为的手段所增进的公共利益与其所造成的损害成比例。[84]

下文将运用比例原则审视数据化本地存储的价值目的与管制手段之间的关系，依据比例原则中适当性和必要性的要求，构建“数据本地化存储合理界限理论”。由于比例原则中均衡性的要求，需跳脱狭义的目的手段关系，把目的列为检验与衡量的对象，追问为特定目的而要求某人或某些人承受特定负担是否合理。[85]本章的分析论证是基于各国成文法规范，以此抽象出严苛度措施和价值目的，为我国相关立法提供借鉴指导。对均衡性的讨论，需要更高层次的理论框架才能胜任，笔者将另文探讨。

接下来，本部分将从上文提出的三个层次的目的出发，讨论什么样的本地化措施，分别符合适当性和必要性要求。

（二）判断目的与手段之间的适当性和必要性

1. 数据安全与本地化存储

按比例原则中必要性原则的要求，限制数据的存储地点需要能提升数据的安全水平。但许多研究表明，数据安全实际上并不取决于数据的存储地点，而是数据存储和传输的方式。[86]

首先，数据安全无非是攻防两方力量对比的结果。现阶段，攻方显示出压倒性的优势。[87]对于黑客和犯罪组织来说，无论数据存放在哪里，只要被他们盯上都会无所不用其极，例如使用钓鱼、木马、病毒等技术手段，或直接收买内部人员等。他们并不会因为地域限制而放弃某

项攻击，而互联网的特性也允许他们能够方便地实施跨地域攻击。[88]

从防守方的角度来看，强制数据留存本地或许有一定意义。毕竟数据留在国内，网络安全主管部门可以按照自己的判断，强制信息系统所有者或运营者等，采取足够或额外的安全措施。但即便在这个意义上，数据本地化存储也并非必要，因为当数据需要传输至境外时，数据输出者可以通过合同等形式，将境内主管部门施加的额外安全义务“传导”到境外数据接收者身上，作为数据跨境传输的前提条件。如此一来，安全保护措施便跟随着数据一路从境内延展到境外。

也许有人认为，从侦查机关的角度来说，数据本地化存储能使得境内的侦查机关获得对案件的管辖权，对黑客、犯罪分子是一种震慑，因此能降低攻击风险。仔细思考，这样的观点也无法成立。首先，侦查机关获得管辖权无须仅仅依赖数据在境内留存。例如，我国《刑法》第8条规定：“外国人在中华人民共和国领域外对中华人民共和国国家或者公民犯罪，而按本法规定的最低刑为三年以上有期徒刑的，可以适用本法，但是按照犯罪地的法律不受处罚的除外。”其次，即便境内机关通过数据本地化存储获得了管辖权，但在很多时候，对黑客、犯罪分子的威慑力也相对很有限。先不说来自境外的黑客和犯罪分子，目前国内有经验的黑客和犯罪分子基本都利用国外的服务器作为跳板，制造境外攻击的假象。一旦涉及境外调查取证、耗时费力的双边司法合作程序等，侦破的难度往往大幅上升。

当然，上述分析仅停留在理论层面。实践中，数据跨境传输往往意味着数据链条上环节的增多，从常识上来讲，这意味着出错的风险在增高，保密性、完整性、可用性被破坏的可能性在增大，或许强制数据境内留存能在一定程度上降低风险。但同时应当牢记的是，即便将数据存储和传输局限于境内，上述风险并非就一定比数据跨境传输要低，因为意识到跨境传输带来的高风险会促使数据输出方采取额外的安全措施。

综上所述，强制数据存放在国内，事实上并不能降低信息系统被攻破、数据被窃取的风险，同时也并非保障数据安全的必要措施。

2. 个人数据保护与本地化存储

对于数据保护来说，本地化存储具有一定积极意义。如前文所述，个人数据保护=数据安全+数据主体的信息自决权利+数据控制者等相关方满足个人信息自决权利的义务。而个人信息自决权利范围、程度的大

小，以及数据控制者等相关方承担的满足个人信息自决权利的义务等，往往是一个国家在平衡以下三方面利益时做出的选择：

（1）个人信息自决利益：包括在一定程度上控制个人信息的收集、使用、共享、披露，以及控制基于数据做出的各项决定对个人的影响。

（2）发展利益：企业和产业充分利用个人信息，提供、改进、创新产品和服务的合理诉求。

（3）公共利益：政府部门利用个人信息完成公共管理，以及社会发展所必需的信息自由流动和公众知情权。

很显然，每个国家在平衡利益冲突时做出的选择不尽相同。因此从个人数据保护的角度来说，数据留存本地能确保个人的权利、数据控制者等相关方的义务等，能够遵循这个国家做出的特定的利益平衡选择。[89]

但应该注意到，如果通过合同、公司内部准则等形式，能够确保数据传输至国外后依然能够享有和境内相同的安全水平、个人信息自决的权利配置等，基本上各个国家也都允许此种情形豁免于数据本地化存储的要求。当然，也有部分国家仅要求数据主体明示同意即可豁免于本地化存储。

总的来说，从数据保护这个层面来说，数据留存本地的主要意义在于确保本国在个人信息自决权利、数据控制者等相关方满足个人信息自决权利的义务等方面做出的配置安排，能够适用于特定数据，而非保护数据安全。

3. 国家层面的数据保护与本地化存储

如前文论述的，国家层面的数据保护=数据安全+数据支配权+防止敏感数据遭恶意使用对国家安全的威胁。而在网络世界中，能够威胁到国家安全的也主要是敌对国家，或具有国家背景的敌对势力。目前，已有各种具备国家背景的黑客组织，对我国境内组织、机构发动了许多高级持续性威胁（Advance Persistent Threat，简称APT）。[90]这些事例都说明，即便强制数据存放国内，仍无法避免敌对国家或具有国家背景的敌对势力的黑手。因此，就数据安全来说，强制本地化事实上不能

保障数据安全。

但强制数据存放在国内，确实能杜绝一类特定的风险——境外国家利用法律、行政等手段，合法、秘密地获取传输至其境内的数据，特别是敏感数据。在斯诺登曝光的美国“棱镜”计划中，美国国安局正是利用了经互联网传输的数据大部分都要途经美国的有利条件，得以直接截取了海量数据，同时还合法、秘密地要求美国互联网公司与其合作，获得了大量的境内外用户数据。在这个例子中，美国政府通过对其境内的数据光缆、数据中心行使主权，成功地监听了全世界。[91]因此，在“棱镜门”曝光之后，德国等欧洲国家提出建立自己的电子邮件系统、云数据中心、不途经美国的光缆等技术手段，这些措施的共通之处在于使美国主权之手无法触及数据存储、传输的全过程。[92]

另一个例子是不久前美欧通过的“隐私盾”协议。原有的“安全港”协议之所以被宣判无效，根本原因是“棱镜门”让欧洲意识到：虽然可以通过合同等手段约束美国公司，要求其在美国境内也提供与欧洲相同的数据保护水平，但美国政府（特别是国家安全局）能通过法律或行政手段，合法、秘密地要求美国公司将数据交出来；而美国公司自然要受美国法律的管辖，就算心里不情愿，也只能乖乖就范。换言之，欧盟原本认为可以通过合同、公司内部准则等手段，对传输至境外的数据进行全程保护，但这样的保护手段还是会轻易地被一国的主权撕开口子。因此，新的“隐私盾”协议的重点内容之一，就是约束美国的主权——美国政府明确承诺其情报机关将暂停大规模、无差别收集数据的行为。[93]

（三）数据本地化存储合理界限理论

数据本地化存储合理界限理论的主要观点如图7-5所示。首先，数据本地化存储可能实现的目的包括数据安全、个人数据保护、国家层面的数据保护，每一目的包含不同的内容，如：

数据安全=保密性+完整性+可用性；

个人数据保护=数据安全+个人信息自决权利+数据控制者等相关方满足个人信息自决权利的义务；

国家层面的数据保护=数据安全+数据支配权+防止敏感数据遭恶意

使用对国家安全的威胁。

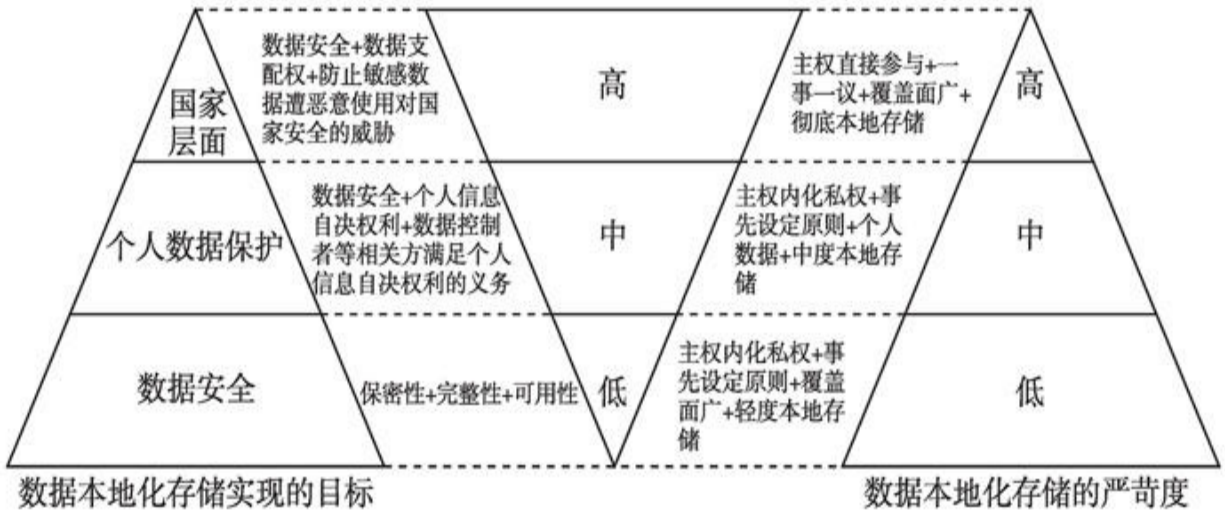

图7-5 数据跨境传输的原则或基本条件

其次，经分析可知，对保障数据安全，数据本地化贡献度较小；对数据保护，数据本地化存储主要在于使数据能遵循每个国家就个人信息自决方面做出的权利、义务配置选择，具有一定的数据本地存储需要；对国家层面的数据保护，数据本地化存储的功效主要在于杜绝境外国家利用法律、行政等手段，合法、秘密地获取传输至其境内的数据，因此具有较高的数据本地存储需求。

再结合前一部分对数据本地化严苛程度的描述模型，还可得出：为满足数据安全、个人数据保护而要求数据本地化时，国家主权通过事先设定数据跨境传输的原则或基本条件，以及对涉及的各个私主体通过规则事先设定权利义务即可，并无必要实际参与到各个场景中；在具体场景中，私主体事先知晓各自的权利义务、跨境传输的条件，只要达成的数据传输安排“过了门槛”，即可开展传输。

当数据本地化是为了满足国家安全需求时，国家主权具有广泛的自由裁量权，应一事一议，按照个案实际情况做出裁量，同时可对各个私主体附加任何特定的要求，包括彻底的本地化存储，不允许来自境外的访问请求。

八 检视《网络安全法》的数据本地化存储规定

对照关于“数据化本地存储合理界限理论”，检视我国《网络安全法》第37条关于数据本地化存储的规范，会发现该条存在以下四个方面的问题：一是关键信息基础设施如何认定？范围多大？二是个人信息和重要数据的定义和范围多大？关键信息基础设施中是否还存在第三类数据？又或者个人信息和重要数据是不是关键信息基础设施上存储的所有数据的总和？三是“应当在境内存储。因业务需要，确需向境外提供的”应如何解读？是仅仅要求境内留存副本而已，还是“向境外提供”包括从境外发起的访问数据请求？四是如何进行安全评估？关于第四个问题，本章将在结论中一并论述。

（一）关键信息基础设施的范围

关键信息基础设施是一个相对新的概念，与关键基础设施不同，特指信息系统或控制系统。它可能单独成为设施，也可能是设施的一部分。其范围在《网络安全法（草案）》一读、二读、三读中均有划定。考虑到《网络安全法》第39条的规定，[94]中央网信办于2016年12月发布的《国家网络空间安全战略》和2016年7月开启的“全国范围关键信息基础设施网络安全检查工作”，对关键信息基础设施的界定具有十分重要的参考意义。具体规定参见表7-3。

表7-3 界定关键信息基础设施的相关规定

	关键信息基础设施的范围
网络安全法（一读）	1. 提供公共通信、广播电视传输等服务的基础信息网络； 2. 能源、交通、水利、金融等重要行业和供电、供水、供气、医疗卫生、社会保障等公共服务领域的重要信息系统； 3. 军事网络； 4. 设区的市级以上国家机关等政务网络； 5. 用户数量众多的网络服务提供者所有或者管理的网络和系统。
网络安全法（二读）	对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施。
网络安全法（三审）	公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施。
网络安全法	公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施。
全国范围关键信息基础设施网络安全检查工作①	面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，这些系统一旦发生网络安全事故，可能影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境及人民生命财产造成严重损失。
国家网络空间安全战略	包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。

① 《全国范围关键信息基础设施网络安全检查工作启动》，中国网信网，http://www.cac.gov.cn/2016-07/08/c_1119185700.htm。

综合研读，可将关键信息基础设施的范围总结如下：一是军政部门的网站、信息系统或控制系统；二是重要行业和领域的信息系统或工控系统，重要行业和领域包括能源、交通、水利、金融、供电、供水、供气、医疗卫生、社会保障等等；三是面向公众提供网络信息服务的网站和平台。事实上，上述三个类别也不一定涵盖了全部的关键信息基础设施，只要是“一旦发生网络安全事故，可能影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境及人民生命财产造成严重损失”[95]的系统，都将被认定为关键信息基础设施。

（二）个人信息和重要数据的范围

《网络安全法》在第76条规定了个人信息的定义：“指以电子或者其他方式记录的能够单独或者与其他信息结合能够识别自然人个人身份的各种信息，包括但不限于公民的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。”

关于“重要数据”，《网络安全法（草案）》三读与最终稿之间出现了一个微妙的变化。三读使用“重要业务数据”。对此，可能存在两种理解：一是认为“业务数据”英文为business data，是组织机构与外界发生交互（transactions）的记录，不包括内部运营数据，例如组织机构人力方面的数据；二是认为“业务数据”同时包括组织机构“内部运作”和“外部交互”的数据。如果最终“重要业务数据”的定义采用前者，则关键信息基础设施里其他类别的数据无须本地存储；如果采用后者，则可认为关键信息基础设施里的所有数据都要本地存储。

在2016年11月7日全国人大发布的最终稿中，删除了“业务”两字，体现了立法者最后时刻的考量。在笔者看来，重要数据的重要性，针对的是整体层面的利益保护，即保护国家安全、国计民生、公共利益。因此，只要运营者的数据不涉及整体层面利益，就不属于“重要数据”的范畴。因此，从“重要业务数据”改为“重要数据”，说明立法摒弃了我们熟悉的“个人数据、企业数据、国家数据”的分类方法，进而从数据所影响的价值着手。换句话说，不论是个人数据或是企业数据，只要有可能危及整体层面的利益，就会被认定为“重要数据”。

（三）“因业务需要，确需向境外提供的”的含义

从字面上看，第37条要求的是彻底的数据本地化存储，即要求数据的存储、处理、访问都必须在境内进行。此处“提供”应当包含来自境外的访问。这一判断有两方面证据。首先，如前文所述，中国人民银行规定“除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息”，对于此处的“提供”，中国人民银行上海分行专门指出“境内银行业金融机构向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规”。很明显，此处的“提供”包含了来自境外的数据访问请求。

其次是《网络预约出租汽车经营服务管理暂行办法》（以下简称《办法》）第27条的规定。《办法》要求网约车平台公司应在中国内地存储和使用个人信息和业务数据，且“除法律法规另有规定外，上述信息和数据不得外流”。该《办法》在《网络安全法（草案）》（二读）公布后才出台，而且沿袭使用了个人信息和业务数据。其“不得外流”的规定，很可能代表了《网络安全法（草案）》（二读）中“向境外提供”的含义。

（四）对第37条的基本评价

在对第37条的条文进行简要分析后，借用本章提出的“数据本地化存储合理界限理论”，可对该条得出如下评价：

一是受本地化存储规定覆盖的数据范围非常广，全球范围内来看属于特例。将《网络安全法》的一读和二读对比，第37条在原来的个人信息基础上，增加了重要业务数据。[96]如前所述，关键信息基础设施的范围已经很宽泛，而“个人信息和重要业务数据”的规定还有可能包括了关键信息基础设施的所有数据。相比其他国家和区域，欧盟没有要求所谓的“重要业务数据”的本地存储，而在要求所谓的“重要业务数据”本地存储的国家，基本上也仅仅是对某一特定行业的数据做出规定。因此，二审稿增加了区区六个字，却很可能一下子使我国数据本地化方面的规定在国际层面显得十分“特立独行”。虽然《网络安全法》的正式版本中删除了“业务”两字，但似乎没有明显改变范围过大的情况。

二是默认的数据本地化存储严苛程度很高。第37条的字面意思，要求数据彻底的本地化存储。而且，第37条还要求法律、法规以下的规范性文件都从其规定。就此，原本允许境外处理、访问的卫生和计生委

《人口健康信息管理办法（试行）》、允许境外存储数据镜像的《网络出版服务管理规定》和《保险公司开业验收指引》都要“升级”执行彻底的本地化存储规定。

三是从适当性和必要性的要求出发，仅仅出于保障“运营安全”目的似乎难以为如此广泛、严苛的本地化要求提供足够的正当性。第37条位于第三章“网络运行安全”中的第二节“关键信息基础设施的运行安全”之中，因此可以认为，第37条的价值在于保障“运营安全”。而“运营安全”基本可以认为处于保障数据安全这个层面，无法涵盖个人数据保护的要求，如实现个人信息自决的权利，也无法涵盖国家层面的数据保护要求，如敌对国家情报机关合法、秘密地获取数据并分析、挖掘后，并不直接用于破坏关键信息基础设施，而是用于其他领域。而且如前文论证的，仅仅是数据安全，本质上并不取决于数据存储的地点；相反，个人和国家层面的数据保护才真正有数据本地化存储的必要性。

四是局限于“运营安全”将限制后续数据跨境传输安全评估的范围。如果“运营安全”是安全评估的全部目的，则安全评估无法囊括另外两个层面的目的，这将严重地限制安全评估的效用。因此，若为了给第37条规定的数据本地化提供足够的正当性以及去除对安全评估不必要的束缚，该条文似乎应当从第三章“网络运行安全”中移出，转而放置于第四章“网络信息安全”中。

九 相关立法建议

按《网络安全法》第37条的规定，国家网信部门将会同国务院有关部门制定的数据向境外提供的安全评估办法。在最后一部分，将根据前文提出的“数据本地化存储合理界限理论”，提出数据跨境流动安全评估办法的设计方案。具体如图7-6所示：

