面向 IPv6 的网络空间国际治理联合研发与示范课题组发布

网络空间国际治理：现状与问题

清华大学课题组

2021 年 7 月

目录

前言

新冠肺炎疫情爆发以来，世界各国安危相依，人类命运休戚与共，你中有我、我中有你的人类命运共同体理念愈发彰显出时代价值。但在网络空间，国际社会就治理问题尚未达成一致意见。一方面，随着信息和数字技术对国家安全与发展的影响日益增加，单边主义、霸权主义的国际交往策略从物理空间蔓延到网络空间，使后者俨然成为大国博弈的新场域；另一方面，国际组织、跨国互联网企业、技术社群等多种主体，为全球互联网治理领域注入新的变数。

全球互联网治理将走向何方？未来的治理规则将体现何种关切？互联网将如何影响国际格局、一国的安全和发展，进而影响人们的生活？

太阳底下无新事也许过于绝对，但未来总是从过去和现在中生发出来的。

这份白皮书爬梳了网络空间国际治理总体架构、安全治理和数字发展的现状，是“面向 IPv6 的网络空间国际治理联合研发与示范项目”课题组深度合作与交流的成果。我们期待以此抛砖引玉，引发更多思索和探讨。

第一篇 治理架构

2020 年 12 月 7 日，中共中央印发《法治社会建设实施纲要（2020—2025 年）》，强调“网络空间不是法外之地”，“依法治理网络空间”。[1]2020 年 11 月 23 日，国家主席习近平向世界互联网大会（WIC）的互联网发展论坛致贺信，强调“打造网络安全新格局，构建网络空间命运共同体”。早于 2015 年，习近平就在第二届 WIC 提出“四项原则”“五点主张”，倡导尊重网络主权，为全球互联网发展治理贡献了中国智慧、中国方案。[2]为进一步阐释理念，WIC 组委会于 2020 年发布《倡议》文件，呼吁各国政府、国际组织、互联网企业、技术社群、社会组织和公民个人等多元主体，坚持共商共建共享的全球治理观，秉持“四个共同理念”，建设“五个共同体”，其中强调：一发挥联合国的主渠道作用，尤其是联合国信息安全开放式工作组（OEWG）和政府专家组（GGE）；二共享共治的国际治理机制，支持联合国互联网治理论坛（IGF）、世界互联网大会（WIC）、世界移动大会（MWC）、国际电信联盟（ITU）等平台发挥积极作用；三平等参与互联网基础资源管理，涉及互联网名称与数字地址分配机构（ICANN）的 DNS 名称与 IP 地址分配。[3]“窥一斑而知全豹”，这反映出网络空间的国际治理。治理（governance）比政府（government）的概念更包容，后者特指自上而下的科层制权力体系，而前者包含指导与塑造等非强制性元素。

那么网络空间国际治理的核心问题是什么？在于“谁用什么治理网络空间”。

首先，网络空间作为对象是复杂的。从“三阶层”看，网络空间在物理层、逻辑层、内容层展现不同的面相[4]，在具体场景中又关联起来。例如，网络空间往往被认为超越国家主权边界，但是在物理层上互联网与电信网紧密关联，而电信网的关键基础设施受到国家以安全为由的强监管。再例如，逻辑层上 ICANN 分配 DNS 域名，规定“仇恨言论”的负面清单。这实质上是对内容层的治理，因为其所规制的并非域名，而是域名指向网站的内容偏好。因此，问题在于国家对“网络空间”采取怎样的对外立场。这涉及到国际政治学的三大视野，即现实主义的

“权力”（power）、自由主义的“制度”（institution）、建构主义的“观念”（idea）。

其次，“谁”作为主体是多元的。国际关系缺乏超越主权的政治实体，因此处于“anarchy”状态。在这前提下，传统国际治理有赖于主权国家参与展开。因此，“主权国家”是主体的存在。例如，多边主义中，国家参与信息社会世界峰会（WSIS）制定《突尼斯议程》，区分互联网的“技术”与“政策”命题，并强调国家在“政策”命题中的主体性。双边主义中，美国与欧洲制定的“隐私盾”机制因欧洲法院判定违法无效而折戟。单边主义中，美国对微软公司用户在爱尔兰服务器的电子邮箱发出秘密调查令，并因此法律纠葛推动 CLOUD 法案的产生。同时，网络空间的国际治理涌现出“他者”的存在。例如，以“私有化”与“利益相关者”逻辑运作的 ICANN，主导 IP 标准制定的国际民间技术组织 IETF。此外，拥有跨国业务的互联网巨头企业也参与其中，如 GAFA 与 BAT，其中微软等公司参与《巴黎倡议》与《基督城行动协议的人道主义和军备控制》。因此，问题在于一国处于国际治理格局中的什么地位。

再者，“什么”作为治理方法是多样的。传统国际治理围绕国际公法，而国际公法渊源于国际条约、国际惯例等，皆是基于威斯特伐利亚体系以降的“主权”概念展开。主权滥觞于地理空间的划疆而治。但是，网络空间是新型空间。因此，需要重新体认“网络主权”的概念。此外，除了滥觞于主权的法律，代码、标准、市场也展现出作为治理方法的倾向。因此，问题在于一国对国际治理方法有什么偏好。