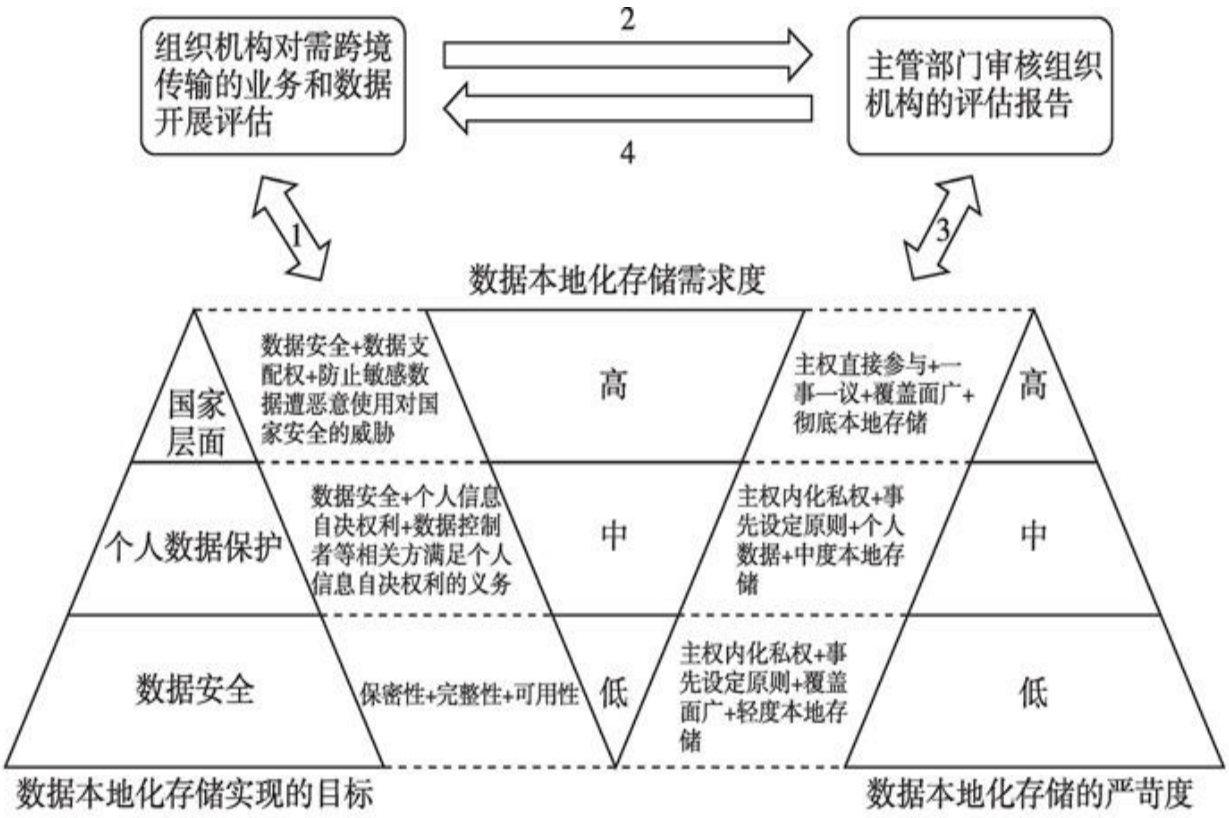

图7-6 数据跨境流动安全评估办法设计方案

首先是评估流程。最开始，由有跨境数据传输需求的组织机构按照“数据本地化存储合理界限理论”进行自评估并提出配套保障措施（“步骤1”），并将评估结果和配套保障措施提交给主管部门（“步骤2”）。其次，主管部门按照“数据本地化存储合理界限理论”对评估报告和配套保障措施进行审核，并做出自己的判断（“步骤3”），最后要求组织机构按照主管部门的要求形成数据跨境传输的具体安排（“步骤4”）。

其次是对评估的实质内容。如果评估显示数据仅仅涉及数据安全，此时公权力应采取“轻监管”模式，设定各私主体的权利义务，并事先列出跨境原则和“门槛”，在满足上述条件后，就可放行。如评估显示数据涉及个人数据保护，公权力同样通过事先设定各私主体的权利义务和跨境原则的方式，达到监管目的，只不过为保障个人信息自决权利，门槛相对数据安全要更高。如果评估显示数据涉及国家安全，则公权力开展“强监管”，一事一议，直接介入具体场景，参与设计特定的数据跨境保障措施，或者在风险无法管控的情况下要求数据必须存储于本地。

综上，围绕“数据本地化存储合理界限理论”构建数据跨境传输安全评估办法的最大好处在于，能将比例原则的精神贯穿于数据跨境的监管过程之中，也能使得国家在行使数据主权的过程中，在安全和发展之间取得平衡。

---

[1]《习近平在第二届世界互联网大会开幕式上的讲话》（全文），新华网，http：//news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm。

[2]《习近平：努力把我国建设成为网络强国》，新华网，http：//news.xinhuanet.com/mrdx/2014-02/28/c_133149933.htm。

[3] 详见下文论述。

[4] 应当旗帜鲜明地指出，国际上对我网络主权主张的批评，除源自上述理论难题外，在相当程度上还有对中国的陌生、偏见，也有部分利益集团出于维护既得利益所需，“为了批评而批评”。

[5]《习近平在第二届世界互联网大会开幕式上的讲话》（全文），新华网，http：//news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm。

[6] 习近平：《在网络安全和信息化工作座谈会上的讲话（2016年4月19日）》，http：//news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm。

[7] See Anupam Chander and Uyen P. Le，“Data Nationalism”，Emory Law Journal，vol.64（2015），p.680.需要说明的是：本章中“数据本地化存储”和“数据本地化”混用，不加区分。此外，本章将“数据”和“信息”两个概念混用。或许可以认为数据是信息的载体，信息则是数据呈现的有实际意义的内容，但大多数国家立法并不严格区分数据和信息。

[8] 详见下文论述。

[9] 见《网络安全法》第37条。

[10] 《中国网络安全规则将阻碍增长》，2016年8月11日，http：//www.ftchinese.com/story/001068889。

[11] The US-China Business Council，Technology Security and IT in China：Benchmarking and Best Practices，July 2016，https：//www.uschina.org/reports/technology-security-and-it-china-benchmarking-and-best-practices.

[12] 详见下文论述。

[13] 应当首先说明的是，本章讨论范围所指的数据，并不包含党政军及国有企事业单位的数据，而主要指私人主体包括个人、企业、社团等非公组织和机构产生、存储、处理的数据。前者往往因为“公有”属性而被要求本地化存储，本就是许多国家的惯例，而且并非争议的焦点。例如，美国国防部要求其云服务提供商需要在本地存储国防部的数据。See US Department of Defense，DoD Interim Rule on Network Penetration Reporting and Contracting for Cloud Services，https：//www.federalregister.gov/articles/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for.

[14] 中国保监会：《保险机构信息化监管规定（征求意见稿）》，http：//www.circ.gov.cn/web/site0/tab5168/info3975814.htm。

[15] The US-China Business Council，Technology Security and IT in China：Benchmarking and Best Practices，July 2016，https：//www.uschina.org/reports/technology-security-and-it-china-benchmarking-and-best-practices.

[16] Matthias Bauer，Martina F. Ferracane，and Erik van der Marel，Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization，Global Commission on Internet Governance Paper

Series （2016），p.2，https：//www.cigionline.org/publications/tracing-economic-impact-of-regulations-free-flow-of-data-and-data-localization.

[17] 下文将会详细描述主要国家的数据本地化存储措施。

[18] 根据Albright Stonebridge Group的报告，淡灰色的国家表示尚未发现有本地化规定。

[19] Albright Stonebridge Group的报告对数据本地化存储严格程度的评估主要是主观层面。本章将在第三部分提出一个模型，客观地描绘数据本地化存储的严苛程度。

[20] Martina Francesca Ferracane，How Data Localization Wipes out the Security of Your Data，June 2016，http：//www.securityeurope.info/how-data-localisation-wipes-out-the-security-of-your-data/.

[21] 见国家标准《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）中4.2对云计算服务模式的介绍。

[22] 如，王玥：《试论网络数据本地化立法的正当性》，《西安交通大学学报》（社会科学版）2016年第1期。

[23] Matthias Bauer，Martina F. Ferracane，and Erik van der Marel，Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization，Global Commission on Internet Governance Paper Series （2016），p.10，https：//www.cigionline.org/publications/tracing-economic-impact-of-regulations-free-flow-of-data-and-data-localization. Also see：Bauer，Matthias et al，The Economic Importance of Getting Data Protection Right：Protecting Privacy，Transmitting Data，Moving Commerce（2013），https：//www.uschamber.com/sites/default/files/documents/files/020508_Ec Final_Revised_lr.pdf；Bauer，Matthias et al，The Costs of Data Localization：Friendly Fire on Economic Recovery，ECIPE Occasion Paper no. 3/2014，

http：//www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf.

[24] Lee-Makiyama，Hosuk，Data localization requirement in Russia，http：//www.ecipe.org/blog/data-localisation-russia/.

[25] Lee-Makiyama，Hosuk，European leaders show leave data flows open，http：//www.euractiv.com/infosociety/european-leaders-leave-data-flow-analysis-530785；Susan Aaronson and Rob Maxim，Data Protection and Digital Trade in the Wake of NSA Revelations，http：//elliott.gwu.edu/sites/elliott.gwu.edu/files/downloads/research/aarons

[26] American Chamber of Commerce in China，Protecting Data Flows in the US-China Bilateral Investment Treaty，http：//www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization；US Chamber of Commerce，Safeguard Cross-border data flows，https：//www.uschamber.com/issue-brief/safeguard-cross-border-data-flows；Office of the United States Trade Representative，Trans-Pacific Partnership：Summary of US Objectives，https：//ustr.gov/tpp/Summary-of-US-objectives.

[27] Global Commission on Internet Governance，One Internet，pp.36，55，https：//www.ourinternet.org/report.

[28] Anupam Chander and Uyen P. Le，Breaking the Web：Data Localization vs.the Global Internet，UC Davis Legal Studies Research Paper No. 378，http：//papers.ssrn.com/sol3/papers.cfm? abstract_id=2407858.

[29] Richard Bennett，Surge in data localization laws spells trouble for Internet users，http：//www.techpolicydaily.com/internet/surge-in-data-localization-laws-spells-trouble-for-internet-users/.

[30] Dana Polatin-Reuben and Joss Wright，An Internet with BRICS Characteristics：Data Sovereignty and the Balkanisation of the Internet，4th USENIX Workshop on Free and Open Communications on the Internet

（FOCI 2014），https：//www.usenix.org/node/185057.

[31] 关于中俄与美西方在国际互联网治理方面理念、实践上的冲突，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。

[32] 详见下一部分的论述。

[33] 少有的例外见吴沈括《数据跨境流动与数据主权研究》，《新疆师范大学学报》（哲学社会科学版）2016年第5期。该章将本地化存储概括为刚性禁止流动模式、柔性禁止流动模式、本地备份流动模式。笔者认为吴教授的归纳以定性为主，相比之下，本章提出的严苛程度指标体系更为全面。

[34] 曹磊：《网络空间的数据权研究》，《国际观察》2013年第1期。

[35] 曹磊：《网络空间的数据权研究》，《国际观察》2013年第1期。

[36] The Personal Information Protection Act，http：//www.koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf.

[37] See Anupam Chander and Uyen P. Le，“Data Nationalism”，Emory Law Journal，vol. 64 （2015），p.694.

[38] Regulation （EU） 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data，and Repealing Directive? 95/46/EC （General Data Protection Regulation），http：//eur-lex.europa.eu/legal-content/EN/TXT/? uri=uriserv：OJ.L_.2016.119.01.0001.01.ENG&toc=OJ：L：2016：119：TOC.

[39] See Office of the Privacy Commissioner of Canada，Privacy Topics，

https：//www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp.

[40] Personally Controlled Electronic Health Records Act 2012，https：//www.legislation.gov.au/Details/C2012A00063.

[41] 我国台湾地区《个人资料保护法》，全文见http：//www.6law.idv.tw/6law/law/%E5%80%8B%E4%BA%BA%E8%B3%

[42] 我国台湾地区《个人资料保护法》第22条还规定：“主管机关或直辖市、县（市）政府为执行数据文件安全维护、业务终止数据处理方法、国际传输限制或其他例行性业务检查而认有必要或有违反本法规定之虞时，得派员携带执行职务证明文件，进入检查，并得命相关人员为必要之说明、配合措施或提供相关证明资料”；“主管机关或直辖市、县（市）政府为前项检查时，对于得没入或可为证据之个人资料或其档案，得扣留或复制之。对于应扣留或复制之物，得要求其所有人、持有人或保管人提出或交付；无正当理由拒绝提出、交付或抗拒扣留或复制者，得采取对该非公务机关权益损害最少之方法强制为之。”由此，在我国台湾地区，公权力可介入具体数据跨境传输安排的程度可见一斑。

[43] See Anupam Chander and Uyen P. Le，“Data Nationalism”，Emory Law Journal，vol. 64 （2015），p.699.

[44] 俄罗斯第242-FZ号联邦法律英文全文，见https：//pd.rkn.gov.ru/authority/p146/p191/.

[45] 关于俄罗斯通信和大众传媒部针对第242-FZ号联邦法律发布的一个无约束力澄清的综述，见http：//www.law360.com/articles/698895/3-things-to-know-about-russia-s-new-data-localization-law。

[46] Personally Controlled Electronic Health Records Act 2012，https：//www.legislation.gov.au/Details/C2012A00063.

[47] 支持这样理解的证据，见中国人民银行上海分行《关于银行业

金融机构做好个人金融信息保护工作的通知》（上海银发〔2011〕110号）中对“四、关于银行业金融机构向境外提供个人金融信息的问题”的解答：《通知》第6条规定：“除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。”为客户办理业务所必需，且经客户书面授权或同意，境内银行业金融机构向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规。银行业金融机构应当保证其境外总行、母行或分行、子行为所获得的个人金融信息保密。该文件全文可查询“北大法宝”数据库，http：//www.pkulaw.cn。

[48] Law on Payment and Security Settlement Systems，Payment Services and Electronic Money Institutions，Art.23，https：//www.bddk.org.tr/websitesi/english/Legislation/129166493kanun_ing

[49] See Anupam Chander and Uyen P. Le，“Data Nationalism”，Emory Law Journal，vol. 64 （2015），p.704.

[50] Decree No. 72/2013/ND-CP of July 15，2013，on the Management，Provision and Use of Internet Services and Online Information，Article 24，https：//www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF.

[51] DLA Piper，Data Protection Laws of the World. p.53，https：//www.dlapiperdataprotection.com/#handbook/world-map-section.

[52] The Federal Privacy Act 1988 and Its Australian Privacy Principles（especially Australian Privacy Principle 8—cross-border disclosure of personal information），https：//www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles#australian-privacy-principle-8-cross-border-disclosure-of-personal-information.

[53] The Office of the Privacy Commissioner for Personal Data of Hong Kong，Guidance on Personal Data Protection in Cross-border Data

Transfer，
https：//www.pcpd.org.hk/english/news_events/media_statements/press_201
有必要指出，目前香港个人数据保护法律中的规范跨境数据转移的章节至今未生效。

[54] DLA Piper，Data Protection Laws of the World. p.21，
https：//www.dlapiperdataprotection.com/#handbook/world-map-section.

[55] DLA Piper，Data Protection Laws of the World. p.212，
https：//www.dlapiperdataprotection.com/#handbook/world-map-section.

[56] DLA Piper，Data Protection Laws of the World. p.229，
https：//www.dlapiperdataprotection.com/#handbook/world-map-section.

[57] DLA Piper，Data Protection Laws of the World. p.327，
https：//www.dlapiperdataprotection.com/#handbook/world-map-section.

[58] DLA Piper，Data Protection Laws of the World. p.404，
https：//www.dlapiperdataprotection.com/#handbook/world-map-section.

[59] Personal Data Protection Act 2010，
www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf.

[60] Personal Data Protection Act 2012，
https：//www.pdpc.gov.sg/legislation-and-guidelines/legislation.

[61] 中国人民银行上海分行：《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》，全文见“北大法宝”数据库，
http：//www.pkulaw.cn。

[62] 几乎任何一本信息安全教材都会在第一章中介绍CIA三性，并将这三性奉为信息安全的基本原则。See Michael T. Goodrich and Roberto Tamassia，Introduction to Computer Security，Pearson，2014，pp.1-54.

[63] 另见《网络安全法》第10条规定：“建设、运营网络或者通过

网络提供服务，应当依照法律、法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。”该条文将网络数据的安全概括为完整性、保密性和可用性。

[64] 1890年美国法学家沃伦（Samuel D. Warren）和布兰戴斯（Louis D. Brandis）在《哈佛法律评论》上发表了题为《隐私权》（The Right to Privacy）的文章，首次提出隐私权概念。

[65] 谢远扬：《信息论视角下个人信息的价值——兼对隐私权保护模式的检讨》，《清华法学》2015年第3期。

[66] 王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，《现代法学》2013年第4期。另见王利明《隐私权概念的再界定》，《法学家》2012年第1期。

[67] 廖宇羿：《我国个人信息保护范围界定——兼论个人信息与个人隐私的区分》，《社会科学研究》2016年第2期。

[68] Orla Lynskey，The Foundations of EU Data Protection Law，Oxford University Press，2015，pp.91-106.

[69] 廖宇羿：《我国个人信息保护范围界定——兼论个人信息与个人隐私的区分》，《社会科学研究》2016年第2期。

[70] 对个人信息保护国际标准的综述，见洪延青、左晓栋《个人信息保护标准综述》，《信息技术与标准化》2016年第6期。

[71] 谢远扬：《信息论视角下个人信息的价值——兼对隐私权保护模式的检讨》，《清华法学》2015年第3期。

[72] 王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，《现代法学》2013年第4期。

[73] 见欧盟《通用数据保护条例》第二章。基本原则包括“合法、公平、透明原则”、“目的拘束原则”、“数据最小化原则”、“准确性原则”、“存储限制原则”、“安全原则”、“问责原则”。See Regulation （EU） 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data，and Repealing Directive 95/46/EC （General Data Protection Regulation），http：//eur-lex.europa.eu/legal-content/EN/TXT/？uri=uriserv：OJ.L_2016.119.01.0001.01.ENG&toc=OJ：L：2016：119：TOC.

[74] 见欧盟《通用数据保护条例》第三章。权利主要包括知情权、查询权、纠错权、删除权（被遗忘权）、限制数据处理的权利、携带数据的权利、反对数据处理的权利、不受对个人有显著影响的、以自动化方式做出的决定的权利等。

[75] 《阿里巴巴集团公布2016年9月底季度业绩》，http：//www.alibabagroup.com/cn/news/article？news=p161102。

[76] 《淘宝网：法律声明》，https：//www.taobao.com/go/chn/tb-fp/2014/law.php？spm=a21bo.50862.1997523009.38.26IY3m。

[77] Kevin Townsend，Kaspersky Lab Accuses Microsoft of Aggressive Attitude Towards Endpoint Security Firms With Windows 10，http：//www.securityweek.com/security-firms-allege-microsoft-anti-competitive.

[78] 习近平：《在网络安全和信息化工作座谈会上的讲话（2016年4月19日）》，新华网，http：//news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm。

[79] 孟斌、曹建海、姜炜、陈国强：《空置率为何成了机密》，《中国财富》2010年第10期。

[80] 见国家统计局《关于印发〈经济工作中国家秘密及其密级具体

范围的规定〉中有关统计工作条目的解释的通知》，http：//www.stats-fj.gov.cn/xxgk/fgwj/gfxwj/201211/t20121114_35768.htm。

[81]《住房空置率：一直在争论，从未有定论》，http：//gz.house.163.com/special/gz_kongzhilv/。

[82] 土耳其现有人口8000万。2016年4月，土耳其国家警察部门所持有的将近5000万土耳其公民的个人信息遭泄漏，并在黑市上售卖。这些数据中包含土耳其前任、现任国家领导人的个人和亲属信息。See Doug Olenick，50 Million Exposed in Turkish Data Breach，https：//www.scmagazine.com/50-million-exposed-in-turkish-data-breach/article/528739/。

[83] 胡锦光：《中国社会当务之急——把公权力关进制度的笼子》，《紫光阁》2014年第7期，http：//cpc.people.com.cn/n/2014/0714/c68742-25279102.html。另见王雅琴《德国公法的比例原则》，《学习时报》2014年11月3日第A2版。

[84] 代表性著述见：余凌云《论行政法上的比例原则》，《法学家》2002年第2期；蒋红珍：《论比例原则——政府规制工具选择的司法评价》，法律出版社，2010；杨登峰：《从合理原则走向统一的比例原则》，《中国法学》2016年第3期；刘权：《目的正当性与比例原则的重构》，《中国法学》2014年第4期。

[85] 杨登杰：《执中行权的宪法比例原则兼与美国多元审查基准比较》，《中外法学》2015年第2期。

[86] Mirko Hohmann，Tim Maurer，Robert Morgus and Isabel Skierka，Technological Sovereignty：Missing the Point？An Analysis of European Proposals after June 5，2013，http：//www.gppi.net/publications/global-internet-politics/article/technological-sovereignty-missing-the-point/.

[87] 见洪延青《“以管理为基础的规制”——对网络运营者安全保护义务的重构》，《环球法律评论》2016年第4期。

[88] See Anupam Chander and Uyen P. Le，“Data Nationalism”，Emory Law Journal，vol. 64 （2015），pp.718-721.