综上，网络空间的国际治理场景中，对象复杂、主体多元、方法多样，指向核心命题“谁用什么治理网络空间”。

1. 作为治理对象的网络

1.1 网络

可以治理网络空间吗？其本质是什么？

劳伦斯·莱斯格（Lawrence Lessig）认为，网络空间基于互联网产生，所涵盖的内容却比互联网丰富得多。[5]可见，他是从内容层的互动角度来认识的。“网络”的概念滥觞于数学分析，分为链路（links）与节点（nodes）。社会学家沃尔特·鲍威尔（Walter Powell）提出“网络”既非市场也非科层组织，其以“关系”而非以“交易”为基础，由行动者之间长期的互惠关系于信任维系，因此太过稳定而不能归类为市场交易，但又因组织上太过松散而不能归类于科层组织。[6]约翰·本克勒（Yochai Benkler）则结合开源软件与维基百科例证，认为网络是“基于共享协议的对等共创生产模式”。[7]弥尔顿·穆勒（Milton Mueller）则认为，本克勒与鲍威尔的理论区别，在于本克勒否认“关系”的归依，而强调网络的基础在于“通过分享所获利益、从贡献中所获满足以及系统运作所需的最基础信任”。[8]这就与边沁以降的功利主义相关系，从而更好地解释现代“陌生人社会”中网络何以迅速发展壮大。例如，内容层的 P2P 模式。再如，逻辑层的互联网服务提供方（ISP）[9]基于边界网关协议（BGP）而松散合作，通过规模流量的对等清讫来免除彼此收费。

穆勒将“网络”按照“是否有意识安排”区分为“事实的网络”与“人为的网络”，前者称为“关联集群”，后者称为“网络组织”。 关联集群”又可继而分为“政策网络”“议题网络”与“跨国倡议网络”。[10]这实质上是事实与规范的二分。实事求是，就“国际治理”而言，网络空间的实然事实不得不鉴，但治理的命题还是在于应然的规范，即“网络空间应当如何”。例如，“域名系统根”的根服务器在事实层面仅是一个分配区域文件的松散电脑网络，但在规范层面全球其他电脑“应当”将该文件视为权威，从而将技术命题过渡到“权威”的政策命题，并通过 ICANN 有意识地制度化，为主权国家所关切。

应当注意的是，当称呼“网络”为“网络空间”时，其已预设了空间场景的概念。但是“网络空间”与“地理空间”存在差别。诚如学者指出，网络同时存在于一个“空

间”中，但没有一个“点”。“这里”所做的操作具有“在那里”的瞬时作用。结果，网络空间没有提供任何实际堡垒或避难所。国防基础设施所在的网络空间与其他国家的国防基础设施所在的网络空间位于同一位置。关键基础设施在与其他国家相同的“空间”中运作。[11]

1.2 互联网

“互联网”与“网络”是什么关系?

一种观点认为，互联网是网络的网络。一个被互联网连接的网络的内部通信协议，完全是这个网络的自治，互联网不干涉每个网络的内政。诚如互联网国际标准化组织 IETF 的使命定位“above the wire, below the application”，wire 及其以下的事情，交给每个被互联的“网络”自行解决，而“application”及其以上的事情，交给用户应用去解决。而 IETF 关注的领域，则是 IP 协议、路由协议、传送协议、网络管理、网络安全，即概括为“互联网体系结构技术”。[12]

互联网兴起与电信行业自由化相关。例如，美国联邦通信委员会（FCC）提出《计算机调查报告》，建议把美国“基本的”电信服务从涉及数据处理以及计算机网络的“增强型”服务中分离出来，前者作为公共载体仍受到管制，而后者将会开放而不受管制。这推动互联网在全球的扩张，因为美国的上述改革导致互联网服务提供方（ISP）的市场准入门槛降低，而且该标准通过 WTO 等贸易谈判议程推广到其他发达国家经济体。就互联网扩张与自由贸易谈判的关系，2020 年签订的《区域全面经济伙伴关系协定》（RCEP）关于“电信服务中网络元素的非捆绑”内容就是实例。

值得注意的是，互联网天生具有社群自治的属性。例如，当网络社群所认可内容被外部力量（尤其是由上至下的垂直治理）破坏，由于社群的网络化关系还在，被破坏的内容会迅速恢复。[13]此外，互联网体现私人市场与共享机制的互补关系。从制度经济学上看，互联网排除了私人与公共的机械二分，承认互联网终端的私有化与互联网核心的共享化是可以互相依存的。

2. 谁来治理

制定规则的权力来自哪里？这是主体性的问题。“网络现实主义”与“网络自由主义”存在争论，前者强调国家基于主权的主体地位，后者强调技术决定论而以技术解决治理问题。但是，穆勒指出一部分“网络自由主义”是“网络现实主义”的存在，因为只要被挑战的国家是美国，他们就为美国辩护，允许其（通过 ICANN 技术机制）控制、主导互联网。[14]这揭示出美国与 ICANN 的微妙关系。

就发展而言，本克勒阐述“基于群体的对等共创生产”（commons-based peer production）来解释开源软件实践，其强调技术的去科层制。[15]可见，这是“网络自由主义”的衍生。与此对比，“多方利益相关主义”（multistakeholderism）则强调治理对国家之余的其他利益相关者开放，展现出对“网络现实主义”的修正。