[89] 如前文所述，欧盟赋予个人被遗忘权，而被遗忘权在美国则不那么被认可。

[90] 天眼实验室《OceanLotus（海莲花）APT报告摘要》，http：//blogs.360.cn/blog/oceanlotus-apt/。在该报告中，360公司的安全团队揭露了从2012年4月起，某境外黑客组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。另见安全客《360追日团队APT报告：摩诃草组织（APT-C-09）》，http：//bobao.360.cn/learning/detail/2935.html。摩诃草组织是一个来自于南亚地区的境外APT组织，该组织已持续活跃了7年。摩诃草组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。相关攻击活动最早可以追溯到2009年11月，至今还非常活跃。在针对中国地区的攻击中，该组织主要针对政府机构、科研教育领域进行攻击，其中以科研教育领域为主。

[91] Lorenzo Franceschi-Bicchierai，The 10 Biggest Revelations From Edward Snowden’s Leaks，http：//mashable.com/2014/06/05/edward-snowden-revelations/#NSc.Xn8fSiq2.

[92] 欧洲方面提出的各种技术手段可参见：Mirko Hohmann，Tim Maurer，Robert Morgus and Isabel Skierka，Technological Sovereignty：Missing the Point? An Analysis of European Proposals after June 5，2013，http：//www.gppi.net/publications/global-internet-politics/article/technological-sovereignty-missing-the-point/.

[93] European Commission，European Commission launches EU-U.S.Privacy Shield：Stronger Protection for Transatlantic Data Fows（Press Release on12 July 2016），http：//europa.eu/rapid/press-release_IP-16-2461_en.htm.

[94] 第39条规定：“国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估……”

[95] 《全国范围关键信息基础设施网络安全检查工作启动》，中国网信网，http：//www.cac.gov.cn/2016-07/08/c_1119185700.htm。

[96] 按照全国人大法工委的修改说明，增加“重要业务数据”的原因是“有的地方、部门和社会公众提出，关键信息基础设施运营者的重要业务数据也应存储在境内”。参见《网络安全法（草案二次审议稿）全文》，中国人大网，http：//www.npc.gov.cn/npc/flcazqyj/2016-07/05/content_1993343.htm。

第八章

全球互联网关键资源管理中的主权问题

积极把握国际互联网治理体系发展变革期的历史机遇，深度参与国际互联网治理和全球互联网资源管理规则制定，提升我国在相关领域的影响力和话语权，是维护我国网络主权，推动全球互联网关键资源管理向公平、合理、稳定、有序方向发展的重要举措。

互联网是基于信任和平等互惠原则，由众多网络自愿加入形成的格局，这造就了互联网全球化、跨边界特性与网络主权原则并存。域名是互联网的关键资源，域名系统是互联网的“中枢神经系统”，其良好运转直接关系着互联网的持续安全稳定运行。根位于域名系统顶端，根区管理决定了顶级域能否正确解析，其管理模式是各方关注的焦点，美国政府也在其中持续施加主权影响。

作为国际互联网治理和全球互联网关键资源管理的核心平台，美国非营利机构ICANN遵循私营部门主导、多利益相关方的治理模式，政府部门的作用被其显著弱化，ICANN承担的根区管理及顶级域发展与管理政策制定职责无一例外地与主权问题密切相关。积极把握国际互联网治理体系发展变革期的历史机遇，深度参与国际互联网治理和全球互联网资源管理规则制定，提升我国在相关领域的影响力和话语权，是维护我国网络主权，推动全球互联网关键资源管理向公平、合理、稳定、有序方向发展的重要举措。

一 全球互联网关键资源管理主权问题概述

（一）互联网全球化、跨边界特性与网络主权原则并存

互联网由冷战催生，自1969年互联网的雏形“阿帕网”（ARPANET）建立以来，历经近半个世纪的发展，走过了一条军用、科研、商用、民用的道路，从美国本土扩展到全球各个国家和地区，与经济社会各领域不断融合发展，极大地改变了人们的生产生活方式。尽管互联网诞生于美国，但其全球发展和普及应用，则得益于互联网“对等互联”的内在特性和基础协议，是各个国家和地区借助以TCP/IP协议为代表的先进网络技术，基于信任和平等互惠原则，将本国信息基础设施与他国进行互联互通的共同历史选择。利用TCP/IP协议的标准接口，各个国家和地区、基于任何技术的区域网络实现了组网互联，同时区域网络内部（自治域）仍可维持各自的技术架构和管理方式，形成了“万网之网”（Network of Networks）。现实世界与互联网的交融，使得现实世界的主权原则向互联网延伸（即网络主权），形成了当今互联网全球化、跨边界特性与网络主权原则的并存。

（二）根位于域名系统顶端，具有全球域名解析锚点作用

作为互联网的关键资源，域名是用于互联网上识别和定位计算机的层次结构式的字符标识，与该计算机的互联网协议（IP）地址相对应。域名系统（DNS）是互联网运行的关键基础设施，通过域名与IP地址之间的对应关系，为人们提供基于互联网的通信服务。域名系统采用倒置的树形结构自顶向下构建名称，通过分级授权、各域自治的方式进行管理。根域（简称“根”）位于DNS的顶部；其下为顶级域，包含国家和地区代码顶级域（ccTLD）、通用顶级域（gTLD）两类；顶级域下依次设立二级域、三级域等。我国国家顶级域“.CN”即属于ccTLD，具有国家主权含义。[1]作为互联网的“中枢神经系统”，DNS的良好运转直接关系着互联网的持续安全稳定运行，进而影响互联网的创新与健康发展。

自20世纪80年代设立以来，根就是域名系统的构建起点与全球解析的信任锚点，在全球互联网基础设施和关键资源管理中具有突出地位，2010年根系统完成域名系统安全扩展（DNSSec）[2]部署后，进一步强化了其作为最高信任源（即锚点）的地位和作用。此外，在多语种域名（IDN）支持、新顶级域扩展等方面，根系统发挥了无可替代的引领作用。

（三）根区管理涉及网络主权，是国际互联网治理的焦点

域名根系统由以管理数据为主的根区管理系统和以提供解析服务为主的根服务器系统共同构成。其中：

根区管理系统是整个根系统的唯一数据源，主要承载记录有顶级域名及其IP地址对应关系信息的根区文件。根区管理工作主要包括完成根区文件的修改和生成（含顶级域的设立、删除及运营机构变更）、将更新后的根区文件写入根区数据库服务器并分发给所有的根服务器等。根区文件的修改、生成和分发情况直接决定了顶级域能否正确解析，进而影响互联网的正常使用，因此根区管理模式一直是国际互联网治理的焦点。出于互联网起源和发展的历史原因，根区管理长期受美国政府监管，由美国机构执行。写入根区的ccTLD能否得到妥善管理，直接关系到国家主权和国家网络安全，主权国家对于根区文件是否会被恶意篡改、删除从而导致本国顶级域无法实现全球解析（他人无法访问该顶级域及其下设域名），始终存在担忧和戒备。

根服务器系统由各根服务器及其镜像服务器组成，根据接收到的根区文件，向用户提供访问并获取这些顶级域权威数据的“渠道”和“入口”。根服务器运行机构负责管理各自的根服务器，相互之间独立且地位平等，均以志愿者方式提供解析服务，对接收到的根区数据无修改权限，使得各根服务器所提供的数据内容完全一致，不受地理位置及运行机构性质的影响。为提高解析性能与安全性能，根服务器运行机构可根据需要在全球其他地理位置设立镜像服务器，每个根服务器与其镜像服务器使用相同的IP地址，以分布式集群形式提供顶级域解析服务。各根镜像服务器无权修改根服务器运行机构分发的根区数据。根服务器及镜像服务器的解析服务遵守全球统一的技术规范，不受地理位置及运行机构性质的影响，不涉及主权问题。

（四）ICANN是国际互联网治理和全球互联网关键资源管理的核心平台

ICANN是总部位于美国加州的非营利性私营机构（公司），负责互联网号码分配管理（IANA）职能运行工作，包括全球互联网域名系统根区日常管理、互联网号码资源（IP地址和自治域号码）协调分配、互联网协议参数（如端口号）维护，以及与域名和IP地址发展与管理相关的政策制定，是国际互联网治理和全球互联网关键资源管理的核心平台。

根区管理是IANA职能的核心，在2000～2016年间，ICANN通过与美国政府签署合同获得美国政府的授权，负责维护根区文件并接受美国政府的监督。根区文件的修订需经美国政府审核后才能写入由美国公司威瑞信（VerSign）维护的根区数据库，再分发给根服务器运行机构用于开展全球解析服务。

ICANN所坚持的私营部门[3]主导、多利益相关方参与的治理模式，仍不能缓解国际社会对美国单边控制互联网关键资源的质疑，要求在联合国框架下管理互联网的呼声一直存在。随着美国政府于2016年10月1日将IANA职能管理权移交给ICANN为代表的全球互联网多利益相关方社群（简称IANA移交），美国政府正式退出根区管理事务，全球迎来了互联网关键资源管理制度的重大调整。

近年来，为鼓励创新、促进竞争和增加用户选择，ICANN启动了新gTLD计划，以在域名空间成批引入gTLD。ICANN关于gTLD的发展和管理政策，决定了相关顶级域能否在快速发展中充分保障公共利益，避免引发国家主权及其他敏感问题和危害国家信息安全，因而受到政府的普遍重视。政府部门作为利益相关方之一，通过加入ICANN设立的政府咨询委员会（GAC）[4]，参与全球域名发展与管理政策制定工作；同时依据本国或地区法律法规和规定，对本国或地区域名行业开展管理，维护网络主权。

总体来讲，网络主权在全球互联网关键资源管理领域的具体体现包括：各国家具有自主选择域名行业发展、本国家顶级域管理方式以及平等参与国际互联网治理和全球互联网资源管理的权利；各国政府具有自主制定本国互联网公共政策及法律法规和规定，并依法对本国域名、域名服务的基础设施和域名服务活动实施行业管理的权利等。

二 主权影响下的根区管理模式历史沿革

在域名系统30多年的发展历程中，美国主权的影响持续存在，集中体现在美国政府在根区管理中的作用，即由项目资助者向监管者角色转变，加强对根区的全面控制，大力防范国际电信联盟、欧盟等政府间组织及其他国家和地区政府部门对管理权的争夺等。在这一影响下，全球根区管理的变迁大体经历了五个主要发展阶段：一是在美国政府资助下，由John Postel为代表的技术专家与美国斯坦福国际研究院（SRI）

共同负责的民间管理阶段；二是非军用互联网独立发展，以技术专家为代表的民间社群与美国政府争夺管理权的阶段；三是美国政府为缓解矛盾设立私营机构ICANN，但继续强化根区管理监管的阶段；四是基于对美国单边控制全球互联网关键资源的不满，全球围绕互联网治理模式的持续斗争阶段；五是为扭转“棱镜门”事件的不利影响，美国政府推动完成IANA移交，带来根区管理新模式的阶段。

（一）美国政府科研资助阶段

20世纪80年代，随着域名系统的诞生，最初的根区管理工作主要由美国南加州大学信息科学研究所（USC/ISI）的John Postel教授团队以及美国斯坦福国际研究院（SRI）分工负责。美国国防部国防高级研究计划局（DARPA）则作为相关科研项目的资助者，通过合同方式分别为两方开展根区管理工作提供资金支持。

作为技术专家、域名系统创始人之一以及IANA的创始人，John Postel与其他科研人员共同以民间、公益、免费的方式管理或协调使互联网正常运行的众多标识符，包括根据需求分配互联网地址、协议参数和主机名称/域名，设计和分配gTLD和ccTLD，开展根系统管理等，形成了早期的互联网关键资源发展和管理规则。

SRI也基本延续域名系统出现之前的职责，维护写有主机名称/域名和IP地址对应关系的host.txt列表并定期发布，还提供顶级域和二级域域名注册、维护域名注册数据库等。

美国DARPA、美国国家科学基金会（NSF）、美国国家航空航天局（NASA）、能源部、卫生和人类服务部等多个政府部门于1987年联合组建了联邦研究互联网协调委员会（FRICC），以加强对互联网研究的资助。

（二）美国政府介入、民间社群与美国政府争夺管理权阶段

1990年，美国NSF、NASA、能源部等政府部门联合组建了联邦网络委员会（FNC），并将当时的互联网社群纳入FNC的咨询委员会，开始参与对互联网特别是根区的管理。随着互联网由军事用途逐步拓展至科研和民用领域，非军用互联网得以拆分出来，与军用部分区别发展和管理。美国政府对民用网络日益关注，进一步由互联网项目资助者向监管

者角色转变。

1991年，一个拥有美国政府背景的公司Network Solution（NSI）成为军用互联网合同的转包商，接管了SRI此前负责的绝大部分工作。后来，NSI基于这一短暂运营经验，又于1993年获得美国政府的非军用互联网域名和地址注册服务合同，开始负责根区文件的生成和分发、向非军用网络及互联网用户提供顶级域名注册服务等，与John Postel负责的IANA共同开展根区管理。1997年，IANA 职能被记录于美国能源部的Tera-node网络技术合同工具之中。[5]

NSI对域名的销售加速了互联网商业化，美国政府日益关注甚至涉足互联网日常管理，使互联网创立者们最初坚持的一个平等、开放的互联网环境受到了威胁。为了将互联网的发展路径重新扭转到“由无私的计算机专家运作的、开放的、非商业化的、为全人类利益而存在的网络”上来，他们开始采取行动试图夺回管理主导权。

1992年1月，Vin Cerf、John Postel等人成立了国际互联网协会（ISOC），宣称互联网管理权属于全球社群，该非营利性组织才是互联网领域真正的管治权威。ISOC于1996年联合互联网架构委员会（IAB）、IANA、国际电信联盟（ITU）、世界知识产权组织（WIPO）、世界商标协会（INTA）、NSF等成立“国际特别委员会”（IAHC），研究并发布了“通用顶级域谅解备忘录（gTLD-MoU）”，对顶级域分配和管理规则等提出建议，并获得了大量的业内支持。[6]然而，美国政府担心ISOC被ITU利用，成为其他政治体（特别是欧盟）控制互联网的工具，因此先后约见Vin Cerf和John Postel，表明美国政府基于国家主权和网络安全，坚决维护互联网控制权的明确立场，并反对gTLD-MoU。

1998年1月，美国政府将互联网域名管理权转移至美国商务部。出于对美国政府管控互联网的不满，John Postel以运行测试为由，指示各根服务器运行机构将根区文件同步地址由NSI转而指向自己管理的IANA地址，12家根服务器运行机构中的8家都遵从这一指示，使John Postel成功挑战了美国政府权威，将全球互联网一分为二。但在美国政府的高压之下，John Postel承认错误并且很快取消了之前做出的变动，美国政府再度掌握了全部13台根服务器。

（三）美国政府加强管控阶段

为了杜绝根服务器挟持等类似事件再度发生，美国商务部国家电信和信息管理局（NTIA）于1998年1月发布《加强互联网域名和地址技术管理的方案》（即“绿皮书”）并公开征求意见，其中强化了美国政府对IANA乃至整个互联网的管理。同年6月，“绿皮书”的修改稿《互联网域名和地址管理政策声明》（即“白皮书”）正式发布，其中表明了美国政府将治理权归还互联网社群的姿态，作出域名系统私营化承诺，一定程度上缓解了与民间社群的矛盾，并在事实上否定了国家间协商或者国际组织治理的模式。

白皮书催生了ICANN这一私营部门主导的非营利机构。1998年9月，ICANN在美国加州洛杉矶成立。10月，John Postel因心脏衰竭去世，年仅55岁。11月，美国商务部与ICANN签署谅解备忘录，授权ICANN执行IANA职能。12月，南加州大学将IANA移交给ICANN，IANA成为ICANN机构内部的独立部门。此外，随着2000年美国VeriSign公司对NSI的收购，NSI在互联网领域的相关职能和资源随即转入VeriSign。NSI与美国政府关于IANA的合同于2000年到期，之后美国政府开始与ICANN签署IANA职能合同。

美国商务部通过与ICANN和NSI/VeriSign分别签署合同，[7]对两机构涉及根区管理的有关职能进行授权，同时依法对相关职能实施情况开展监管，并保留了其下设的国家电信和信息管理局（NTIA）作为根区文件变更的“最终授权机构”，实现了美国政府对根区管理的强化管控，形成了“美国政府（NTIA）监督-ICANN（IANA）运行-VeriSign维护”的三级根区管理模式。其中，ICANN（IANA）继续负责根区日常管理，包括接收有关设置、删除顶级域或变更顶级域运营机构的申请（即根区文件的变更申请）、进行申请材料初审、将工作流程推送至根区管理的其他参与者（即NTIA和VeriSign）、维护根区注册数据库等，相关程序与我国开展的行政审批工作极为相似。可以说，ICANN接替John Postel成了根数据源。NSI/VeriSign则获得了根区文件的修改权，并继续负责根区文件生成、全球根区数据库系统维护以及根区文件的分发。

（四）全球围绕互联网治理模式持续斗争阶段

ICANN所坚持的私营部门主导、多利益相关方的治理模式，仍不能缓解国际社会对美国单边管控互联网关键资源的质疑，有关互联网治理模式之争持续了十余年。与多利益相关方模式相竞争的是一种国家间多边治理模式，代表了各主权国家作为互联网治理主体实现平等参与的模

式。

2005年6月，NTIA发布《美国关于互联网域名和地址系统的原则声明》，宣布为保护域名系统的安全与稳定，美国政府将维持其在根区管理的权威地位。同年7月，美国国会宣布商务部长继续保持对ICANN的监督。

美国的强硬态度激起欧盟及广大发展中国家的强烈不满，2003年和2005年分两阶段召开的信息社会世界峰会（WSIS）上，欧盟、我国及其他一些发展中国家提出由联合国下属的政府间组织（如ITU）接管域名管理权。作为交换条件，美国政府同意由联合国秘书长设立一个开放性论坛，即互联网治理论坛（IGF），为各方提供有关国际互联网治理问题的交流和磋商平台。但IGF议而不决的性质决定了其难以成为国际互联网治理和政策制定的核心平台，整体来看仍符合美国利益。

此后，印度、巴西和南非于2011年9月召开峰会，提出将互联网治理权转移至联合国互联网相关政策委员会（称为IBSA提案）。同一个月，以中俄等为成员国的上海合作组织向第六十六届联合国大会提交了信息安全国际行为准则，[8]旨在推动多边互联网治理规则制定。2012年，国际电信世界大会（WCIT-12）对新修订的《国际电信规则》（ITR）进行审议，由于ITR中增加了互联网治理的相关内容，挑战了以美国为首的西方发达国家拥护的互联网多利益相关方治理模式，ITR遭到这些国家的强烈反对，最终经89个成员赞成通过，另有55个成员拒绝签字。ITR引发的阵营对立促成美国对互联网治理进行反思，并成为后来2014年启动移交的起点。2013年6月，“棱镜门”事件爆发，各国对美国管理互联网的不信任度到达顶点。根区管理问题也因此再次升温，要求对ICANN及IANA进行改革的声音显著提升。2013年11月，ICANN、ISOC、IETF、RIRs等互联网技术社群联合发表《蒙得维的亚宣言》，推动关键资源管理私营化。2014年4月在巴西举办的“有关互联网治理的未来的全球多利益相关方会议”（NETmundial会议）上，俄罗斯等国继续表达对美及ICANN的不满。

（五）美国政府退出监管阶段

为了积极扭转“棱镜门”事件带来的不利影响，NTIA于2014年3月宣布有条件地将IANA职能管理权移交给全球社群（即ICANN）。ICANN随即设立工作组并建立相关工作机制，开展IANA职能管理权移交方案和加

强ICANN问责制方案的研究制定工作。经过近两年的研究筹备，ICANN董事会于2016年3月代表全球社群向NTIA提交了两个方案，NTIA随即会同十多个美国政府部门进行评估，于6月发布评估报告并宣布两个方案符合相关条件。

随着美国总统选举临近，部分美国国会共和党议员及国内保守派力量，以IANA移交作为手中的工具和博弈的筹码，极力宣扬美国对互联网诞生和发展的巨大贡献以及美国政府对互联网的所有权和管理权，并将攻击对象指向奥巴马政府，以破坏互联网自由、非法转移美国政府财产、违规使用财政资金等为由，多方阻挠IANA移交。NTIA等美国政府部门则采取积极应对措施，推动实现了IANA职能管理权于10月1日按期移交，兑现了其域名系统私营化承诺，成为全球互联网关键资源管理制度的重大进步。

全球互联网根区管理模式相应调整，形成了“ICANN（社群）监督-PTI（IANA）运行-VeriSign维护”的新三级管理模式。其中，美国政府不再直接介入根区管理相关事务，但在退出前确保了ICANN通过机构章程及相关机制，维持美国机构属性；ICANN通过与其新成立的子公司PTI签署合同，[9]授权PTI履行ICANN此前负责的根区日常管理职责；通过与VeriSign签署合同，[10]授权其继续负责根区文件的修改和生成、全球根区数据库维护以及根区文件分发；ICANN则通过设立社群监督机制和对PTI董事会任职进行控制，直接或间接地对根区管理相关工作情况进行监督。美国政府的退出并未改变美国机构持续把控全球根区的现状。

三 从主权维度看顶级域发展与管理政策

（一）全球域名管理体系的主权体现

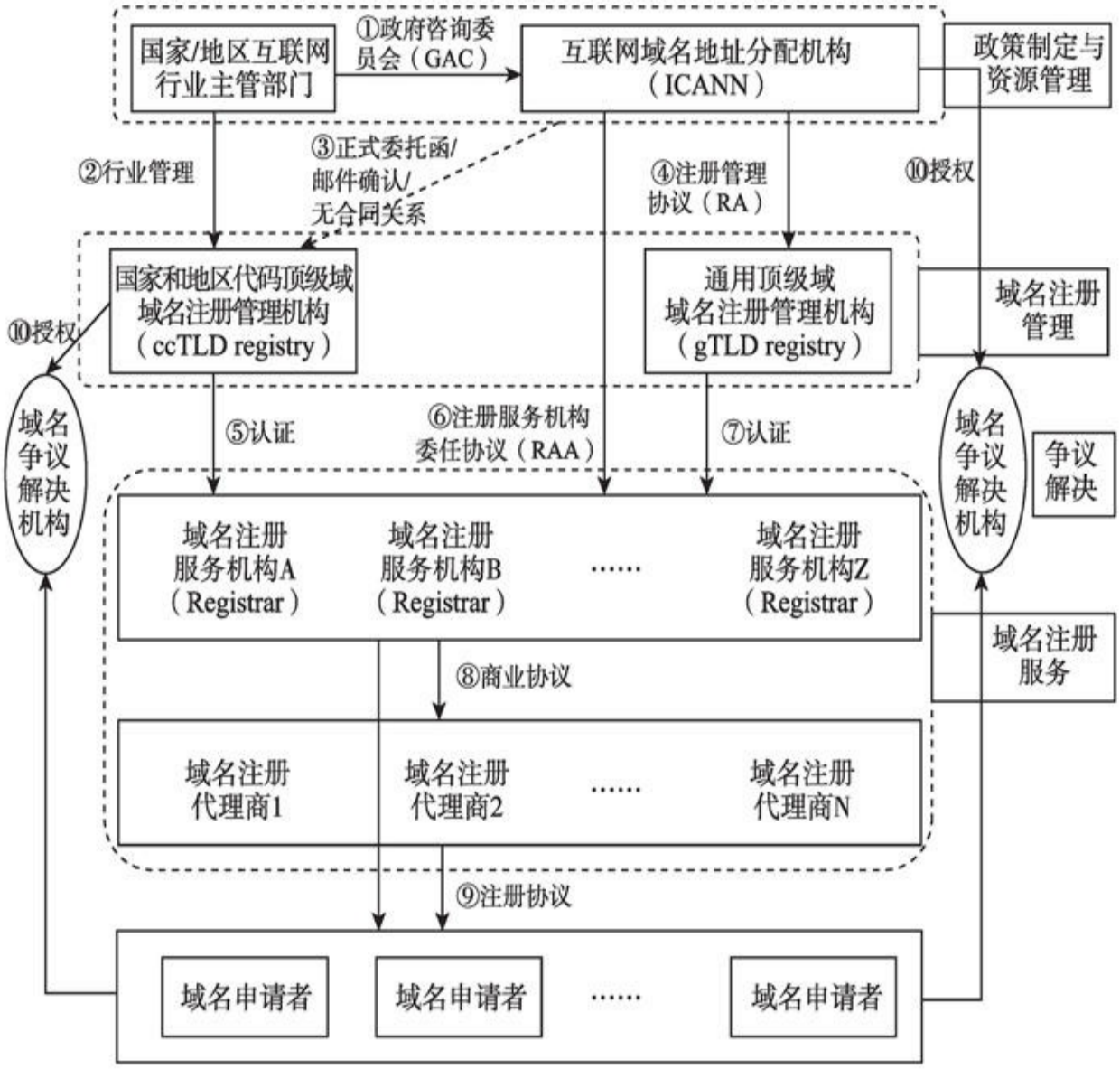

图8-1 全球互联网域名管理架构图

资料来源：CAICT。

与域名系统相对应，全球域名管理体系具备层次化的结构，主要分为政策制定与资源管理、域名注册管理、域名注册服务和争议解决四个方面，分别对应四类责任主体。

1.域名政策制定与资源管理机构

（1）ICANN负责全球互联网资源管理及其政策制定

作为国际互联网治理和全球互联网资源管理的核心平台，ICANN采用私营部门主导、多利益相关方参与的治理模式和自下而上、协商一致的政策制定流程。董事会为ICANN的最高权力机构，ICANN的最终决策由董事会制定；ICANN还设有三个支持组织，分别负责起草与ccTLD、gTLD和IP地址发展与管理相关的全球政策；设有四个咨询委员会，负责就互联网相关政策建议提供咨询意见。

与联合国框架下的政府间平台不同，ICANN并不能实现网络主权原则关于各个国家和地区对国际互联网治理和全球互联网资源管理的平等参与权利。2016年，ICANN上述重要组成机构的133个有表决权职位中，来自美国的任职人员占比接近1/3，其他国家占比则均不足6%，我国仅有2.3%。这一差距一定程度上源于互联网起源和发展的历史原因，也与地理区域划分（全球五大地理区域中，北美地区仅包含2个国家）、语言（英语为工作语言）、各国家和地区的重视程度等有关。

（2）政府在ICANN中作用有限，但具有本国或地区行业管理权

在ICANN的治理模式下，ICANN对与私营部门相对立的政府部门的角色作出了严格限定。IANA移交后，政府部门的作用仍然被显著压制，甚至弱化。根据2016年10月生效的ICANN新版章程，ICANN承诺“保持植根于私营部门性质，同时要认识到政府和公共权力机构是制定公共政策的责任主体，需适时考虑政府和公共权力机构提出的公共政策建议”[11]。政府部门仅可作为利益相关方之一参与ICANN，并且参与渠道非常有限。除四个咨询委员会之一的政府咨询委员会（GAC）专为各个国家、地区和经济体的政府机构、政府间组织及国际条约组织而设外，ICANN董事会等很多重要职位选任条件已明确规定政府部门相关人员不得任职，因此政府部门通常只能通过GAC和公众评议等方式对ICANN相关政策提出意见和建议，但不具有政策制定权和最终决策权，可发挥的作用非常有限。

根据ICANN新版章程，董事会需要适当考虑GAC建议，特别是对于GAC内部无争议（即大多数国家/地区/经济体同意且无反对意见）的共识建议。董事会全体有表决权成员（共16人）中，需至少有60%的成员表决反对才能拒绝接受GAC共识建议；若拒绝接受GAC建议，董事会随后将与GAC及时、有效且诚恳地尝试寻求双方都可接受的解决办法；若找不到这样的解决办法，董事会将在其最终决策中说明未采纳GAC建议的理由。然而，因GAC内部各国家和地区在互联网发展和治理方面的开放

程度不同，在许多关键问题上，GAC共识建议的达成存在相当大的难度，对于董事会接受相关政府部门建议更为不利。各个国家和地区政府部门普遍希望提高GAC地位，提升政府部门在ICANN事务特别是互联网关键资源管理政策制定中的影响力。

此外，与网络主权原则相一致的是，各个国家和地区政府部门可制定本国或地区相关法律法规和规定，并依法对本国或地区的域名、域名系统基础设施和域名服务活动实施行业管理。目前，我国负责互联网域名行业的主管部门为工业和信息化部，依据《中国互联网络域名管理办法》及相关法律法规和规定，与各省、自治区、直辖市通信管理局共同开展域名行业监管，并对在境内设立根服务器及其镜像服务器、设立域名注册管理机构和域名注册服务机构实行许可管理。工业和信息化部代表中国政府派出人员担任GAC成员并参与GAC事务，2016年11月，中国GAC代表当选GAC副主席，一定程度上提升了我国在国际互联网治理和互联网关键资源管理领域的参与度和影响力。

2.域名注册管理机构与域名注册服务机构

域名注册管理机构（即顶级域运营机构）承担顶级域运行和管理职能，主要分为gTLD域名注册管理机构和ccTLD域名注册管理机构。顶级域经ICANN（IANA）、VeriSign执行入根和根区文件分发等操作后，方可实现全球解析。考虑到美国对其专用顶级域“.GOV（政府）”、“.MIL（军事）”、“.EDU（教育）”拥有主权，除上述顶级域外，ICANN与其他的gTLD域名注册管理机构签订注册管理机构协议（RA），对各域名注册管理机构进行授权。

域名注册服务机构直接面向互联网用户提供域名注册服务，负责受理域名注册申请并完成域名在顶级域名数据库中的注册。提供gTLD域名注册服务的机构需要取得ICANN的资质认证，并与ICANN签订注册服务机构委任协议（RAA）。与此同时，还需要得到相应gTLD域名注册管理机构的资质认证，并签署注册管理机构-注册服务机构协议（RRA）。提供ccTLD域名注册服务的机构需要得到相应ccTLD域名注册管理机构的资质认证，但不要求必须获得ICANN的资质认证。

3.域名争议解决机制

对于gTLD域名争议，通常由经ICANN授权的域名争议解决机构[12]依

据ICANN制定的《统一域名争议解决政策》（UDRP）或统一快速暂停政策（URS）进行仲裁。对于ccTLD域名争议，相应的域名争议解决机构一般由本国或地区域名注册管理机构授权。[13]域名争议还可通过辖区法院进行调解或裁决。此外，为了加强对商标持有人权利的保护，ICANN制定了商标权益保护机制（RPM），并建立了全球商标信息交换中心（TMCH），旨在纠纷发生前就开始保护商标权并为权利人提供良好的信息渠道，实时掌握商标在网络空间的保护情况。

（二）ccTLD发展与管理政策的主权体现

1.主权国家使用的ccTLD属于国家主权

信息社会世界峰会（WSIS）的决议规定，（主权国家使用的）ccTLD属于各国主权。根据《突尼斯议程》第63条的表述，“一个国家不应该参与和另一个国家的ccTLD有关的决策。每一个国家在影响其ccTLD决策方面以各种方式表达和确定的合法利益均需要通过一个灵活和经改善的框架得到尊重、维护和解决”[14]。具体实施上，各国家和地区有权自行指定本国或地区的ccTLD域名注册管理机构和域名注册服务机构，自行制定相关管理政策并开展行业监管，自行选择相关技术方案和运营模式等。就我国而言，经工业和信息化部批准，中国互联网络信息中心（CNNIC）为我国国家顶级域的域名注册管理机构，负责运营、维护和管理我国的国家顶级域，并制定相关管理细则、指定域名争议解决机构等。仅“.CN”和“.中国”为代表主权国家的国家顶级域，港澳台地区均可设立ccTLD，但其顶级域所对应的地区代码明确说明该地区为中国领土的一部分，如TW明确解释为指代中国台湾，是中国的一个省。

ccTLD 域名注册管理机构可通过ICANN内部设立的国家和地区域名支持组织（ccNSO）等方式，参与起草全球ccTLD域名发展和管理政策；其他各方可通过ICANN设置的公众评议渠道或参与ICANN其他组成机构，对ccTLD相关政策提供意见和建议。例如，ccNSO联合GAC共同成立的“授权和重授权”工作组，研究制定了ccTLD设置、运营机构变更和退出政策；ccNSO联合GAC、用户咨询委员会（ALAC）等共同成立的解释框架（FOI）工作组，对上述政策的规则与流程作了进一步解释和规范，以确保IANA及其他流程参与方在涉及ccTLD的根区管理工作中规范操作。

2.ccTLD设置、运营机构变更和退出政策

根据字符串类型的不同，ccTLD可分为ASCII码ccTLD和多语种ccTLD（IDN ccTLD）。其中，前者需严格遵循ISO 3166-1两字符国家和地区ASCII码标准进行命名；[15]后者则基于ISO 3166-1所列出的国家和地区，对国家和地区名称按相应语言翻译形成，并根据ICANN 2009年11月启用的IDN ccTLD快速通道流程操作。

为了接入国际互联网，各国家和地区需要向ICANN（IANA）提交本国或地区的ccTLD设置申请及相关证明材料，充分证明该ccTLD字符串具有合规性，运营机构拥有合法资质、政府部门及利益相关方的支持以及相应的技术、运营和管理能力等，以确保该ccTLD的引入不会导致域名系统出现安全性、稳定性问题，同时该机构能够有效、公平运营该ccTLD，并符合该国或地区的公共利益等。经综合评估，以及IANA及ICANN董事会的审核批准，该ccTLD即可完成入根程序并实现全球解析。对于变更现有ccTLD运营机构的情况，申请者除了提交与设置ccTLD类似的相关材料外，还需要额外提供安全平稳开展业务和用户转移的方案等。

ccTLD的退出则往往源于相应国家或地区的政权变故，导致该ccTLD的ASCII码不再包含于ISO 3166-1列表中，或多语种字符串无法再对应于ISO 3166-1列表中包含的国家或地区。对此，运营机构需制定稳妥的转移和退出方案，并向IANA提交申请。

我国的国家顶级域“.CN”于1990年11月完成全球注册（当时由IANA分配，国外机构代管），后经友好沟通移交CNNIC管理。1994年4月，我国全功能接入国际互联网，为我国互联网发展迈出了坚实的一步。我国的中文顶级域“.中国”随后于2010年6月获得ICANN批准并写入根区，对满足我国互联网用户语言和文化习惯、促进我国互联网普及和数字经济全面发展起到了积极的推动作用。

3.涉及ccTLD的根区管理安全风险问题

ccTLD属于国家主权，与国家政治、军事和安全等问题密切相关。鉴于域名系统根区在互联网中的重要地位，根区管理可能引发的安全风险一直是国际社会关注的焦点。

（1）美国政府监管下的根区管理安全风险

其一，根区管理主体和管理模式。

在IANA职能移交前，全球域名系统根区采取“美国政府（NTIA）监管-ICANN（IANA）运行-VeriSign维护”的三级根区管理模式。考虑到美国政府对根区文件变更申请拥有“最终审核”这一关键权力，同时ICANN与VeriSign同为美国注册的公司，共同接受NTIA合同约束和美国司法管辖，理论上存在某一国家或地区ccTLD数据在根区文件中遭到恶意删除、篡改或劫持，导致该国或地区互联网瘫痪甚至从国际互联网“消失”的极端情况。美国政府、ICANN与VeriSign能否采取中立态度，正当、公平、合理地对待各ccTLD，长期以来受到各个国家和地区的密切关注和积极戒备。

考虑到域名系统及其中的根系统基于信任关系而服务于全球所有互联网用户，一旦美国政府或相关机构采取单方面恶意删除或劫持某ccTLD的行为，所需承担的国际压力和造成的负面影响巨大，将彻底破坏各国家和地区对现有根系统的信任，美国政府多年来树立和坚守的以ICANN为代表的互联网多利益相关方治理模式也将存在延续危机，因此这一风险微乎其微。

其二，伊拉克、利比亚国家顶级域停止解析事件始末。

2002年伊拉克国家顶级域“.IQ”停止解析、2004年利比亚国家顶级域“.LY”一度瘫痪等事件发生后，都有观点认为是美国政府出于政治和军事目的采取的行动。然而，各方面的证据证明，两事件的发生主要源于相应ccTLD运营机构主动停止了服务，此后均通过ICANN的ccTLD重授权程序完成了运营机构的变更，并随即恢复了服务。[16]

1997年，伊拉克的通信网络基础设施落后，且没有运行域名系统的能力，John Postel作为当时的IANA，将伊拉克国家顶级域“.IQ”授予了位于美国德克萨斯州的InfoCom公司。该公司的Bayan Elashi是一名巴勒斯坦籍的计算机科学家，承担“.IQ”顶级域管理的技术工作，并担任“.IQ”联系人。2002年12月（“9·11”事件发生后），Bayan Elashi被捕。2004年7月，Bayan Elashi和他的四个兄弟以及InfoCom被判有罪，罪名包括违反了利比亚制裁法令、为恐怖组织洗钱等，导致“.IQ”域名服务被该公司关停。由于“.IQ”域名注册量不高，其停用并未对全球互联网使用产生很大的影响。2004年7月，伊拉克过渡政府正式联系ICANN讨论“.IQ”顶级域重新授权的问题。2004年12月，总理Allawi致信ICANN，将国家通信和传媒委员会（NCMC）指定为代表伊

拉克运营“.IQ”顶级域的机构。在收到NCMC递交的“.IQ”重授权申请材料后，经综合评估，ICANN于2005年6月将“.IQ”的运营机构变更为NCMC，“.IQ”自此恢复服务。

1997年4月，John Postel将“.LY”授予了利比亚一家名为Alshaeen for Information Technology的公司运营，该公司几年后倒闭。此后英国公司Lydomains承接了“.LY”的域名运营和销售工作，“.LY”域名服务器运行则委托给Magic Moments公司。2002年，两家公司出现合作矛盾，Magic Moments公司于2004年4月停止了“.LY”域名服务器的解析服务。2003年，利比亚邮电总公司在利比亚政府的支持下向ICANN提出了申请，要求将“.LY”重新授权给利比亚邮电总公司。经详细调查和综合评估，ICANN最终于2004年6月批准将“.LY”的运营机构变更为利比亚邮电总公司，该公司运营“.LY”直到今天。

（2）美国政府退出监管后的根区管理安全风险

IANA移交后，美国政府不再具有根区管理的相关职能，全球域名系统根区采取“ICANN（社群）监督-PTI（IANA）运行-VeriSign维护”的新三级管理模式。美国政府在根区管理角色的退出，以及ICANN透明问责情况的改善和全球社群监督能力的提升，进一步降低了某一国家或地区ccTLD被恶意删除、篡改或劫持的风险。

即使这一极端情况真的发生，由于域名系统分层分级的特点，通过境内递归服务器的设置更新或者启动应急机制，也可在较短时间内实现解析服务的平稳过渡，影响主要在于境外用户无法解析受到攻击的ccTLD及其注册域名。

（3）本国ccTLD遭他人接管风险

近年来，美国多家法院接到关于扣押和接管某些国家ccTLD的诉讼请求，具体涉及伊朗、叙利亚、朝鲜等国的ccTLD。通过案件审理，美国法院最终均支持ICANN意见，确定ICANN只是域名系统的技术协调机构，ccTLD并非其财产，无法被扣押和接管，并驳回了相关诉讼。[17]

与根区文件ccTLD数据被恶意删除、劫持的后果相同，若法庭同意并执行了相关诉讼人请求，使ICANN及VeriSign按照法庭要求，利用其根区管理职能将该ccTLD数据进行修改，从而导致该国ccTLD遭到他人接

管，那么自20世纪80年代以来各方对根系统建立的信任和当前互联网这种由众多网络“自愿加入”根区形成的格局将彻底崩塌，许多机构将转而建立替代的域名系统和分离的根，互联网也将进入碎片化时代。但考虑到目前已有案例可供参照，某一国家或地区的ccTLD遭他人接管的风险已经微乎其微。

（三）gTLD发展与管理政策的主权体现

1.gTLD发展与管理政策由ICANN制定

有别于ccTLD的管理模式，gTLD的发展与管理政策主要由ICANN制定，相关从业机构的准入和监管也主要由ICANN负责，但所采用的是法律手段（即合同约束），而非行政手段。各国家和地区的gTLD域名注册管理机构和域名注册服务机构可通过ICANN内部设立的通用域名支持组织（GNSO）等方式，参与起草全球gTLD域名发展和管理政策；其他各方可通过ICANN设置的公众评议渠道或参与ICANN其他组成机构，对gTLD相关政策提供意见和建议。同时，各个国家和地区政府部门可制定本国或地区相关法律法规和规定，并依法对本国或地区的域名、域名系统基础设施和域名服务活动实施行业管理。