具体地看，ICANN 与 WSIS 是两个治理方向的实例。ICANN 是美国单边主义的产物，并以“非政府模型”、“技术性议题路径”建立。而 WSIS 是国际多边主义的产物，以国家为中心的外交会议展开。“合纵连横”，WSIS 是否可以“合纵”？一种可能是，WSIS 为发展中国家政府及欧盟提供挑战美国优势地位的“围攻光明顶”平台。基于“自由主义”的解释，机制一旦发展成熟即有其独立性而不为发起者的意志左右。换言之，即使 ICANN 由美国主导建立，但其一旦成熟则不再受美国意志桎梏，甚至反而制度性地规范美国行为。因此，ICANN 与 WSIS 都面临这个问题。例如，奉行“多方利益相关主义”的技术社群积极游说 WSIS 对多方开放，而不能仅限于国家政府与国际组织的议事。

2.1 美国

美国与 ICANN

一些观点抨击网络空间是“以美国为中心”。这与历史有关。诚如前文 2.2 所述，美国电信行业自由化改革推动互联网兴起，并通过美国主导自由贸易谈判推动互联网全球化。同时，互联网技术在美国发展起来，协调关键技术的 ICANN 与美国政府有合同关系。ICANN 的私有化是由美国主导的，克林顿政府选择将互联网政策的制定权力委派给这家位于美国的私营非赢利机构，并阻止各国政府代表进入 ICANN 董

事会（包括美国政府，但是“XXX 域名”事件反映出美国政府对 ICANN 的实际影响力，即便不进董事会也无妨），名义上只允许各国政府通过“政府咨询委员会”（GAC）参与其中。

对此的一种辩解是“良性利维坦”，即美国单边主义权威总比国际“无政府状态”（anarchy）下的权威缺位要好。这种辩解曾受美国盟友（如欧盟诸国）的青睐。但是，斯诺登的揭露事件冲击“良性利维坦”的说服力，也损害了与欧洲盟友的关系，后者愤怒地做出反应，并威胁说如果政府不改变美国政策，中止信息共享安排（information-sharing arrangements）。结合 Stuxnet，斯诺登的披露也削弱了美国政府开放，安全和全球网络空间（open, secure and global cyberspace）的国际战略。美国为促进国际网络规范所做的复杂努力；并对美国政府不支持的规范提出了新要求，例如将国际人权法应用于美国在美国境外进行的网络监视（surveillance）和间谍（espionage）活动。[16]

无论如何，美国通过“三合同”确保对 ICANN 的政治监管：一是美国商务部与 ICANN 订立的《互联网数字地址分配局合同》（IANA），授权 ICANN 执行 IANA 的技术职能，包括 IP 地址资源、编辑根区文件以及协调唯一协议号码的分配，但是对 IANA 根区文件的修改都必须经美国商务部的审核与同意；二是美国商务部与 ICANN 订立的《联合项目协议》（JPA），提供一份美国政府期望 ICANN 执行的政策制定任务清单，其中特定优先事项和阶段性目标反映美国政府利益；三是美国商务部与威瑞信有限公司（Verisign）订立的合同，约定主根服务器运营公司 Verisign（拥有.com 和.net 顶级域名 TLDs）应当执行 ICANN 流程通过的技术协调决策，而且应当遵守美国政府有关根区文件的指示。

为应对国际社会对美国单边监管 ICANN 的压力，“多方参与主义”是一种合法性辩解。原因在于，ICANN 作为私营部门将政策制定者、技术专家、商业团体与用户等多方利益纳入同一框架。这似乎与欧盟的立场趋同，即多方参与中“以私营部门为主导的体系”，因此美国争取欧盟支持，连横以分离与发展中国家强调“以国家政府为主导的多边体系”。

2005 年 6 月 30 日，美国商务部下属的国家电信和信息管理局（NTIA）发表《美国有关互联网域名和地址系统的原则性声明》，重申美国的单边监管只是技术监管，基于保护 IP 与 DNS 的安全性和稳定性，因此有意维持“在授权改变和

修改权威的根区文件方面上的传统地位”，但同时意识到他国对国家和地区代码顶级域名（ccLTDs）主权的担忧，认为互联网治理对话应在多场合展开而非限于一个政治平台。可见，美国有意将网络治理拉张到“多方参与主义”对传统网络现实主义的修正方向，通过开放性议题纳入私营部门与技术群体而赋予 ICANN 合法性，同时尝试将其他国家的不满纳入 ICANN 的 GAC 建制中，并通过多平台而非一平台来离间“合纵”倾向。

但是，美国在“XXX 域名事件”中很快就打破了上述技术监管的承诺。2005 年 8 月，商务部部长助理迈克尔·加拉格（Michael Gallagher）给 ICANN 主席文特·瑟夫（Vint Cerf）及其 CEO 保罗·图梅（Paul Twomey）致信，表达对 XXX 域名用于色情网站域名引发美国社会呼声的担忧，并要求 ICANN 推迟决定，同时该信亦发给 GAC 主席穆罕默德·沙利尔·塔尔米茨（Mohd Shari Tarmizi）及成员。随后，塔尔米茨致信给 ICANN 董事会，表达国家政府中存在对“XXX 域名”的担忧，要求 ICANN 在作出最终决定前给予额外时间让政府和公众表达担忧。于是，ICANN 推迟决议并最终否决 XXX 域名申请。虽然美国政府与 ICANN 强调推迟是因为 GAC 主席的信函而非美国干预，但穆勒认为美国施压才是真正原因，因为美国政府受到宗教右派施加的国内政治压力。[17]可见，美国所谓技术监管承诺是形式上的，实质上的技术与公共政策命题难以二分，国际治理的中立承诺也难以与国内政治压力干预相区分。虽然“XXX 域名事件”冲击美国单边监管承诺，但其在某种程度上又被拿来反对国际多边主义。大卫·麦奎尔（David McGuire）提出一种逻辑，如果 XXX 域名因美国一国的意识形态压力而被否决，那么在国际多边主义下，各国林林总总的意识形态怎么能够解决域名是否应被否决的问题呢？[18]更何况，域名系统安全扩展（DNSSEC）与网络安全相关，但其数字签名被美国掌握的技术要求又引起其他国家的国家安全担忧。