（1）gTLD发展政策

gTLD的出现始于域名系统发展早期，首个gTLD名为“.ARPA”，1984年，RFC920提出取消“.ARPA”并设置新的顶级域，[18]“.COM”（公司）等7个gTLD被陆续设立并投入使用。ICANN成立后，为了满足不同利益相关方群体的使用需求，ICANN从2000年起分两批推动设立了“.BIZ”等15个gTLD（与之前的7个统称为“传统gTLD”）。

表8-1 2011年之前设立的传统gTLD

序号	顶级域	域名注册管理机构	所在地	面向用户
1	. COM	VeriSign, Inc.	美国	商业机构
2	. NET	VeriSign, Inc.	美国	网络组织
3	. ORG	Public Interest Registry	美国	非营利组织
4	. INT	IANA . int Domain Registry	美国	国际组织
5	. EDU	Educause	美国	美国教育机构专用
6	. GOV	US General Services Administration	美国	美国政府部门专用
7	. MIL	US DoD Network Information Center	美国	美国军事部门专用
8	. BIZ	Neustar Inc.	美国	商业
9	. INFO	Afilias Ltd.	爱尔兰	网络信息服务组织
10	. NAME	VeriSign Information Services, Inc.	美国	个人姓名
11	. PRO	Registry Services Corporation	美国	会计、律师和医生
12	. MUSEUM	MuseDoma	国际组织	博物馆
13	. AERO	SITA Information Network Computing USA, Inc.	美国	航空业
14	. COOP	DotCooperation LLC	美国	商业合作团体
15	. TRAVEL	Tralliance Corporation	美国	旅游业
16	. ASIA	DotAsia	中国香港	泛亚太地区
17	. JOBS	Employ Media LLC	美国	人力资源服务
18	. MOBI	mTLD Top Level Domain, Ltd.	爱尔兰	移动通信
19	. TEL	Telnic Ltd.	英国	联系方式
20	. CAT	Fundació puntCAT	西班牙	西班牙加泰罗尼亚社群
21	. POST	Universal Postal Union	国际组织	邮政业
22	. XXX	Internet Content Management Registry	美国	成人娱乐产业

为进一步鼓励互联网创新，促进市场竞争，增加用户选择，经过数年的讨论、磋商和博弈，ICANN于2011年正式批准启动新gTLD计划，并于2012年开放首轮新gTLD申请。该计划改变了以往gTLD个别发展的方式，在根区成批地引入更多gTLD，允许申请机构申请运营多语种顶级域、地名（不含国家和地区）顶级域、品牌顶级域以及具有通用属性、行业属性的顶级域等，将提供全球解析的gTLD规模由20余个迅速扩大到超过1200个。目前，ICANN对新gTLD首轮申请的授权工作已接近尾声，下一轮开放申请的前期准备工作正在不断推进，包括开展：新gTLD计划首轮申请对促进竞争、用户信任和用户选择的效果评估；新gTLD计划首轮申请对根系统安全性和稳定性的技术影响评估；商标信息交换中心对新gTLD商标权保护的效果评估；新gTLD政策制定工作组对后续开放程序的研究等。关于下一轮开放的时间，部分ICANN董事会成员及ICANN职员的心理预期是2020年，但目前仍无确切时间表。

（2）gTLD管理政策

ICANN采用授权或认证的方式，对除美国专用的“.GOV”、“.EDU”、“.MIL”外的其余gTLD域名注册管理机构，以及全部gTLD域名注册服务机构开展准入管理，并通过与两方分别签署合同（即RA和RAA）实施从业机构监管。

其中，RA中主要规定了域名注册管理机构需遵守的相关运营和管理要求，包括：依获批事项和范围提供服务、仅使用获ICANN认证的域名注册服务机构提供域名注册、遵守适用法律法规及ICANN现行政策规范、符合域名注册管理机构行为准则和性能规范、确保互操作性与业务连续性、落实数据托管要求、提供域名注册数据公共查询服务（即Whois）、建立权利保护机制、制定保留字列表、保护域名持有者个人数据、向ICANN支付费用、向ICANN报送月度业务报告、配合开展经济研究活动、配合合同合规审计等。

RRA主要规定了域名注册服务机构需遵守的相关运营和管理要求，包括：遵守适用法律法规及ICANN现行政策规范、符合域名注册服务机构行为准则和业务规范、保留并及时向域名注册管理机构提交域名注册及域名持有者数据、落实数据托管要求、提供域名注册数据公共查询服务（即Whois）、设立域名争议解决政策和程序、规范域名注册代理商行为、向ICANN支付费用、完成培训课程、配合合同合规审计等。对于未履行合同约定，出现严重过错的从业机构，采取取消授权或认证的方

式予以退出。

截至2016年上半年，获ICANN授权的域名注册管理机构主要分布在欧洲（40.1%）、北美（29%）和亚太（27.3%）地区，覆盖47个国家和地区；获ICANN认证的域名注册服务机构主要分布在亚太（35.7%）、欧洲（33.5%）和北美（24.9%）地区，覆盖67个国家和地区。[19]自2014年以来，新获认证的域名注册服务机构超过92家；因合同违约被取消资格的域名注册服务机构超过17家，其中也包括我国的一家公司，原因是该公司为大量非法销售医药品的网站提供服务，并且未保存相关域名滥用行为记录、未验证域名注册数据公共查询服务（Whois）信息的真实准确性以及未向ICANN提供域名注册数据。

2.gTLD设置政策

目前的gTLD设置即新gTLD的设置，要求申请机构根据ICANN《新gTLD申请人指南》[20]文件的要求，向ICANN提交申请标书（包含对50个已设定问题的解答）及相关证明材料，充分证明该gTLD字符串具有合规性及相应的发展空间和应用领域，运营机构拥有合法资质、政府部门及利益相关方的支持以及相应的技术、运营、管理和财务能力等。

ICANN会同外部评估机构对各申请机构提交的申请材料进行完整性检查，启动公众评议程序供各方提出意见，同时启动正式异议程序供特定利益群体提出反对意见（包括字符串混淆、侵犯法定权利、违背道德和公共秩序、社群反对四方面），随后开展字符串及申请机构初始评估，以确保相关顶级域的引入不会导致域名系统出现安全性、稳定性问题，相关申请机构能够有效、公平、良好运营该gTLD，并符合相关国家或地区的公共利益或特定利益群体的利益等。

公众意见被提交至初始评估专家组予以考虑；若存在字符串争用（即与其他机构申请的字符串相同或相似）或收到正式异议，则通过域名争议解决途径进行仲裁，败诉者将退出申请；若初始评估未通过，即进入进一步评估程序，若该程序仍未通过也将退出申请。通过初始评估，且未出现字符串争用、未收到正式异议的顶级域申请，将进入管理系统实地测试阶段。测试通过后，申请机构即可与ICANN签署RA，并完成入根程序以实现全球解析。

结合GAC此前提出的建议，《新gTLD申请人指南》针对公共政策问

题设计了相关异议提交和处理机制，以保障各个国家和地区的公共利益。对于存在公共政策敏感性问题的字符串，如违反了相关法律法规，涉及国家主权、种族或族群、宗教信仰、文化、政治观点、地名、特定部门和机构名称等敏感内容，或者易引发网络欺诈与滥用等问题，各个国家和地区政府部门可通过公众评议、正式异议、GAC早期预警（可据此单独提出本国或地区意见，但不具强制力）以及GAC关于新gTLD的建议（即GAC共识建议）程序提出反对意见。若GAC内部一致认为不应通过某一申请，则很可能导致ICANN董事会否决该申请，否则董事会须提供理由。例如，拉美国家在GAC内部共同反对美国企业申请“.AMAZON”、“.PATAGONIA”等新gTLD（都属于品牌与地名重合的情况），最终使上述顶级域退出申请，维护了相关国家的公共利益。其中，“.AMAZON”的申请争议几经波折，最终在美国不持立场的情况下形成GAC共识建议。关于gTLD的运营机构变更和退出问题，则与主权关系不大。

3.涉及国家主权的gTLD政策问题

（1）国家和地区代码二级域开放问题

为了减少新gTLD开放申请所引发的国家主权及其他相关敏感问题，根据ICANN《新gTLD申请人指南》文件，域名注册管理机构应制定保留字列表，对该顶级域下的国家和地区代码字符串予以保留（不对外提供注册）。

在近年来对这一议题的研究和讨论中，ICANN社群内部主要形成了两方力量：产业部门从经济利益角度出发，大多希望并积极推动在gTLD下全面开放注册两字符和三字符ASCII码（也包含ISO 3166-1列出的国家和地区代码，如我国的“CN”和“CHN”）；政府部门（GAC）从公共利益角度出发，却始终未能达成一致意见，其中美国、德国、瑞士、瑞典、澳大利亚等国赞同相关注册政策，欧盟、英国、法国、俄罗斯、印度、我国及部分中东和非洲国家则认为这一政策将导致与相应的国家和地区代码产生混淆，可能引起主权相关敏感性问题，对本国信息安全和国家形象等造成不利影响，因此反对将本国或地区代码作为二级域开放注册。

在两方力量的博弈中，ICANN推动完成了两字符ASCII码在二级域的开放注册政策。经公开征求意见，《避免 字母/字母 两字符ASCII码与

相应的国家和地区代码混淆的建议措施》框架[21]于2016年11月获得ICANN董事会批准，并于12月20日起执行。实施该措施框架的gTLD域名注册管理机构即可提供两字符ASCII码作为二级域注册，而无须告知相关政府部门，更无须征求GAC成员意见并取得相关授权。

措施框架规定：一是对于涉及国家和地区代码的两字符二级域注册，gTLD域名注册管理机构可以专门为相应的政府或ccTLD域名注册管理机构提供为期30日的预注册期，供其进行相应的二级域注册；二是gTLD域名注册管理机构须对两字符注册者提出要求，确保注册者或其业务不会被误解或虚假暗示为与相应的政府或ccTLD域名注册管理机构存在隶属、赞助或担保关系（如无相应关系）；三是对于有政府机构报告表明两字符二级域的注册使用已导致与相应国家或地区代码相混淆，gTLD域名注册管理机构应根据与ICANN签署的协议，对报告所提违规行为予以处理。

在2017年3月召开的ICANN第五十八届会议上，尽管欧盟、巴西、伊朗、新加坡等GAC成员认为上述措施框架仍不能充分保护各国家和地区的公共利益，存在易混淆、注册费高昂、程序不透明等方面的问题，GAC也声称ICANN董事会并未充分考虑GAC此前提出的建议，但ICANN董事会成员回应称，任何政府对gTLD下的二级域不具法律权利。经过长时间磋商，GAC发布此次会议的GAC公报，其中建议董事会考虑一些GAC成员的严重关切，并立即寻找解决措施。

若在GAC层面难以扭转措施框架实施的既成事实，考虑到目前全球已有超过1200个gTLD（含新gTLD）入根并实现全球解析，我国国家代码“CN”均存在作为二级域开放注册的可能性。目前已有至少一家境外机构宣布开放所有两字符二级域相关注册。预计开放三字符ASCII码注册的政策方向也基本确定。

（2）司法管辖权问题

ICANN司法管辖权及其对ICANN有效履行使命（即职责）能力的影响情况，是IANA移交之后备受瞩目的焦点之一。

尽管根据ICANN新版章程，ICANN承诺在其履行使命的过程中，“维护互联网社群的整体权益，在开展活动时遵循国际法、国际公约和适用的本地法律的相关原则”，但章程也规定，“ICANN应继续作为美国加州具有独立法人资格的非营利性公益机构提供IANA服务”，这意味着

ICANN公司治理已经被牢固约束在ICANN总部所在地——美国加州的法律框架下。

目前，这一议题正在ICANN内部设立的加强ICANN问责制跨社群工作组第二阶段（CCWG-Accountability WS2）工作中进行研究。WS2司法管辖权工作组于2016年2月发布了司法管辖权问题调查问卷，邀请互联网社群积极反馈。ICANN第五十八届会议期间，GAC对这一议题进行了讨论，其中美国及其盟友基本反对变更当前ICANN管辖权，绝大多数发展中国家和部分欧洲国家则认为，ICANN目前的司法管辖权安排是不合理的，全球互联网关键资源管理不应受到美国本地的司法管辖，同时表示，ICANN司法管辖权问题关系到ICANN作为一个国际机构的合理性，也是ICANN后续国际化进程当中面临的关键问题。但由于GAC成员意见存在严重分歧，GAC未能形成共识建议，仅呼吁各国家和地区政府及其他利益相关方于截止日期前答复问卷。

ICANN受美国司法管辖这一情况可能引发的问题主要包括：

第一，对ICANN公司治理的影响问题。

尽管美国政府不再直接介入根区管理，但ICANN的运作和关键决策仍然受到美国政府及国内政治因素的影响，使美国在ICANN中较其他国家拥有特殊地位，不符合国际关系准则，也不利于其以客观、中立的立场履行职责，与其国际化改革目标存在冲突。

为此，在IANA移交相关方案起草之时，就有一些国家和地区及政府间组织等提出将ICANN总部所在地搬离美国，转移至瑞士等中立国家，但遭到美国政府及ICANN社群部分人士的极力反对。ICANN在新版章程及IANA职能管理权移交相关方案中均明确了ICANN总部所在地维持不变，特别是将该内容写入了ICANN新版章程的“基本章程”部分，该部分条款只有获得ICANN董事会全体有表决权成员（共16人）3/4以上同意以及赋权社群[22]的批准，才能被调整、修改及废除。但目前，WS2司法管辖权工作组中并无成员提出转移ICANN总部所在地的建议。

第二，对域名从业机构和域名注册者的影响问题。

受到与ICANN的合同关系约束，来自所有国家和地区的域名注册管理机构和域名注册服务机构都需要承诺遵守美国法律、法规和规定，包括美国财政部海外资产控制办公室（OFAC）制定的经济和贸易制裁计

划。因此，在未经OFAC许可的情况下，一方面，受制裁国家的域名注册管理机构和域名注册服务机构申请者将无法取得ICANN授权或认证并提供相关服务，然而，ICANN已声明其并无义务为相关实体申请这一许可；另一方面，美国以外国家的域名注册管理机构和域名注册服务机构也可能会停止向受美国制裁国家提供服务，其中域名注册服务机构可能在不提前告知的情况下取消受制裁国家的域名注册，导致相应互联网接入被阻断、域名持有人权益受损。上述两方面问题都对ICANN履行使命、确保域名系统的全球互操作性和开放性造成了严重阻碍。

此外，因欧盟等地有关个人数据保护的法律法规与ICANN的RAA存在冲突，ICANN多年来依申请批准了丹麦、瑞典、荷兰、奥地利、爱尔兰等国域名注册服务机构的数据保留豁免请求，将域名注册服务机构数据保留的期限从2年缩短为1年。

（3）网络犯罪执法问题

互联网的分布式和去中心化特性，使各国家和地区规范网络使用、调查处理网络犯罪案件和抓捕犯罪嫌疑人的难度大大提升。经过多年的实践，以域名和IP地址为代表的互联网基础资源和关键服务，成为政府部门应对这一挑战、加强互联网监管的重要抓手。

为保障网络安全，维护网络主权、国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，近年来各国家和地区纷纷出台网络安全法规、互联网资源和数据管理规范、行业自律公约等，明确了域名和IP地址的注册、留存、使用等规定，并要求本国或地区域名注册管理机构、域名注册服务机构等域名从业机构落实主体责任，配合政府部门开展相关调查和执法活动。

同时，基于ICANN对全球互联网关键资源的管理职责和对域名注册管理机构和域名注册服务机构的合同约束，ICANN在研究和应对域名系统涉及的网络与信息安全问题、在其政策制定和日常运营中充分考虑公共安全利益等方面，发挥了重要作用。2015年，ICANN 董事会与GAC建立了机构框架，设立公共安全工作组 （PSWG），对域名滥用等安全问题及可能的解决方案持续开展研究和评估，以推动公共安全专业化和公共安全相关政策不断完善。

ICANN也与相关域名注册管理机构和域名注册服务机构共同参与配合了若干网络犯罪调查执法工作。例如2016年12月，欧洲国际刑警组织

（Europol）宣布通过30个国家和地区的联合行动，捣毁了名为“雪崩”（Avalanche）的大规模恶意软件管理平台。该平台托管恶意软件家族高达20余种，囊括了僵尸网络、银行木马和勒索软件，受害者遍布全球180多个国家。联合行动对37个场所进行搜查，逮捕了5名疑犯，关停了39台服务器并查封了83万个域名。[23]

四 结语及展望

（一）IANA移交未改变ICANN继续受美控制，ICANN国际化进程仍需不断推进

IANA移交是全球互联网关键资源管理制度的重大调整，在形式上改变了美国政府单边控制互联网关键资源的运作架构，将促进ICANN履行职能的问责和透明，加速ICANN的国际化进程。但也应认识到，ICANN（及其子公司PTI）仍注册在美国，接受美国司法管辖；来自美国的机构和专家数量在ICANN各组成机构中长期占优，ICANN关键决策仍将受到美国政府和美国国内政治的影响；美国公司VeriSign仍继续负责修改和生成根区文件并分发给所有根服务器，通过协议方式与ICANN共同承担根区管理事务。因此，IANA移交并未改变美国对ICANN的控制现状，也没有削弱美国在国际互联网治理体系和全球互联网关键资源管理中的主导作用。

美国通过形式上退出IANA职能监督者角色，摆脱了各方长期指责其单边控制域名系统根区的困扰，在相当程度上改善了“棱镜门”事件以来的负面形象，占据了支持多利益相关方治理的制高点，并将在全球发展以互联网为基础的数字经济过程中全面推行这一治理模式，避免中俄等国政府强势介入互联网治理。

IANA移交不是一个终点，而是新的起点，其对全球互联网治理格局的深远影响将逐步显现。后移交时代，ICANN除了继续做好全球互联网资源管理及政策制定工作，在维护域名系统安全稳定运行的同时，促进竞争、用户信任和用户选择，还将进一步推动改进ICANN问责制，研究解决司法管辖权、ICANN支持组织和咨询委员会问责、透明度、多样性等方面的问题。ICANN国际化并未画上句号，ICANN离成为一个真正得到全球认可与信任的国际组织还存在很大差距。各方将如何在新的国际环境与制度框架下进行博弈，推动ICANN国际化进程，值得高度关注，更

需要加强实践塑造。

（二）坚决维护网络主权和网络安全，政府需发挥应有作用

习近平总书记强调，“要理直气壮维护我国网络空间主权，明确宣示我们的主张”[24]，“坚持网络主权理念，推动全球互联网治理朝着更加公正合理的方向迈进”[25]。我国近期出台的《网络空间国际合作战略》[26]站在网络空间的视角，对主权、安全及两者的关系进行了全面阐释，是对总书记相关论述的丰富和延伸。

当前的网络安全问题已经不局限于一个国家、一个地区的内部，也不是哪一个国家或地区所能单独应对的，网络安全是各国家和地区面临的挑战，需要各国家和地区通力合作、共同应对。在互联网成为全球通用基础设施的今天，各国家和地区政府部门及政府间多边机制在网络事务上的作用受限甚至被有意弱化显得极不合理，政府部门在发展信息基础设施、保障网络安全、打击网络犯罪、维护公共利益等方面仍具有关键和不可替代的作用。政府的管辖范围具有主权属性，而互联网超越了边界的范围；互联网作为创新和增长的引擎，其持续演变需要将边界之外的、不同层次的政策协调一致；互联网治理需要所有利益相关方的合作参与，国家和地区政府需在这一生态系统中发挥应有作用。

在坚决维护网络主权的同时，还应充分尊重互联网诞生发展至今的基本运行机制，以保持全球互联网标识符的唯一性和统一性为前提，加强全球互联网关键资源管理相关事务的参与及合作，避免过度强调国家控制而导致根区分裂和互联网碎片化加剧，实现网络全球化与网络主权之间的平衡。