美国与网络安全

奥巴马上任的目的是将网络安全放在首位。2009 年 5 月发布的《网络空间政策评论》传达的信息直言不讳：美国对信息和通信技术的日益依赖，加剧了网络犯罪，恐怖主义和外国攻击的脆弱性，而美国政府，私营部门和社会对此无能为力。该结论清楚地表明，布什政府的努力，包括 2003 年 2 月的《国家网络安全战略》（National

Strategy to Secure Cyberspace）和 2008 年 1 月制定的机密的《国家网络安全综合计划》（Comprehensive National Cybersecurity Initiative，CNCI），均未能实现。奥巴马政府治下，2010 年成立美国网络司令部，，并于 2011 年发布了美国国防部首项网络空间战略文件。[19]2011 年，时任国务卿希拉里·克林顿（Hillary Clinton）在 Chris Painter 的领导下成立了网络问题协调员办公室（Office of the Coordinator for Cyber Issues）。这个办公室主要致力于通过联合国和 20 国集团等多边机构建立关系并支持有关网络挑战的对话，从而推动关于网络空间中国家行为和责任的议程。

2013 年，奥巴马政府通过联合国政府专家小组（U.N. Group of Governmental Experts）来推动“国际法应适用于网络空间”的主张，但这与中国与俄罗斯强调的“网络主权观”有所出入。

特朗普政府则通过诸如“数字连接和网络安全合作伙伴计划”（Digital Connectivity and Cybersecurity Partnership）之类的计划，试图建立对其他国家的监管能力。美国国际开发署公布了有史以来的第一个数字战略，该战略旨在通过与外国政府和民间社会团体建立伙伴关系来推进美国“开放，包容和安全的数字生态系统”（open, inclusive, and secure digital ecosystems）的愿景。[20]诚如奥巴马政府前任网络协调员（former cyber coordinator）迈克尔·丹尼尔（Michael Daniel）认为，在 2020 年形势下网络安全跨越了美国国家安全的优先领域，包括情报，执法和商业等。例如，《国家网络总监法》（National Cyber Director Act）得到了两党的支持，将遵循“Solarium Commission”的建议，在总统执行办公室中建立白宫网络问题首席顾问（lead White House adviser）。[21]

2.2 欧盟

欧盟积极介入网络空间治理。但其机制是迭代的，而非创新的。诚如学者指出，欧盟进入网络安全领域后，欧洲网络的运营和监管状况发生了明显的制度性变化，但这种变化既不是突然的，也不是革命性的。而是在现有的欧洲网络中安装了一个新的协调中心。在新法规实施时，欧盟对部署的机构中的状态进行了微小的增量更改。[22]

在 WSIS 中，欧盟支持“利益相关主义”与“多边主义”的杂糅。这种立场导致美国在“利益相关主义”一端积极争取欧盟的支持，而持“多边主义”的国家也争取欧盟的支持。需要明确地是，欧盟强调的是新合作模式，虽然有公私合作治理的存在，但是以私营部门为主导，国际政府只在“原则层面”制定公共政策。这与“多边主义”强调以国家政府为主导有很大不同。因此，难以将欧盟立场视为对“主权导向”的认可。

而欧盟强调的“私营部门主导”治理，则与美国主导的 ICANN 私有化暗合。但是，欧盟反对美国单边监管，而认为美国应该放手。这是欧美的隔阂所在。例如，2005 年 9 月的 WSIS 筹备委员会会议上，英国作为欧美的轮值主席国就呼吁改革 ICANN 体制，令 ICANN 监管国际化。

除了逻辑层上对 ICANN 监管有分歧外，欧盟与美国在内容层上的个人数据方面也有分歧。例如，为了衔接美国与欧盟在个人数据保护领域的标准不同，尤其是为了满足美国互联网企业在欧盟的经营需要，双方行政当局先是达成“安全港盾”（Safe Harbor Shield），后被欧盟法院（the Court of Justice of the European Union）宣告无效后，又达成“隐私盾”协议（Privacy Shield），旨在美国企业在履行美国标准之外自愿承诺达到欧盟标准，并为欧盟公民提供法律救济程序，从而达到《通用数据保护条例》（GDPR）。但是 2020 年 7 月 16 日，欧盟法院再次宣告“隐私盾”无效。[23]这反映出欧盟与美国在内容层上双边治理的困境。

综上，在网络治理问题上欧盟与美国存在分歧。但是，一些专家认为分歧可以弥合，并将美国与欧盟的治理合作摆在首要地位。美国总统拜登的国务卿人选安东尼·布林肯（Antony Blinken）就持这种立场：首先，他认为欧盟与美国的融合联系就在于英语和互联网，故会把互联网治理摆在外交议程的首要地位。[24]其次，他主张发挥互联网的主动作用，尤其与希拉里在利用互联网发动“阿拉伯之春”等外交攻势相一致，即将互联网公共政策化。[25]再者，他判断美国与欧盟的分歧不会消失，在有争议的问题上也不会立即出现共识，但是欧盟与美国合作的基础建立在经济富有、民主价值上，因此倡导“欧盟优先”的外交政策。[26]