（三）深度参与国际互联网治理和全球互联网资源管理，提升影响力和话语权

作为互联网的“中枢神经系统”，以及全球重要的互联网关键资源和基础设施，域名系统既服务于全球互联网的互联互通，也承载着保障互联网安全稳定的重任，更是构建公平正义互联网治理体系的核心组件，并将在“互联网+”时代继续担任基础资源的角色，为各行各业的互联网化提供保障设施。

当前，国际互联网治理体系正处于重要的发展变革期。积极把握历

史机遇，立足当前、着眼未来，深度参与国际互联网治理和全球互联网资源管理规则制定，提升我国在相关领域的影响力和话语权，是维护我国网络主权，推动全球互联网关键资源管理向公平、合理、稳定、有序方向发展，共同构建和平、安全、开放、合作、有序的网络空间，建立多边、民主、透明的全球互联网治理体系的重要举措，已得到中央网信办、工信部、外交部等我国相关政府部门的高度重视。

经过长期的积累，我国政府和我国互联网社群已经在相当程度上具备了深化参与的基础，但仍然面临战略部署、资源投入和中高端人才不足等问题。我国相关政府部门有望基于现实诉求与长远利益、兼顾国际和国内两个大局，做好短、中、长期规划与工作部署；同时，将进一步加强统筹协调，在努力增强政府地位的同时，更多鼓励和发挥企业、智库、技术社群和社团组织等各方面力量的作用，为国际互联网治理和全球关键资源管理贡献中国智慧，推动国际秩序和全球治理体系朝着更加公正合理的方向发展。

（四）以区块链为代表的新技术方案为探索推动根区共治模式提供技术条件

IANA移交后，全球域名系统根区仍维持集中式管理模式，存在由人为因素和技术因素导致的安全风险，如根区数据被篡改或删除、根区数据安全认证机制（即DNSSEC）初始信任公钥（即信任锚）遭泄露、根区数据传输被劫持等。

近年来，以区块链为代表的“去中心化”技术方案快速发展，使探索推动根区管理的多方共同治理模式初步具备了技术可行性，可大大降低上述安全风险。区块链技术也被称为分布式账本技术，是一种以去中心化和去信任的方式，由系统中所有分布式节点共同维护一个可靠数据库（即共同“记账”与“核账”）的技术方案，以确保信息的真实性和不可篡改性。区块链存储数据的结构是由系统中一个个数据块组成一根链条，一段时间内系统中全部的信息交流数据将通过密码学算法计算和记录到一个数据块，并且生成该数据块的指纹用于链接下个数据块并进行信息真实性校验。基于区块链技术，根区不再单独受到IANA和VeriSign两主体的管理和控制，根区数据的完整性将依赖于一个去中心化的存储群组，从而实现根区的共享共治。

此外，通过多方分别持有密钥进行联合签名、赋予根服务器自主管

理权实现平行同步[27]等技术方案，也为根区管理模式向共同治理模式演进提供了技术方向。但何时演进、如何演进，从国际上相关议题的讨论进展来看，目前并无确切预期。同时，根区管理模式演进引发的新问题，例如区块链系统中各分布式节点如何设计、由谁运行，联合签名方案中密钥由谁持有、如何管理，平行同步方案中根服务器能否增设、如何管理、根服务器运行机构的选取是否应改变地理分布严重不均现状等，都有待进一步研究和评估。但推动改进根区管理模式对于促进各国家和地区平等参与全球互联网关键资源管理、维护网络主权带来新的机遇，值得持续关注和期待。

---

[1] ccTLD命名基于ISO 3166-1标准，因此ccTLD所对应的国家和地区，除主权国家外，也包含非国家经济体（如我国港澳台地区分别对应“HK”、“MO”、“TW”）。允许以经济体方式参与资源管理和设立ccTLD的国家，主要涉及ccTLD设立和管理的主权问题，例如ISO 3166-1明确“TW”对应于中国台湾，是中国的一个省。本章讨论的全球资源管理相关的主权问题，除特殊说明外均不涉及我国港澳台地区。

[2] DNSSec是由国际互联网工程任务组（IETF）开发的一系列域名系统安全认证机制，通过软件方式实现对数据来源和数据完整性的验证，对于数据篡改类的攻击提供了很好的防范手段。

[3] 这里指商业群体、社会团体、技术社群、学术界和终端用户等，与其对应的即政府部门。

[4] 不同于联合国框架下的政府间组织，GAC的组织结构相对松散，并且GAC有表决权成员除了主权国家外，还包括许多非国家经济体（如我国台湾、香港地区）。本章讨论的主权问题均不涉及我国港澳台地区。

[5] See John Postel & Joe Bannister：Tera-node Network Technology（TASK 4） Network Infrastructure Activities （NIA） final report（March 15，2000），http：//www.osti.gov/scitech/biblio/802104.

[6] Internet Society，Formation of International Ad Hoc

Committee（IAHC），http：//www.internetsociety.org/history-timeline/formation-international-ad-hoc-committee-iahc.

[7] 美国商务部与ICANN签署的合约主要包括两份：一是1998～2006年签署的谅解备忘录（也称JPA）；二是2000～2016年签署的IANA职能合同。美国商务部与NSI/VeriSign签署的合同为1998～2016年签署的合作协议（Cooperation Agreement）。

[8] 中国外交部：《信息安全国际行为准则》，http：//wcm.fmprc.gov.cn/preview/jks/zcwj/t858317.html。

[9] ICANN与PTI签署的涉及根区管理的合同包括两份：IANA域名职能合同及服务协议。

[10] ICANN与VeriSign签署的合同为根区维护者服务协议（RZMA）。

[11] ICANN章程参见https：//www.icann.org/resources/pages/governance/bylaws-en。

[12] 目前获ICANN授权的5家域名争议解决机构包括：亚洲域名争议解决中心、美国国家仲裁论坛、世界知识产权组织（WIPO）、捷克仲裁法院互联网争议仲裁中心和阿拉伯域名争议解决中心（ACDR）。

[13] 目前获CNNIC授权的域名争议解决的机构共有2家，分别是香港国际仲裁中心和中国国际经济贸易仲裁委员会。

[14] World Summit on the Information Society（WSIS），Tunis Agenda for the Information Society，http：//www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[15] 英国国家顶级域因分配较早除外。

[16] IANA，IANA Report on the Redelegation of the.ly TopLevel Domain，http：//www.iana.org/reports/2005/ly-report-05aug2005.pdf.

[17] See Philip S. Corwin，Court of Appeals Avoids “Doomsday Effect” in Iran ccTLD Decision，http：//www.circleid.com/posts/20160802_court_of_appeals_avoids_doomsd ICANN，U.S.Court Quashes Attempts to Attach ccTLDs：Federal Judge Agrees with ICANN，https：//www.icann.org/news/announcement-2-2014-11-12-en.

[18] 此后，“.ARPA”仅作为互联网内部功能——反向域名解析使用。

[19] See ICANN，gTLD Marketplace Health Index（Beta），December 2016，https：//www.icann.org/en/system/files/files/gtld-marketplace-health-index-beta-21dec16-en.pdf.

[20] See ICANN，Applicant Guidebook，https：//newgtlds.icann.org/en/applicants/agb.

[21] See ICANN，ICANN Implements Standardized Framework for Release of Two-Character Labels，https：//www.icann.org/news/announcement-2016-12-13-en.

[22] 赋权社群是根据IANA移交相关方案，在美国加州法律框架下成立的一个非营利性法律实体。其权力包括：任命和罢免除ICANN董事；撤销整个董事会；拒绝ICANN 预算、IANA预算、运营计划和战略规划；拒绝ICANN章程修订、拒绝PTI治理行动等。赋权社群的组成成员包括来自ICANN通用域名支持组织（GNSO）、国家和地区域名支持组织（ccNSO）、地址支持组织（ASO）、政府咨询委员会（GAC）及用户咨询委员会（ALAC）的人员。

[23] 《“雪崩”崩了 欧洲国际刑警组织捣毁大规模恶意软件管理平台》，极客网，http：//www.fromgeek.com/it/68591.html。

[24] 《习近平：要理直气壮维护我国网络空间主权》，人民网，http：//media.people.com.cn/n1/2016/1010/c40606-28764045.html。

[25]《习近平：在第三届世界互联网大会开幕式上的视频讲话》，新华网，http：//news.xinhuanet.com/politics/2016-11/16/c_1119925133.htm。

[26]《网络空间国际合作战略》（全文），新华网，http：//news.xinhuanet.com/2017-03/01/c_1120552767.htm。

[27] 平行同步方案类似于Handle技术体系。该体系设有四台根服务器（MPA），每台MPA除了各自维护管理自己的下级记录外，同时与其他3台MPA保持数据同步。

第九章

《塔林手册》2.0版的网络主权观[1]

我们有必要为进一步丰富我国上述网络主权观的法理基础、进一步完善中国网络主权观提供更多的法理和规则层面的思想和方案，更好地服务我国参与和引导网络空间全球治理和规则制定进程。

一 《塔林手册》2.0版概况

（一）有关历史背景

20世纪90年代，随着互联网和信息技术的飞速发展和广泛应用，国际法学界开始关注网络战问题。1999年美国海军战争学院首次主办了关于网络战的国际法会议，并出版了《计算机网络攻击与国际法》论文集。[2]2007年以后发生的一系列重大网络攻击事件加速提升了国际社会对网络战的关注度。2007年4～5月间，爱沙尼亚遭受三轮大规模的网络黑客攻击，其总统和议会网站、政府各部门、各政党、三大主要新闻机构、最大两家银行以及通信公司均遭受严重的网络攻击，该事件在国际军事界和法学界引发广泛关注，被军事专家称为人类历史上首次“网络战”。[3]此后，2008年，在格鲁吉亚和俄罗斯的战争期间，格鲁吉亚遭受大规模网络攻击；2010年，伊朗核设施遭受“震网”（Stuxnet）病毒攻击。在政府层面，美、英等国在2010～2011年期间，均将网络战作为重要安全威胁在其国家安全战略、网络安全军事或国际战略中予以明确，美国还在2010年5月组建了网络司令部。[4]

在上述背景下，2008年5月，北约14国在爱沙尼亚首都塔林正式建立“网络防御合作卓越中心”（英文全称“The NATO Cooperative Cyber Defence Centre of Excellence”，以下简称“中心”），目的在于为增强北约成员国网络防御能力建设、教育培训、信息共享和科学研究提供智力和专业支持，它并非北约官方军事架构的组成部分。[5]2009年开始，该中心启动“塔林手册进程”，旨在澄清复杂的网络军事行动的有关国际法问题，特别是现行诉诸武力法和武装冲突法如何适用的问题。[6]中心希望该手册能够像国际人道法学会1994年编纂的《适用于海上武装冲突的国际法圣雷默手册》、美国哈佛大学“人道主义政策与冲突研究”2009年编纂的《空战和导弹战国际人道法手册》一样，对新的战争形式的国际法适用提出指导性建议。该项目由美国海军战争学院教授迈克尔·施密特（Michael Schmitt）担任项目主任，由20名西方国家专家组成编纂《关于网络战国际法适用的塔林手册》（《塔林手册》1.0版）国际专家组。编纂工作历时4年，手册于2013年3月由剑桥大学出版社出版面世。[7]该手册内容分为国际网络安全法（international cyber security law）和网络武装冲突法（the law of cyber armed conflict）两部分，总计7章、95条规则及相应评注，约300页。具体涉及主权、管辖、国家责任、使用武力、敌对行动、占领、中立等内容。[8]

（二）塔林手册从1.0版到2.0版的“升级”

《塔林手册》1.0版在2013年出版后，在国际上引发热议。为了进一步扩大影响，将更加广泛的低烈度国家网络行动纳入研究范围，以实现对网络空间国际法的全覆盖，中心马上开始着手编纂包括和平时期国际法适用在内的《塔林手册》2.0版。[9]同时，为增强其代表性和权威性，《塔林手册》2.0版在总体维持原班人马（包括项目主任不变）的前提下，邀请了包括我国、白俄罗斯和泰国的3名非西方国家的专家加入其19人国际专家组；中心还与荷兰外交部共同举办了三次、每次为期两天的“《塔林手册》2.0版国际咨询会议”（即所谓“海牙进程”），邀请50多国政府法律顾问参加，就手册的草案发表非正式的意见，供国际专家组起草参考，但专家组无反映或接受上述意见的义务。[10]值得注意的是，《塔林手册》1.0版与《塔林手册》2.0版起草过程的最大不同还在于：前者草案（含规则及其评论）的起草由19个专家组成员参与和负责，而后者草案则由项目负责方另行邀请各主题的国际知名专家起草，草案经由编辑委员会审核和同行审议程序后，再交19

个成员组成的国际专家组在有限的时间内审议通过（3次会议，每次一周）[11]。

《塔林手册》2.0版编纂历时近4年，于2017年2月正式出版，内容分为一般国际法与网络空间（General international law and cyberspace）、国际法特别制度与网络空间（Specialised regimes of international law and cyberspace）、国际和平与安全和网络活动（Internationational peace and security and cyber activities）以及网络武装冲突法（The law of cyber armed conflict）四大部分，总计20章、154条规则及相应评注，近600页。具体包括主权、审慎义务（due diligence）、管辖、国际责任法、本质上不受国际法规制的网络行动（cyber operations not per se regulated by international law）、国际人权法、外交和领事法、海洋法、航空法、外空法、国际电信法、诉诸武力法、集体安全制度、和平解决国际争端、不干涉原则和武装冲突法。

总体上看，相较1.0版，2.0版有以下明显的变化：一是在篇幅和内容上有较大增长，这表现在手册总体篇幅增加了一倍，规则的数目以及具体阐述有较大增加。二是在结构和总体体例编排上更加科学合理，特别是对一般国际法、各领域国际法特别制度以及国际和平与安全体制与网络空间的关系进行了较深入阐述。三是从手册的撰写过程看，尽管2.0版的国际专家组的“代表性”有所“改善”，表面形式上还增加了征求各国政府法律顾问环节，但从前述可见，手册编撰的主要和核心工作仍由西方学者一手主导，主要为反映西方的观点和主张服务。

《塔林手册》2.0版出台后，中心即已与荷兰政府、美国大西洋理事会、澳大利亚战略政策研究所等在华盛顿、海牙、塔林和堪培拉合办该手册的系列宣介活动。[12]中心及一些西方国家高官称该手册为当前最为综合系统地分析现行国际法适用网络空间的论述，将为各国和国际社会讨论国际法适用网络空间提供指南。[13]荷兰外长称在手册出版后拟继续召集手册的国际咨询会议，推动各国关于网络空间国际法规则的对话。[14]预计西方国家政府和学界未来将继续加大对手册的推广力度，意图形成“影子立法”之效果。

（三）对《塔林手册》2.0版的总体评价

中心以及手册的项目主任迈克尔·施密特对外强调，手册不属于官

方文件，不代表北约、中心或其成员国的意见，仅反映了国际专家组成员以个人名义对现行国际法适用网络空间的看法和主张，在政策和政治上中立（policy and politics-neutral）。[15]另一方面，结合当前主要各方，特别是西方发达国家和新兴国家围绕网络空间规则国际博弈大背景，以及西方国家和学者在该手册编纂工作的组织、内容取材和手册推广等方面的作为，我们不难看出手册具有鲜明的政治和政策倾向性。初步看，手册有以下几个特点：

1. 西方学者主导和政府背景浓厚

如上所述，专家组19名成员中16名为西方国家学者，2.0版草案及其评论的起草由项目负责方另行邀请专家撰写供专家组讨论，西方学者主导色彩浓厚。美国、荷兰、爱沙尼亚、澳大利亚等西方国家通过政府或智库层面支持和推广该手册，爱沙尼亚总统和荷兰外长还为该手册作序，强调手册对各国厘清和制定网络空间国际法规则的重要意义，荷兰政府并为该手册发起和推进所谓“海牙进程”，这也充分体现出其政府背景。手册除援引有关国际条约、案例外，还援引了美国、英国、德国、加拿大四国国防部编撰的《战争法手册》以及西方学者撰写的国际法著述，发展中国家的相关材料和论述鲜有提及。[16]

2. 手册不乏机械套用或者“越权”解释适用现有国际法的现象

例如，手册中的国家责任法、武装冲突法等章节是简单将现有国际规则机械套用至网络空间，有关内容缺乏国家实践的支撑。事实上，长期以来，中国、俄罗斯及其他发展中国家主张和平利用网络空间，反对网络空间军事化及机械套用武装冲突法和国家责任法。又如，虽然手册号称仅如实反映现有国际法、不创造新的规则，但在界定网络行动侵犯国家主权的标准问题上，手册一方面避而不谈为包括中国、俄罗斯、巴西及欧盟等所关切的大规模数据收集和网络监控活动对国家主权的危害，另一方面创设了所谓的“对目标国领土完整造成的损害程度”和“是否干扰或篡夺了政府的固有职能”两大标准。[17]此外，在有关人权保护义务的域外适用（extraterritoriality）[18]以及使领馆网络基础设施不受侵犯[19]等问题上，手册有关内容超越现行国际法，极富争议性。如此等等，表明手册并未平衡反映各方意见和关切，似难以成为国际共识。

总之，手册是西方通过学者“释法”的方式影响和引导网络空间国

际规则的一次尝试，但手册的政府背景以及对现有法的机械、片面或歪曲的解释和适用，值得我们关注和警惕。同时，手册对于云计算、大数据、物联网和人工智能等网络新技术对国际法解释和适用带来的挑战鲜有深入研究；对于是否有必要根据网络空间的特殊性制定新的国际法这一重要问题亦未有论述。

二 《塔林手册》2.0版网络主权观的内容简析

与手册1.0版相比，2.0版在网络主权问题上有较大的变化。在1.0版中，主权作为第一章第一节五条规则中的一条，仅涉及一国对其主权领土范围内的网络设施和活动行使控制权的问题；在2.0版中，主权单独成章（第一章），并且包括5条规则，涉及一般原则、对外主权、对内主权、对主权的侵犯和主权豁免等内容，在规则数目和具体内容上均有大幅扩张。2.0版网络主权观的主要内容如下：

（一）总体上确认国家主权原则适用于网络空间的所有层面

手册将网络空间分为物理层、逻辑层和社会层：物理层包括物理网络成分（即硬件和其他基础设施，如电缆、路由器、服务器和计算机）；逻辑层由网络设备之间存在的“链接”构成，包括保障数据在物理层进行交换的应用、数据和协议；社会层包括参与网络活动的个人和团体。手册认为主权原则涵盖和适用网络空间的上述三个层面，对这三个层面所涉及的物体、人员和活动行使主权管控。[20]

手册认为，与公海、国际空域或外层空间等全球公域在法律性质上不同，网络空间本身具有领土特征，一国可对发生在本国领土内涉及有形物体或由境内个人或实体实施的网络活动行使主权权利；即使有关网络活动虽可能横跨多国边界，或发生在国际水域、国际空域或者外层空间，但实施这些行为的个人或实体均受一国或多国管辖。[21]

手册认为，由于构成网络空间不可分割的组成部分的网络设施分布于各国的主权领土上，因此，一国不能对网络空间本身主张主权。同时，一国将境内的网络设施连接到网络空间这一事实，不能解释为该国放弃其主权。根据主权原则，一国有权在不违反国际法义务的情况下，将其领土上全部或部分网络设施与互联网断开连接。[22]

综上，手册摒弃了在西方曾流行一时的网络空间的全球公域论，强调了网络空间的属人、属地和社会属性，确认国家主权对于网络空间所有层面和领域的适用。对于网络空间作为人类共享的空间，手册一方面认为，由于各国的网络设施均是这个共享空间不可或缺的组成部分，各国不能直接对这个共享空间本身行使主权，这对主权国家平等参与国际互联网治理和构建“网络空间命运共同体”具有法理借鉴意义；另一方面，手册也认为，一国接入互联网不意味着放弃网络主权，其在不违反国际义务的前提下拥有“断网权”，这对确认和完善各国管控境内互联网的基本主权具有重要意义。