2.3 联合国

“花开两朵，各表一枝。”2018 年 11 月 8 日，联合国大会通过两项关于网络空间国家行为的独立决策。其中一项由俄罗斯提交，将在联大之下设立一个开放性工作组（open-ended working group，OEWG），负责研究联合国信息安全政府专家组此前报告中的既有规范、提出新规范并探索“在联合国框架下建立定期对话机制”的可能性。另一项由美国提起，将设立一个新的政府专家组（Group of Governmental Experts, GGE），负责研究现有国际法如何适用于网络空间的国家行为，并提出促进遵守现有网络规范的途径。[27]

OEWG 与 GGE 的方案存在差别。程序上，GGE 成员较少，授权期限有限，从而避免 GGE 议事拖延。而 OEWG 成员众多，所有联合国会员国都可参与审议，“开放性”意味无期限授权，除非各会员国统一解散该工作组。范围上，OEWG 还在闭会期间举办多利益攸关方的磋商会议，而会议发言过程的公开透明、有迹可循。

从“合纵联横”角度考虑，俄罗斯主导的 OEWG 在于扩大“合纵”，即扩大与会国的参与而通过“合纵”施压来改变现状。而美国主导的 GGE 在于限制“合纵”，并尝试与特定成员国（如欧洲国家）连横来维护现状，同时通过限制多边主义的范围来维护多方主义下 ICANN 机制的现状。诚如在该提案的辩论会上，俄罗斯代表称，美国提议设立的新的政府专家组将是一个无法考虑到所有联合国会员国意见的“排他俱乐部”，并指出政府专家组难以为继，因 2016-2017 年的政府专家组未能达成共识。但是美国学者埃里克斯·格林格斯比（Alex Grigs）辩解称，政府专家组曾在 2013 年和 2015 年就国际法在网络空间的适用等问题达成重要的共识性文件，而俄罗斯对于阻碍通过 2017 年的共识性报告发挥了突出作用。[28]

值得注意的是，俄罗斯的 OEWG 方案删去源自上海合作组织《信息安全国际行为准则》的一些表述，进一步修改了其决议，以回应西方国家对人权问题的讨论。而联合国多数成员国，包括中国，投票同时通过了这两项决议。因此，在现行联合国框架中，OEWG 与 GGE 并行运作。

2020 年 9 月 11 日，中国和俄罗斯外交部长发表联合声明，双方强调在互联网治理问题上立场一致，包括保障各国平等参与全球网络治理进程。双方支持联

合国为规范信息空间中各国负责任行为制定规则、准则及原则，欢迎并指出根据联合国大会第 73/27 号决议启动联合国信息安全开放式工作组（OEWG）这一由联合国主导、各国均可参与的首个信息安全谈判机制十分及时，呼吁所有国家建设性参与根据联合国大会第 74/247 号决议设立的特设政府间专家委员会（GGE）的工作。[29]可见，中俄在外交立场上表明一致，通过联合国的多边主义机制发挥作用，支持 OEWG，并呼吁“以所有国家参与”的方式对 GGE 进行改革。

2.3.1 信息安全开放式工作组（OEWG）

2019 年 OEWG 开始运作。2020 年 3 月，OEWG 主席约尔格·劳伯（Jurg Lauber）拟定了报告草案（Pre-draft）指出两点：其一，在国际法适用问题讨论艰难前行的背景下，工作组进程要在负责任国家行为规范方面要取得实质性进展，提出自己的规范，从而有别于 2015 年专家组报告所规定的 11 条现有规范；其二，通过工作组进程的讨论，在联合国层面确立一个由所有会员国广泛参与的常设性对话机制，对国际信息安全问题进行定期、持续和连贯的谈判。有学者指出，OEWG 存在进展与分歧。其中的进展包括：

其一，负责任国家行为规范。尤其是以中国提出的关于网络空间国家主权、关键基础设施保护、数据安全、供应链安全和反恐怖主义的提案同时兼顾了规范多向发展的需要；

其二，规范与国际法协调互动。一方面国家行为规范需要符合国际法的基础上，规范作为国际法的补充，起到给各国在网络空间行为提供国际法之外的指引作用。另一方面，工作组开始认识到规范作为国际软法向有约束力的国际法转化的可能性。例如，中国在 2020 年 4 月就工作组报告草案提交的意见中指出，负责任国家行为规范的发展和执行实际上是在为未来制定有约束力的国际法文件积累共识，如果各方在未来能就相关规范达成共同且高度的共识，规范转化为有约束力的国际法是可能的；

其三，平衡现有国际法适用和制定新国际法需求。制定一个适用于网络空间的国际法新框架，同时解决适用现有国际法和制定新国际法的两方面问题。例如，俄罗斯主张根据信息通信技术的特点和发展所需，专门国际法文件既要“搭载”经

调整后能够适用于网络空间的现有国际法，还要在查明现有国际法未能解决的法律空白后，填补网络空间“法律真空”现状，专门制定新的国际法。

其四，技术中立。这与 GGE 主张的“军民二分”， 信息通信技术的军事运用可能给国际和平与安全带来威胁的理解相区别。尽管“技术中立”概念早前已由欧盟及其成员国在区域性范围内提出，而在联合国层面，尚属首次，并获得英国、澳大利亚的深度支持解读。

其五，强调非国家行为体的负责任行为。例如，克罗地亚、芬兰、法国和斯洛文尼亚号召各国关注对非国家行为者行为的规制，还认为对负责任国家行为规范的相关解读中要提升国家在规制非国家行为者方面的作用。这代表西方国家内部由强调发挥其他利益攸关方的积极作用向强调其行为责任的转变，以及西方国家对国家主权重视的回归。[30]

其中的分歧包括：

其一，对“新规范”的不同认识。例如，英国质疑其他国家提出的“新规范”提案，要么仅是现有规范的替代性表述，要么是对现有规范某一具体方面更细致地表述，类似于“换汤不换药”。英国还认为，数据保护、互联网治理、自由贸易、反恐等相关的新规范提案超出了 OEWG 工作组的授权范围；

其二，对负责任国家行为规范与国际法协调互动程度的认识。虽然中国主张规范向有约束力国际法转化的可能，但是 OEWG 的报告草案仍强调规范不取代或改变各国根据国际法承担的义务，而是就各国在使用信息通信技术时的责任行为提供额外的具体指导。而这种“规范指导论”的表述，获得澳大利亚、爱沙尼亚、德国的支持；

其三，对现阶段是否将国际法在网络空间的适用问题交由国际法委员会（ILC）研究和澄清的认识。尽管国家间关于国际法在网络空间的适用方面存在较大分歧，但是，大多数国家认为现阶段交由联合国国际法委员会研究和澄清这一问题的决定还为时过早，许多国家仍在加深国际法在网络空间适用方面的理解并形成相应的国家立场。与此相比西方国家认为现有国际法适用不存在障碍、坚持现有国际法全部适用。[31]

可见，OEWG 反映出“谁来治理”以及“用什么治理”的问题。前者涉及负责任国家行为与非国家行为体的负责任行为。后者涉及新旧规范、新旧国际公法的性

质与关系，即“旧瓶装新酒”还是“新瓶装新酒”的问题。

2.3.2 政府专家组（GGE）

2004年起，联合国组织 GGE，探讨“信息和通信技术”（ICT）使用过程中可能产生的威胁与如何维护网络安全。GGE 有 25 位成员，中国是成员国之一。在 2015 年，GGE 的报告提交给联合国大会并获得批准，并在 2016 年以联合国大会决议方式正式提出，倡议各个成员国，恰当地利用 ICT 技术。其中成果包括：其一，建立相应的国际法，特别是充分利用和尊重《联合国宪章》规范有关行为；其二，重塑人们的信心，增强透明度，恰当利用 ICT，并且纠正以往的误解、冲突，特别是国家在滥用 ICT 过程中产生的冲突；第三，能力建设。不同的国家可能需要不同国家程度的建设，例如，在基础设施方面；其四，国家行为达成约束性的自愿性的行为准则，例如，有关数据的分享，有关基础设施建设及保护工作等；其五，就是如何在整个供应链上完成目标，保障网络安全。[32]

为应对 OEWG 多方主义倾向（闭会期间举办多利益攸关方的磋商会议），GGE 也尝试跟行业、非政府组织和学术界举行闭门会议，进一步协商，而且会请来自相关机构的代表参与。此外，针对 OEWG 主导国俄罗斯对 GGE“小圈子”的抨击，GGE 也尝试与所有联合国成员国进行非正式的协商。此外，政府专家组的成员和非盟、欧盟、美洲国家组织、欧洲安全与合作组织、东南亚国家联盟区域论坛等有关区域组织合作，也会有磋商。

可见，OEWG 与 GGE 的并行增加制度竞争性，从而倒逼 GGE 向开发透明方向改革。问题在于，GGE 的成员范围限制、闭门会议形式、外交代表主导、授权期限固定是既定的，这与 OEWG 存在本质不同。

2.4 信息社会世界峰会（WSIS）

信息社会世界峰会（WSIS）是联合国的派生物。诚如汉斯·克莱因（Hans Klein）所谓联合国峰会是政策制定者描绘原则性共同愿景，并对人类具有挑战性的问题提出解决方案。[33]峰会的性质，本身就反映出网络治理的困难，以及各国在该等问题上的林总分歧。1998 年，国际电信联盟（ITU）全权代表会议决定召开 WSIS。其后受联合国教科文组织的推动，于 2001 年的联合国大会批准提议，并指定 ITU

为 WSIS 的领导机构。

峰会分为日内瓦与突尼斯两个阶段。WSIS 起初并未料到“互联网治理”是优先考虑议程，但是与会国围绕 ICANN 的“关键互联网资源”（CIR）[34]产生重大争议。例如，ICANN 的首席执行官保罗·图梅（Paul Twomey）因并非政府代表而被驱逐出 WSIS 筹备委员会。再例如，一些发展中国家受 ITU 支持，一方面挑战美国单边主义对 ICANN 的影响力，另一方面反对如 ICANN 的非政府政策制定机制。关于 ICANN 的公共政策议题化，莱斯格不赞同，认为 ICANN 仅尝试提供范围最狭窄的技术功能，WSIS 各国对 ICANN 抨击并无必要。[35]但是，穆勒不认同莱斯格，认为 ICANN 动了主权国家治理的“奶酪”，改变主权“划疆为治”的政府与国民关系，这也正是与会国抨击 ICANN 的原因。[36]

可见，WSIS 内部存在两种声音：一是以主权国家为中心达成国际公法条约；二是跨国的非国家行为者达成私法契约，并依靠美国单边主义保障实施。前者受发展中国家青睐，并获得政府间国际组织 ITU 的支持。后者则受美国支持。这似乎展现出发展中国家“合纵以制”美国的倾向。