（二）从对内和对外主权两方面构建了网络主权内涵

1. 关于对内主权

承认一国拥有在不违反国际法义务的情况下，可对境内的网络设施、从事网络活动的人员以及网络活动本身采取任何其认为必要或合适的措施的主权权威，包括对境内网络设施和活动的监管权、保护权、立法和执法权等；网络设施的权属和用途、网络活动参与者的身份和国籍不影响一国对内的网络主权权威。一国可对境内人员的网络活动进行监管，同时，对在线通信和活动的审查与限制，不得违反可适用的国际人权法。一国可对特定的网上内容的连接进行限制和审查，包括阻断境内与社交媒体或其他网站上的恐怖主义内容的连接；但一切对言论表达自由的限制，必须具有非歧视性，并且须有法律明确的授权。一国拥有自主决定其涉及网络空间的政治、社会、文化、经济和法律秩序的权力。同时，各国负有对源于其境内并对他国造成危害的网络活动进行制止的“审慎义务”。[23]

2. 关于对外主权

强调对外主权源自主权平等原则，每个国家均有义务尊重他国的国际法人格、领土完整和政治独立，并忠实履行其国际义务。在不违反国际法的前提下，一国可自由从事境外网络活动。各国有权自由决定是否加入特定的网络条约体系，亦可就特定网络领域国家实践的习惯法性质发布“法律确信”。一国基于对外主权实施网络行动不得违反禁止侵犯他国主权、不干涉原则以及禁止使用武力原则等具有约束力的条约或习惯国际法规范。[24]

综上，手册认可一国在不违反国际义务的前提下，拥有对内最高网络主权权威，自主决定本国网络空间法律秩序；对外可自由从事网络活动、加入网络条约体系或发布“法律确信”。总体而言，这部分内容，尤其是对外主权篇幅较少（两者共4页），对具体内涵论述的广度和深度相对单薄。

（三）对侵犯网络主权的法律标准作了较深入探讨

（1）明确只有国家能构成对他国主权的侵犯，非国家行为体行为不能构成侵犯主权，除非这些行为可归责于国家。同时，这不妨碍受攻击国依国际法对非国家行为体网络行动予以回应，包括在合适的情形下基于“紧急措施”规则或者自卫权予以回应。此外，如一国对非国家行为体在其境内的网络攻击行为未尽到“审慎义务”，受攻击国亦可就上述非国家行为体的行为对该国采取反措施。[25]

（2）明确一国在未经他国同意或缺乏国际法上的正当事由（如安理会授权）的情形下，从物理上进入他国领土或领空，构成侵犯主权。专家组对以物理存在的方式在他国境内实施网络间谍行为是否侵犯主权存在不同观点。但均认为仅从目标国境外拦截无线信号不构成侵犯主权，因该网络行动没有涉及目标国境内的网络基础设施。[26]

（3）对于远程网络行动（即无须物理上进入他国境内的网络行动），手册制定了两类不同的法律标准来评估其合法性：①网络行动对目标国领土完整造成的损害程度；②是否干扰或篡夺了政府的固有职能。前一标准是基于一国对其主权领土的入境管控权原则，后一标准则是基于一国在其领土上行使“排他性国家职能”的主权权利。[27]

对前一标准又通过三个不同层次进行分析：一是网络行动造成物理损害或伤亡，则构成侵犯主权；二是使他国境内网络基础设施丧失功能，引起类似上述的物理损害或伤亡的后果，也构成侵犯主权；三是对于既未造成物理损害，也未造成功能丧失的网络行动是否以及何时构成侵犯主权，专家组未有共识。[28]

关于是否干扰或篡夺了政府的固有职能标准。手册认为，对政府履行固有职能所必需的数据或服务造成干扰的网络行动，构成侵犯主权而被禁止。手册并列举了可能出现的实例，包括篡改或删除涉及提供社会服务、选举行为、征税、有效执行外交行为或者履行重要国防活动的数

据。多数专家还认为，无论（干扰或篡夺政府固有职能的）网络行动在何处实施或发生，均构成对受害国主权的侵犯。手册并分析了篡夺政府固有职能与干涉内政行为的区别，强调前者涉及政府固有职能，而后者涉及的是内政，两者并不相同；前者要求有“胁迫”（coercion）这一构成要件，后者无此要求。[29]

（4）相关网络行动构成侵犯主权须产生必要的后果，主观意图并非构成要件。因此，如一国旨在侵犯他国主权的网络行动最终失败，则该网络行动的目标国的主权未受到侵犯。如一国的网络行动，虽并无侵犯他国主权的意图，但客观上产生此种后果的，构成侵犯主权。但是，一国经他国同意在该国实施的网络行动，不构成对主权的侵犯。[30]

这部分的最大亮点是制定了侵犯主权的两大类法律标准以及相关的子标准，这事实上已经超出了手册对自身的授权，即仅仅反映现有国际习惯法的适用，不创设或制定新的网络空间国际规则。此外，该部分对网络间谍，特别是网络强国利用自身在网络设施和技术上的优势对他国进行网络监控和窃密行为的合法性设置了较低的门槛。对一国承担管控境内非国家行为体、防止对他国进行不法网络活动则规定了较高的标准，强调在攻击来源地国未履行上述“审慎义务”时，受攻击国可对攻击来源地国采取反措施。

（四）主权豁免

手册对于主权豁免作了规定，强调“一国针对位于享有主权豁免平台上的网络基础设施的干涉行为，不论该平台位于何处，均构成对主权的侵犯”。同时，享有主权豁免的平台和构造须遵守相应的国际法规范和原则，如其违反尊重他国主权等原则，其依然保有主权豁免，但这一豁免无法阻止他国为维护其法律公认的利益采取合法、恰当且必要的措施，包括在特定情形下使用武力。[31]

关于主权豁免平台，手册认为，国际法对用于非商业性质之政府用途的特定物体赋予主权豁免，例如军舰、国有航空器等，不论该物体位于何处。但在这些平台上的网络基础设施必须完全用于政府用途，才能享有主权豁免和不得侵犯权。手册认为，对享有主权豁免的对象的任意干涉行为均违反国际法。这些干涉行为包括但不限于破坏享有主权豁免物体或严重损坏其运行的活动。但在国际性武装冲突期间，主权豁免原则和不受侵犯在冲突各方之间停止适用，有关物体如符合军事目标标

准，则可被摧毁或成为敌方军队的战利品。[32]

对不属于上述范围的场所和物体，仍可依据诸如军队地位协定等双边或多边协定进行特殊的保护，如依外交和领事法，对特定网络基础设施以及电子档案、文件和通信予以特别保护。[33]

该部分内容总体较原则，未对位于主权平台上的网络设施所享有的司法管辖和执行两类豁免进行系统深入论述。此外，手册认为，只有有关网络基础设施完全用于非商业政府用途，且其位于用于非商业性质之政府用途的特定物体（主权豁免平台）上时，才享有主权豁免。这对网络设施的主权豁免设置了很高的门槛，与中国等国家在国家主权豁免领域的实践不符。

三 对《塔林手册》2.0版网络主权观的初步评价

《塔林手册》2.0版的网络主权观是西方学界主导下、具有浓厚西方政府色彩的比较成系统的“国际法学术作品”，其影响国际立法的意图亦十分明显。结合上述《塔林手册》2.0版网络主权观的内容以及现有的国际社会关于网络主权讨论和研究的成果，对其初步评价如下。

（一）总体较《塔林手册》1.0版以及现有的国际文件成果有所发展，对网络主权的阐述更系统、全面和具体

《塔林手册》1.0版关于主权的专门论述仅有一条，即“一国可对其主权领土内的网络设施和行为行使主权管控”。该条规定主要侧重于一国对有形物体或活动的主权。现有的关于网络主权的国际共识主要体现在2003年和2005年的信息社会世界峰会的成果文件——联合国信息安全政府专家组（GGE）2013年和2015年的报告，主要包括确认：一国对境内的网络设施的管辖权；[34]制定管理互联网的法律和公共政策的权威；[35]参与网络治理的主权权利和责任；[36]主权平等、不得通过网络干涉他国内政的义务等。[37]这些共识散见于上述各个国际文件相关的部分（如2003年信息社会世界峰会《日内瓦原则宣言》关于网络主权的论述纳入到重要原则下的“环境建设”部分；2013年GGE报告有关网络主权的论述放在“关于国家负责任行为规范、规则和原则”部分；2015年GGE报告有关网络主权的论述见于“国际法如何适用于信通技术的使用”部分），没有专门和成系统的关于网络主权的国际法阐述。

如前面所介绍，《塔林手册》2.0版设置专章、5条具体规则以及相关的评注对网络主权进行了较为系统的法理论述，确认了网络主权适用于网络空间的物理层、逻辑层和社会层所有层面和领域，从对内主权和对外主权两个方面入手较系统地阐述了网络主权的内涵，并重点就侵犯主权的法律标准进行了较为深入的探讨，就此提出了具体的规则设计。此外，还就主权豁免问题进行了初步论述。因此，无论从形式还是内容上看，《塔林手册》2.0版网络主权观是当前国际法界在网络主权问题上较成理论体系的作品，值得我们关注和研究。

（二）由于《塔林手册》2.0版的“封闭性”和倾向性，其网络主权观在框架结构、具体内容上存在不足

如前所述，虽然形式上《塔林手册》2.0版增加了3名非西方国家代表，并召开了所谓的“国际咨询会议”，但其草案的起草、修订和定稿均由西方学者一手操办，缺乏代表性、开放性。[38]这相应地体现在其最终成品在结构和内容上的不足。

在结构上，手册对网络主权一般原则、对内主权和对外主权的阐述总体仍相对薄弱（共6页），特别是在对外主权方面存在明显不足（仅1页）；在侵犯主权问题上，尽管内容较为丰富（10页的论述），但如前所述，其创设的有关法律标准，缺乏现有国际法理论和实践的支撑，在手册的专家组内部亦不乏分歧（如网络间谍是否侵犯主权；对于既未造成物理损害，也未造成功能丧失的网络行动是否以及何时构成侵犯主权；政府固有职能的内涵和外延等）。

在具体内容上，手册对网络主权一般原则和理论的探讨多照搬现有法原则，缺乏对网络空间的特殊性的深入阐述，且对互联网内容管理、国际治理等重要问题未有涉及或仅一笔带过；在确认对内主权权威的同时，突出强调人权法和“审慎义务”等对国家行使主权的限制；[39]对外主权方面则强调从事境外网络活动的自由，对于平等参与网络国际治理和公平分配互联网国际资源、不得对他国进行大规模网络监控等发展中国家关注的问题未予涉及；[40]在讨论侵犯主权的问题时，多用假设的理论和案例支撑，缺乏现有理论和实践的支持。[41]此外，手册对于网络新技术的发展带来的挑战未予以足够关注和回应，对数据主权等新问题未提出解决之道；[42]由于手册宣称仅针对现有法的适用问题，手册对于是否需要就因应互联网发展带来的新问题制定网络主权新的规则

也未予论述。

（三）《塔林手册》2.0版网络主权观的可接受性、适应性和可操作性有待观察

从前述可见，该手册代表性、开放性不足，无法全面、客观和平衡反映国际社会各方关切以及相关国际法领域的理论和实践，对网络空间新发展及其特殊性缺乏深入研究和探讨，其所设定的有关规则能否为国际社会特别是广大发展中国家所接受，真正影响或转化为国际规则，并从理论层面转化为国际实践，仍然是个问号。

四 结语

近年来，我国数字经济快速发展，取得举世瞩目的成就；网络安全立法政策不断完善，中国特色网络主权观正在逐步形成。习近平总书记关于网络安全和网络治理的系列重要讲话以及我国近期颁布的《网络安全法》、《国家网络空间安全战略》、《网络空间国际合作战略》等重要文件为中国网络主权观勾勒了一个初步框架。

习近平总书记在多次对外讲话中提出要尊重网络主权，并提出“网络空间是人类共同的活动空间，网络空间前途命运应由世界各国共同掌握。各国应该加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体”。[43]《网络安全法》明确要保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展。[44]两个战略文件提出：网络空间主权不容侵犯；相互尊重自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利，不搞网络霸权，不干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动，不得利用自身优势损害别国信息通信技术产品和服务供应链安全；各国自主管理主权范围内的网络事务和制定有关网络空间的法律法规，管理本国信息系统及本国疆域上的网络活动；保护本国信息系统和信息资源免受侵入、干扰、攻击和破坏；保障公民在网络空间的合法权益；防范、阻止和惩治危害国家安全和利益的有害信息在本国网络传播，维护网络空间秩序；维护网络空间和平安全，在国家主权基础上构建公正合理的网络空间国际秩序。[45]

上述网络主权观符合我国实际需要，也契合国际社会特别是广大发展中国家对维护网络空间国家主权的关切和需求，在内容上较《塔林手册》2.0版更加全面、平衡，因而赢得了世界大多数国家认同，有力地提升了我国在网络空间的国际话语权。我们应以上述重要讲话和文件为指导，深入开展网络空间国际法特别是网络主权法律问题的研究，包括对《塔林手册》2.0版网络主权观的研究；同时，也有必要为进一步丰富我国上述网络主权观的法理基础、进一步完善中国网络主权观提供更多的法理和规则层面的思想和方案，更好地服务我国参与和引导网络空间全球治理和规则制定进程。

---

[1] 本章为作者在2016年12月武汉大学举行的“网络主权研讨会”上的发言的基础上整理而成。本章内容仅代表作者个人观点，不代表中国政府立场。

[2] Michael Schmitt & Brian O’Donnell （eds.），Computer Network Attack and International Law，Naval War College，2002.

[3] See Kertu Luus，Cyber War I：Estonia Attacked from Russia，http：//www.europeaninstitute.org/index.php/component/content/article id=67：cyber-war-i-estonia-attacked-from-russia；东鸟：《第一场国家间网络战：爱沙尼亚大战》，http：//book.people.com.cn/GB/69399/107423/207171/13142086.html（摘自东鸟《中国输不起的网络战争》，湖南人民出版社，2010）。

[4] US Department of Defense，Cyber Command Fact Sheet，21 May 2010，http：//www.stratcom.mil/factsheets/Cyber_Command/. 美国政府于2010年5月发布的《国家安全战略》将网络威胁列为“国家面临的最严重的国家安全、公共安全和经济挑战之一”。See The White House，National Security Strategy，http：//nssarchive.us/NSSR/2010.pdf. 2010年，美国国防部《网络空间行动战略》将网络空间列为军事行动领域。See US Department of Defense，Strategy for Operating in Cyberspace，http：//csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. 英国政府在其2010年《国家安全战略》中认为，网络攻击是对英国国家安全的四个最严重的威胁之一。See The

Government of UK，A Strong Britain in an Age of Uncertainty：the National Security Strategy，https：//www.gov.uk/government/news/national-security-strategy，p.11.

[5] See CCDCOE，https：//ccdcoe.org/about-us.html. 目前，该中心有美国、英国、德国、荷兰、比利时、希腊、土耳其等17个北约成员国作为发起国（sponsoring nations），奥地利和芬兰两国为资助参与方（contributing participants）。

[6] See CCDCOE，Tallinn Manual Process，https：//ccdcoe.org/tallinn-manual.html.

[7] Michael Schmitt （ed.），Tallinn Manual on the International Law Applicable to Cyber Warfare，Cambridge University Press，2013.另参见北约卓越网络合作防卫中心国际专家小组编、朱莉欣等译《塔林网络战国际法手册》，国防工业出版社，2016，前言，第11～13页。

[8] Michael Schmitt （ed.），Tallinn Manual on the International Law Applicable to Cyber Warfare，Cambridge University Press，2013.

[9] See CCDCOE，Tallinn Manual Process，https：//ccdcoe.org/tallinn-manual.html.

[10] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，p.6.

[11] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 5-6.

[12] See NATO CCDCOE，Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched，https：//ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html.

[13] See NATO CCDCOE，International Law Applies to Cyber Operations，Tallinn Manual 2.0 Reaffirms，https：//ccdcoe.org/international-law-applies-cyber-operations-tallinn-manual-20-reaffirms-0.html；NATO CCDCOE，Tallinn Manual 2.0 Paves the Way for State Action in Cyber Space，https：//ccdcoe.org/tallinn-manual-20-paves-way-state-action-cyber-space.html；Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，p. xxiiii （forword by Toomas Hendrik Ilves，President of the Republic of Estonia） and p.xxvii （forword by Bert Koenders，Minister of Foreign Affairs of the Kingdom of the Netherlands）.

[14] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，p.xxvi （forword by Bert Koenders，Minister of Foreign Affairs of the Kingdom of the Netherlands）.

[15] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 2-3.

[16] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. xxxiv-xxxvii.手册援引的学者著述主要有：Lassa Oppenheim，Oppenheim’s International Law（Robert Jennings & Arthur Watts eds.，9th edn，1992）；Malcolm Show，International law（7th edn，2014）；James Crawford，State Responsibility：the General Part（2013）；Eileen Denza，Diplomatic Law：Commentary on the Vienna Convention on Diplomatic Relations（4th edn，2016）；Yoram Dinstein，The Conduct of Hostilities under the Law of International Armed Confilict（3rd edn，2016）；Yoram Dinstein，War，Aggression and Self-Defence（5th edn，2011）等西方作品。

[17] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International

Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，p. 20.

[18] 关于人权保护义务的域外适用问题，见手册第185、186和198页有关观点。这些观点认为，当个人因为某国家行为而不能享受一项人权权利或保护时，则对该项人权权利或保护的适用具有域外性；当国际人权条约未明确规定域外适用问题时，除非有相反规定，否则应予以域外适用；如某项国际人权的行使发生在一国境内或在该国的有效控制之下，则无论权利人是否位于该国境内，该国均有责任保护权利人对该项人权的行使。

[19] 关于使领馆网络基础设施不受侵犯，手册第214页认为，接受国在紧急情况下可基于自卫对使馆或领馆馆舍，或馆舍内的网络基础设施采取行动。

[20] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp.12，14.

[21] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，p. 12.

[22] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 12-13.

[23] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 13-16.

[24] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 16-17.

[25] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 17-18.

[26] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 19-20.

[27] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 19-20.

[28] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 19-20.

[29] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 22-24.

[30] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 24-27.

[31] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 27-29.

[32] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 27-29.

[33] Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 27-29.

[34] 2013年GGE报告第20段指出：“国家主权和源自主权的国际规范和原则适用于国家进行的信通技术活动，以及国家在其领土内对信通技术基础设施的管辖权”；2015年GGE报告第27段重申该原则，并在第28段进一步指出“各国对其领土内的信通技术基础设施拥有管辖权”。

[35] 2003年信息社会世界峰会成果文件《日内瓦原则宣言》第49段指出：a.与互联网有关的公共政策问题的决策权是各国主权。对于与互联网有关的国际公共政策问题，各国拥有权利并负有责任；……d.政府间组织已经并应继续在互联网有关的公共政策问题的协调中发挥推动作用。2005年信息社会世界峰会第二阶段会议成果文件《突尼斯议程》重申了上述共识。

[36] 2003年信息社会世界峰会成果文件《日内瓦原则宣言》第49段指出：a.与互联网有关的公共政策问题的决策权是各国主权。对于与互联网有关的国际公共政策问题，各国拥有权利并负有责任；……d.政府间组织已经并应继续在互联网有关的公共政策问题的协调中发挥推动作用。2005年信息社会世界峰会第二阶段会议成果文件《突尼斯议程》重申了上述共识。

[37] GGE2015年报告第26段及第28段提及主权平等、不干涉他国内政原则。

[38] 除本章第一部分介绍的有关内容外，具体可参见Michael Schmitt（ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 5-6.

[39] 该规则评注提及的对内网络主权的相关限制性表述包括：“除非为有约束力的国际法规则——如国际人权法（规则35）——所禁止”，“对于在线通信和活动进行的国家审查与限制，不得违反可适用的国际人权法”，“一国限制接入网络的权利必须考虑可适用的国际法准则”，“言论自由表达是习惯国际人权法上的一项权利，因此，对该权利的限制，必须具有非歧视性，并且具有法律授权”，“一国的国内立法，如关于公民自由的国内法可能会对上述主权权利的行使施以进一步的限制”，“主权不仅赋予一国权利，也施加相应法律义务，例如要

求一国负有对源于其境内并对他国造成危害的网络活动进行制止的‘审慎义务’”。See Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 13-16.

[40] 该规则评注提出主权平等以及在遵守国际法的前提下，一国可在其领土之外自由从事境外的相关网络活动，加入网络条约体系或发布“法律确信”。但未涉及其他发展中国家关注的互联网国际治理等问题，也未对尊重他国网络主权、不干涉内政等进行论述。

[41] 如前所述，手册提出的关于侵犯主权的两大标准，即对目标国领土完整造成的损害程度和是否干扰或篡夺了政府的固有职能，具有创造性，其所举的例子均为假设性的例子，缺乏现有国际法理论和实践的支撑。See Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 17-27.