但是，从成果评估来看，WSIS 的实际影响不大，原因在于峰会没有通过有约束力的国家公法，峰会也没有争取到各国的经费支持。就成果文件而言，按照日内瓦阶段与突尼斯阶段，有二：

其一，《日内瓦原则宣言》采“技术”与“公共政策”二分，若网络治理涉及公共政策，则主权国家应当参与其中制定“政治监管”。对二分法，美国是比较纠结的。一方面，美国也强调 ICANN 的技术性，从而与公共政策区分开，以图避免他国对 ICANN 的干预。另一方面，美国自身又是通过“三合同”来对 ICANN 进行政治监管。问题在于，既然美国政府可对 ICANN 政治监管，那么考虑到整个全球互联网的公共政策，其他国家为什么不能参与 ICANN 的政治监管？这反映出美国单边主义监管 ICANN 的“二律背反”。

其二，《信息社会突尼斯议程》有三点内容：一是认可美国的主张，即认可现有的互联网治理安排——私营部门在互联网的日常运营和前沿创新与价值创造中扮演主要的角色，但未提及 ICANN。可见，美国通过“私营部门”议题，避免 ICANN 议题从而争取与欧盟“连横”；二是认可“多边主义”的主张，即各国无需通过 ICANN 就可管理其国家顶级域名，各国对 DNS 根区与公共政策的监管是“平

等的地位和责任”。同时还号召制定“公共政策议题原则”，“强化合作关系”。如本文 3.2 所述，这是欧盟立场的体现。可见，支持“多边主义”的国家通过“公共政策”议题与欧盟“合纵”，同时“摇摆方”欧盟在其中凸显自己的“原则层面讨论公共政策”主张，从而修正传统“多边主义”的立场；三是授权设立互联网治理论坛。可见，《突尼斯议程》是“合纵连横”妥协的产物。

2.5 互联网治理工作组（WGIG）

互联网治理工作组（WGIG）是 WSIS《日内瓦原则宣言》的产物。该宣言明确 WGIG 的任务为明确互联网治理定义，界定治理问题。为此，联合国任命印度外交官尼廷·德赛（Nitin Desai）为 WGIG 主席以及 40 个成员。根据 WGIG 工作报告，互联网治理是多方参与，并不为国家政府所垄断，但是“根据各自的职能”的表述反映 WGIG 对“国家政府排他性负责公共政策议题”的让步。就治理问题而言，WGIG 的界定超越 ICANN 议题，还涉及技术标准，ISP 互联、电信基础设施、言论自由、多语种。从三阶层看，治理问题已从逻辑层泛化到物理层与内容层。

WGIG 展现出反美国单边主义的倾向，认为在互联网国际治理中，没有任何一个政府能够拥有凌驾于其他政府之上的地位。美国政府在 WGIG 中没有代表，而 WGIC 中来自欧洲政府与跨国互联网公司的成员都赞成这种反单边监管的立场。

2.6 信息社会通信权利运动（CRIS）

信息社会通信权利运动（CRIS）涉及“国际公民社会”和“多方参与治理”。约翰·基恩（John Keane）将公民社会定义为“广泛、互连、多层次的非政府空间”，揭示“公民社会”与“空间”概念的互相建构。[37]CRIS 是由 20 世纪 80 年代的跨国行动团体组成的网络组织，包括“麦克布莱德圆桌会议”（MacBride Round Table）、“世界社区无线电广播电台协会”（AMARC）、促进民主通信的“Videazimut”、“促进通信发展协会”（Association for Progressive Communications，APC）以及知识

分子行动者。例如，赛斯·哈姆林克（Cess Hamelink）起草《人民通信宪章》（The People's Communication Charter），肖恩·奥修克鲁（Sean O Siochru）建立"民主与通信合作平台"（Platform for Cooperation on Democratization），由多个学者组成的"21 世纪声音"（Voice 21）发表《21 世纪人民之声全球运动》（A Global Movement for People's Voices in the 21st Century）。[38]

那么，CRIS 与 WSIS 是什么关系？质言之，WSIS 为 CRIS 提供参与平台。早于 WSIS 筹备阶段，ITU 主席穆罕默德·哈比（Mohammed Harbi）表示 ITU 及其本人推动公民社会的全面参与。其后，联合国大会决议授权 WSIS 来鼓励"NGO、公民社会和私营部门积极参与峰会"。为此，WSIS 执行秘书处下设公民社会部门。WSIS 提供平台，好比"华山论剑"，将各门各派互无交集的 CRIS 团体汇聚到一起，并将关心的 CRIS 问题发轫于 WSIS 议题中。这有五个议题：

其一，信息与通信技术促进发展（ICT4D）。其关注产业界与国家资助项目潜力，主要参与者来自发展中国家；

其二，公民自由与人权。其把人权原则具体应用到通信技术上，涉及内容审查、隐私等；

其三，ICANN 与互联网治理。参与者主要是与 ICANN 有关的私营利益相关方。例如，"因特网协会"（Internet Society）、地区互联网地址注册中心（RIARs）、"非商业用户选区组织"（NCUC）、"一般会员咨询委员会"（ALAC）；

其四，知识无界运动（A2K）。其关注穆勒所谓"IP 与 IP 冲突"，即互联网（IP 特征）与知识产权（IP，Intellectual Property）的冲突[39]；