[42] 关于数据主权，手册略有论及，但对于一国对在境外存储或传输的数据的主权是否可独立于其对境内网络设施及人员和活动的主权，手册未给出明确答案，仅表示多数专家组成员认为各国对位于境外的数据并不享有上述主权。See Michael Schmitt （ed.），Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（2nd edition），Cambridge University Press，2017，pp. 15-16.

[43] 《习近平在第二届世界互联网大会开幕式上的讲话》（2015年12月16日，乌镇），新华网，http：//news.xinhuanet.com/world/2015-12/16/c_1117481089.htm。

[44] 《中华人民共和国网络安全法》（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过），中国人大网，http：//www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm。该法第1条规定：“为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。”

[45]《国家网络空间安全战略》（全文），新华网，http：//news.xinhuanet.com/politics/2016-12/27/c_1120196479.htm，第三部分原则的第（一）条“尊重维护网络空间主权”；《〈网络空间国际合作战略〉全文》，新华网，http：//news.xinhuanet.com/2017-03/01/c_1120552767.htm，第二章（基本原则）和第三章（战略目标）相关内容。

附录 重要国际性文件中的网络主权[1]

目录

12.2016年G7关于网络空间原则和行动的声明

13.2016年金砖国家领导人《果阿宣言》

14.2017年“塔林手册2.0版”

15.2012年以来联合国大会和人权理事会有关网络人权的重要决议

小结

1. 2003年联合国信息社会世界峰会通过的《日内瓦原则宣言》[2]

在国家主权层面——“互联网公共政策的决策权是各国的主权”。

在人权与基本自由层面——“重申《世界人权宣言》第19条，即每个人都有自由发表意见和自由言论的权利”，“重申《世界人权宣言》第29条，即每个人对社会均负有义务……在任何情况下行使这些权利和自由时均不可违背联合国的宗旨和原则”，“应特别关注社会边缘群体和弱势群体的特殊需要”。

在多利益攸关方层面——“建设包容性信息社会需要各国政府和其他利益相关方，即私营部门、民间团体和国际组织，形成新型的团结精神、伙伴关系和合作关系……呼吁在国内和国际层面上实现数字团结”。

2. 2005年信息社会世界峰会（WSIS）突尼斯阶段会议在2005年11月18日举行的第八次全体会议上通过了上述文件（WSIS-05/TUNIS/DOC/7号文件[3]）——即《突尼斯议程》[4]：

在国家主权层面——《突尼斯议程》第八条指出，“在重申日内瓦《行动计划》第3段所述各利益相关方的重要作用和责任的同时，我们承认各国政府在峰会进程中的关键作用和责任”。

在人权与基本自由层面——“完全尊重和维护《世界人权宣言》，让世界各国人民均能创造、获取、使用和分享信息和知识”，“重申《维也纳宣言》所揭示的包括发展权在内的所有人权和基本自由权的普遍性、不可分割性、相互依存性和相互关联性，重申民主、可持续发展、尊重人权和基本自由权以及良好治理在各个层面都是相互依存，相辅相成的，进一步决定在国家和国际事务中更加尊重法治”。

在多利益攸关方层面——“提醒各国政府、私营部门、民间团体和联合国以及其他国际组织应展开合作……在各个层面营造有利环境……鼓励国际和区域性合作”。

3. 中俄等国2011年提出并于2015年重新修订的《信息安全国际行为准则》[5]

在国家主权层面——在大会决议部分，重申“与互联网有关的公共政策问题的决策权是各国的主权。对于与互联网有关的国际公共政策问题，各国拥有权利并负有责任”。而在准则内容部分，“遵守《联合国宪章》和公认的国际关系基本原则和准则，包括尊重各国主权、领土完整和政治独立”，重申“各国有责任和权利依法保护本国信息空间及关键信息基础设施免受威胁、干扰和攻击破坏”。

在人权与基本自由层面——在行为准则部分，强调“尊重人和基本自由”，“认识到人们在线时也必须享有离线时享有的相同权利和义务……同时铭记根据《政治与公民权利国际公约》第19条，这些权利的行使带有特殊的义务和责任，因此得受某些限制”。

在多利益攸关方层面——“各国政府应与各利益攸关方充分合作，并引导社会各方面理解他们在信息安全方面的作用和责任，包括私营部门和民间社会”，“加强双边、区域和国际合作……加强相关国际组织之间的协调”。

4. 2011年11月2日伦敦网络空间国际会议主席声明[6]

在国家主权层面——与会者担心一些国家利用主权原则作为限制、

封锁网站，以及对互联网内容进行审查的手段。

在人权与基本自由层面——本次会议认同提升网络安全不能以牺牲人权为代价；大会获得广泛认同的原则是，网络空间必须对思想、信息和表达的革新与自由流通保持开放。

在多利益攸关方层面——与会代表呼吁发展中国家、公众、投资人和国际发展组织协同努力，以确保我们能够驾驭互联网经济、掌控社会收益；在进一步拓展现有的工作，例如发展经济合作与发展组织原则时，许多代表都认同，所有利益攸关方——包括发展中国家和发达国家的公司、社会民众以及政府的共同参与至关重要。

5. 2012年伦敦进程布达佩斯会议[7]

在国家主权层面——青少年论坛中的报告员注意到教育在应对网络安全威胁中的重要性，指出政府应当为学校提供指南并保证该指南在实施中的连贯性。一些与会人员强调国家必须在网络安全中扮演核心角色，而国际组织则扮演重要角色。此外座谈小组成员认可私人主体也是网络空间重要行为人，政府在处理网络安全问题时需要与之合作。

在人权与基本自由层面——来自座谈小组B组有关社会利益和人权的报告员指出，数字时代需要政府采取适当措施以保障人权。青少年座谈小组第一报告员也强调了人权在互联网发展中的重要作用，以及保障网络自由的必要性。

在多利益攸关方层面——在全体大会第二部分“能力建设：政策内涵和驱动”部分指出，能力建设是一项复杂的、需要多层级参与的实践；加强信息社会安全需要所有利益攸关方，例如政府、国际组织、私人主体和公民社会等的协调努力。

6. 2013年6月联合国信息安全政府专家组（简称UN GGE）在一份一致通过的重要报告[8]中指出：

在国家主权层面——“国家主权和在主权基础上衍生的国际规范及

原则适用于国家进行的信息通信技术活动，以及国家在其领土内对信息通信技术基础设施的管辖权”。

在人权与基本自由层面——“国家在加强信息技术安全的同时，必须同时尊重《世界人权宣言》中的人权和基本自由”。

在多利益攸关方层面——“在增进信息技术安全的合作中，国家是引擎，其他主体是有益的参与者”，“国家应当提供最好的技术及其他方面的援助，以便与国际组织、联合国各机构以及私人主体合作共建信息安全能力”。

7. 2013年版的《关于可适用于网络战的国际法的塔林手册》（简称《塔林手册》）

在国家主权层面——在规则1（主权）指出，“一国有权对其领土内的网络基础设施和网络活动行使控制”。

在人权与基本自由层面——在规则31（区分原则）中重申“《日内瓦公约》第一附加议定书第51条和第52条旨在保护平民和民用目标的区分原则”。依据规则87（尊重占领地受保护者），“占领地被保护者必须获得尊重并免受网络操作的有害影响”。

8. 2013年首尔会议达成了《旨在维护网络空间开放与安全的首尔框架及承诺》[9]

在国家主权层面——在国际安全部分明确指出，“国家主权以及由该项权利所延伸出来的原则、准则，适用于国家在信息空间的活动，且国家对其领域内的信息基础设施享有管辖权”。

在人权与基本自由层面——在第2部分（社会和文化利益）中指出，“根据《世界人权宣言》和《政治与公民权利国际公约》第19条，人们在线时也必须享有离线时享有的相同权利和义务，尤其是表达自由，且该权利的行使不受边界和媒介限制”。

在多利益攸关方层面——在第1部分（经济增长与发展）中指出，“要共同努力，以构筑一个包括国际组织和私人主体在内的，值得信赖、安全和可持续的多利益攸关方合作环境”。

9. 2015年联合国信息安全政府专家组报告[10]指出

在国家主权层面——“国家主权和在主权基础上衍生的国际规范及原则适用于国家进行的信息通信技术活动，以及国家在其领土内对信息通信技术基础设施的管辖权”。此外，该报告还在开头的总结部分指出，“国家主权原则是增强国家运用信息通信技术安全性的根基”。

在人权与基本自由层面——“国家在打击网络恐怖主义和网络犯罪过程中，应当充分尊重人权，包括隐私和表达自由”，“适用于网络空间的国际法，包括尊重人权和基本自由原则、人道主义原则等”，“国家在确保网络安全的同时，应当尊重联合国人权理事会《有关增进、保护和享有网络人权的第20/8号和第26/13号决议》”。

在多利益攸关方层面——“考虑到互联网的发展速度和相应的威胁范围，有必要增进共识、加强合作。为此，政府专家组建议联合国内部各机构之间，双边、区域和多边论坛以及其他国际组织，应当开展定期对话”，“国家对维护网络安全与和平负有首要责任，而多利益攸关方的参与是实现有效国际合作的重要条件”。

10. 2015年伦敦进程-海牙会议主席声明[11]

在国家主权层面——在“国际和平与安全”部分明确指出，“有必要达成关于国家主权原则如何适用于网络空间国家行为的国际共识，同时要确保与国家的国际义务、国家责任相一致”。

在人权与基本自由层面——前言部分指出，“必须确保包括表达自由、隐私权在内的人权，在线上和线下受到同等保护”。

在多利益攸关方层面——在互联网治理部分指出，“重申互联网治理的多利益攸关方模式，呼吁所有攸关方进一步加强、维持、参与并革

新该模式”。

11. 2015年G20安塔利亚峰会公报[12]

在多利益攸关方层面——“如同在其他环境中，在信息通信技术环境，国家负有特殊责任，促进安全、稳定，密切同其他国家的经济联系。……所有支持安全使用信息通信技术的国家都应尊重和保护自由原则，使其免受非法和任意干涉隐私所扰，包括在数字通信的情况下。”

12. 2016年G7关于网络空间原则和行动的声明[13]

在国家主权层面——国家在应对网络空间的武装攻击时，可以依照联合国宪章第51条和国际法，行使其固有的单独或者集体自卫权。

在人权与基本自由层面——在“我们寻求的网络空间”部分，确认尊重并促进隐私、数据保护和网络安全；在线上应当享有与线下同样的人权。

在多利益攸关方层面——在“我们寻求的网络空间”部分，强调在网络空间治理中采用多利益攸关方模式；在“促进网络空间安全和稳定”部分，声明要充分实现网络空间的安全与弹性，只有通过国际和国内不同行为主体的紧密合作才能实现。

13. 2016年金砖国家领导人《果阿宣言》

在国家主权和人权与基本自由层面——“我们重申，在公认的包括《联合国宪章》在内的国际法原则的基础上，通过国际和地区合作，使用和开发信息通信技术。这些原则包括政治独立、领土完整、国家主权平等、以和平手段解决争端、不干涉别国内政、尊重人权和基本自由和隐私等。这对于维护和平、安全与开放的网络空间至关重要。”

在人权与基本自由层面——“我们重申，信息通信技术的广泛应用是实现可持续发展、维护国际和平与安全、保障人权的关键推动力。”

14. 2017年“塔林手册2.0版”[14]

在国家主权层面——在“主权”一章包括以下四条规则：①基本原则（国家主权原则适用于网络空间）；②对内主权（国家在遵守其国际法义务的前提下，对其境内的网络基础设施和网络活动享有主权权威）；③对外主权（国家在其国际关系中可自由采取网络行动，除非对其有约束力的国际法规则作出了相反的规定）；④对主权的侵犯（国家不得采取侵犯另一国主权的网络行动）。

在人权与基本自由层面——在“人权”一章包括以下五条规则：①国际人权法适用于网络空间；②个人在网络空间享有的人权与他们在网络空间外享有的人权相同；③对于各种网络活动和行动，国家必须：a.尊重个人的国际人权，b.保护个人人权不受第三方侵犯；④除那些绝对性的人权外，尊重和保护国际人权的义务可以受到某些限制，如果这些限制是为了实现一个正当的国家目标所必需的，并且是非歧视的和得到了法律的授权；⑤在为有关条约所准许并符合该条约所规定的条件时，各国可以克减其根据条约承担的对网络活动的人权义务。

15. 2012年以来联合国大会和人权理事会，有关网络人权的几项重要决议

（1）2012年7月5日联合国人权理事会通过的《关于在互联网上增进、保护和享有人权的第20/8号决议》[15]：“确认，根据《世界人权宣言》第十九条以及《公民权利和政治权利国际公约》第十九条，民众在线上必须能够享有与线下相同的权利，尤其是言论自由，且该权利的行使不受国界和媒介限制。”

（2）2013年12月18日联合国大会通过的《关于数字时代隐私权问题的第68/167号决议》[16]：“重申，根据《世界人权宣言》第十二条以及《公民权利和政治权利国际公约》第十七条，个人隐私、家庭、住宅不受任意或非法入侵”，“民众在线上必须能够享有与线下相同的权利，包括隐私权。”

（3）2013年12月20日联合国大会通过的《关于信息和通信技术促进发展的第68/198号决议》[17]：“注意到在使用信息和通信技术过程中，尊重人权和基本自由的重要性”，“确认民众在线上必须能够享有与线下相同的权利，包括（数字时代的）隐私权。”

（4）2014年3月27日联合国人权理事会通过的《关于数字时代隐私权问题小组的第 25/117号决定》[18]：“根据《世界人权宣言》第十二条以及《公民权利和政治权利国际公约》第十七条，个人隐私、家庭、住宅不受任意或非法入侵”，“民众在线上必须能够享有与线下相同的权利，包括隐私权。”

（5）2016年7月1日联合国人权理事会通过的《互联网上推动、保护及享有人权》[19]：“根据《世界人权宣言》第十九条以及《公民权利和政治权利国际公约》第十九条，民众在线上必须能够享有与线下相同的权利，尤其是言论自由，这项权利不论国界，可以通过自主选择的任何媒介行使”，“国家必须克制和停止任何阻止和干扰在互联网上传播信息的行为。这包括在任何时候关闭全部或部分互联网，特别是在人们急需获取信息的情况下，例如选举期间或是恐怖袭击之后。”

小结

从历史发展和内容更新来看，上述网络空间国际会议及其达成的成果文件以及与人权相关的国际组织决议，既存在共性，也有鲜明的差异性。首先从共性上看，这些成果文件首先都会关注网络空间领域最新发展态势以及国际社会所普遍面临的问题，都会从不同侧面对如何应对这些问题提出建设性方案或者倡议，更重要的是，鉴于网络空间问题的新颖性和复杂性，上述文件普遍强调国家主权原则在信息通信领域（网络空间）的适用，都重视对数字时代网络人权的保护，而在具体操作上基本倾向于采用多利益攸关方合作治理模式。

其次从差异或者发展上看，上述会议及其成果文件对国家主权原则、网络人权以及多利益攸关方的看法和主张，存在着明显的变化和发展：

（1）从强调形式平等走向关注实质平等，例如2003年《日内瓦原则宣言》仅从形式上强调“坚持所有国家主权平等原则”，到了2015年联合国信息安全政府专家组报告，在国际法如何适用于信息通信技术部分，国家主权被明确规定为适用于所有国家对其境内信息基础设施的使用和管理活动，以及解决国家间争议的过程之中。对于网络人权的保护则更加具体明确，例如2016年7月1日通过的《互联网上推动、保护及享有人权》，将国家不干涉的义务具体到选举期间或是恐怖袭击之后。

（2）与（1）相对应，国家主权原则、人权和基本自由、多利益攸关方模式的内容在不断深化和完善。

（3）对网络国家主权原则的制定权争夺日趋激烈，有关网络人权和多利益攸关方合作治理模式的内涵及其发展走向，存在分歧扩大化倾向。新兴国家与西方国家基于价值观、意识形态和国家利益等方面的显著差异和分歧，在网络空间规则的内容和制定场所方面的争夺、对网络人权的理解分歧以及对多利益攸关方治理模式的实施差异都在所难免。网络主权最早由新兴国家提出，但关于该概念的内涵和边界，西方国家与新兴国家尚未达成共识，而要在网络人权和多利益攸关方的内涵和落实方面达成一致，也必将面临重重阻力与困难。

最后，根据2015年联合国信息安全政府专家组报告的总结和展望，随着联合国在推动网络空间行为规则对话和发展方面的主导作用逐渐增强，如果西方国家与新兴国家能够将“人类命运共同体”意识、“和谐”与“共进”理念切实融入对话和合作过程中，那么有关网络主权、网络人权以及多利益攸关方运作的国际共识定会不断增多，网络空间和平与发展将获得更加稳固的保障。

---

[1] 本附录由黄志雄教授和武汉大学国际法研究所博士生刘碧琦共同完成，主要整理了2003年以来各种重要国际场合与网络主权相关的重要表述。这里所指的“国际场合”，既包括更具国际代表性和权威性的联合国等政府间国际组织，也包括主要由西方国家主导的“伦敦进程”历次会议（2011年伦敦、2012年布达佩斯、2013年首尔、2015年海牙），以及二十国集团（G20）、七国集团（G7）领导人声明和《塔林

手册》及其“2.0版”这样的非官方性专家成果。“与网络主权相关的重要表述”，则包括直接涉及网络空间国家主权问题的表述，以及与之密切相关的网络人权与自由、多利益攸关方等问题的表述。

[2] 2003年信息社会世界峰会（WSIS）第WSIS-03/GENEVA/9（Rev.1）-C号文件http：//www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0009！R1！PDF-C.pdf.

[3] 2005年信息社会世界峰会（WSIS）第WSIS-05/TUNIS/DOC/7号文件https：//documents-dds-ny.un.org/doc/UNDOC/GEN/N06/254/41/IMG/N0625441.pdf?OpenElement。

[4] 2005年《突尼斯议程》http：//www.un.org/chinese/events/wsis/promises.htm。

[5] 联合国大会第A/69/723号决议，“2015年1月9日中国、哈萨克斯坦、吉尔吉斯斯坦、俄罗斯联邦、塔吉克斯坦和乌兹别克斯坦常驻联合国代表给秘书长的信”http：//www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_67491

[6] London Conference on Cyberspace：Chair’s Statementhttps：//www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement.

[7] Budapest Conference on Cyberspace，4-5 October 2012，Summary by the Chairmanhttps：//www.gccs2015.com/sites/default/files/documents/Chair’

[8] 联合国大会第2013/A/68/98号决议，Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.https：//ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf.

[9] “Seoul Framework for and Commitment to Open and Secure Cyberspace”
http：//www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf.

[10] 联合国大会第2015/A/70/174号决议，Group of Governmental Experts on developments in the field of information and telecommunication in the context of international
security.http：//www.un.org/ga/search/view_doc.asp？symbol=A/70/174。

[11] Global conference e cyberspace 2015，chair’s statementhttp：//www.interpol.int/News-and-media/News/2015/N2015-043.

[12] 《二十国集团领导人安塔利亚峰会公报》，
http：//news.xinhuanet.com/2015-11/17/c_1117160248_2.htm。

[13] G7 Principles and Actions on Cyberhttp：//www.mofa.go.jp/files/000160279.pdf.

[14] Michael Schmitt （ed.），Tallinn Mannual 2.0 on the International Law Applicable to Cyber Operations，Cambridge University Press，2017.

[15] A/HRC/RES/20/8，The promotion，protection and enjoyment of human rights on the Internethttps：//documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.

[16] A/RES/68/167，The right to privacy in the digital age
http：//www.un.org/en/ga/search/view_doc.asp？symbol=A/RES/68/167.

[17] A/RES/68/198，Information and communications technologies for developmenthttp：//www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/198.

[18] A/HRC/25/L.12 Panel on the right to privacy in the digital agehttps：//documents-dds-

ny.un.org/doc/UNDOC/LTD/G14/123/27/PDF/G1412327.pdf?OpenElement.

[19] A/HRC/32/L.20 The promotion，protection and enjoyment of human rights on the Internethttps：//documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.