其五，媒体活跃分子。其关注在网络建立另类媒体以及相应管理政策。

既然 CRIS 组织林林总总，偏好各有不同，那么它们是如何互动的呢？西德尼·塔罗（Sidney Tarrow）与托马斯·瑞斯（Thomas Risse）注意到国际治理与国际组织的共生关系，把后者比作"珊瑚礁"。[40]穆勒进行图示化研究，指出 WSIS 在成员人际关系上"促进通信发展协会"（APC）发挥公民社会网络核心的作用。[41]当然，CRIS 当然地抗拒政府化的科层制。例如，前述 WSIS 执行秘书处下设公民社会部门，在议程组织上采用"家族"分类，家族的"代表"也被"焦点"称谓所代替。"家庭焦点"模式与传统分组议事的区别在于，"焦点"的组织极其随意，没有固定的加入或退出机制，好比"广场上的尽兴表演，感兴趣者欢迎围观"。

这就展示出 WSIS 中政府代表议事与 CRIS 议事的差异，而差异导致多方对话的鸿沟。ITU 面临着尴尬，因为当初是 ITU 邀请 CRIS 团体参与 WSIS 的，但是 CRIS 在参与过程中极力抗拒 ITU 的管理。因此，WSIS 未能实现其本初目标，即促进国家政府与 CRIS 之间的对话。始料未及地是，WSIS 促进 CRIS 内部的对话。

2.7 互联网治理小组（IGC）

WSIS 激发 CRIS 对 ICANN 与互联网治理的讨论，从而催生互联网治理小组（IGC）。作为跨国行动组织，IGC 的发起人有代表顶级域名与多语域名的利益，也有作为传播学专家在 ICANN 中有会员身份。IGC 旨在 WSIS 中扩大 ICANN 议题的讨论。

值得注意的是，IGC 对 ICANN 没有固定的立场，其成员有 ICANN 的支持者，也有 ICANN 的批评者。IGC 更像是一个“技术中立性”的论坛，为 ICANN 的利益相关方提供讨论平台。这揭示出类似于 IGC 的 CRIS 团体的复杂性，因为其网络化而非科层化，因此并没有一个中心化的立场倾向。从“实体”与“程序”二分看，如 IGC 的 CRIS 更多地发挥程序的功能。

2.8 互联网治理论坛（IGF）

基于 WSIS《突尼斯议程》，联合国成立互联网治理论坛（IGF）。IGF 没有解决而是进一步激起 WSIS 的争议，两极化的倾向更明显，可二分为“鹰派”与“鸽派”。[42]

就“鹰派”而言，巴西主张将 IGF 发展为政府间框架协议，建立全球适用的公共政策原则。俄罗斯则主张将 IGF 发展为传统政府间组织，从而国家政府可通过 IGF“自上而下”科层治理。与政府相比，CRIS 的鹰派则强调“自下而上”的民主选举代表程序，将 IGF 制度化。这与欧盟、澳大利亚主张“不限于 IGF 平台的合作”（美国默许）立场相矛盾。

就“鸽派”而言，西方发达国家、跨国企业、ICANN 倾向将 IGF 视作单纯的年

度会议，反对常规的制度化。ITU 等政府间国际组织也反对 IGF 制度化，因为 IGF 的建制会与 ITU 争取互联网治理领域的目标相竞争。在发展上，出现“新鸽派”，ICANN 对 IGF 改观，转向利用 IGF 来推广自己的政策议题和管理结构。相似地是 Nominet UK, 其作为域名注册公司运营“.uk”国家代码顶级域名，资助支持 IGF 举办国家层级的论坛，这似乎是“engagement”的思路。但是，“鸽派”仍非铁板一块。在 ICANN 监管议题上，美国与欧盟仍在 IGF 中延续 WSIS 中的根本分歧。

那么“鹰派”与“鸽派”发生什么冲突呢？有三个方面：其一，议程设置。在 IGF 的官方立场上争论不休。例如，IGF 第一届年会议程倾向于“鸽派”，围绕开放性的审查制度与言论自由展开；其二，代表权。IGF 的互动核心是“多方顾问小组”（MAG），但对谁可代表参与 MAG 存在争议；其三，原则争执。这反映上述两派及派系内部的根本分歧。

穆勒对 IGF 是悲观的，其认为多方参与模式仅能达成形式上的规范与协议，即使达成也是“一纸空文”难以具体实施，因为政府代表之间以及政府代表与 CRIS 之间的利益不可调和。这就像拉多斯拉夫·季米特洛夫（Radoslav Dimitrov）对联合国深林论坛“环境多边主义规范”的批判[43]，国家政府默契地通过“空洞”的论坛来吸收“多方利益相关主义”（尤其是来自 CRIS）的压力。[44]

因为根本矛盾难以弥合，IGF 面临“退群”风险。例如，“鸽派”澳大利亚国家代码注册机构以退出威胁 IGF 放弃总结性的制度提议。ITU 秘书长演讲认为 IGF 是“浪费时间”。中国则宣布投票反对 IGF 存在，因为 IGF 对 WSIS 的遗留问题并没有直接解决的办法。那么退群有什么影响呢？IGF 是利益相关多方参与的范式，有网络特点。从网络效应看，“退群”会产生负反馈，“千里之堤，溃于蚁穴”。可见，IGF 是形式化的多方参与，其因难以弥合多方根本分歧而容易失败，也因缺乏规制“退群”的范式而导致议题受异议者拉张牵连，导致“离题千里”。

2.9 国际互联网协会（ISOC）

国际互联网协会（ISOC）整合互联网技术社群，如互联网工程任务组（IETF）。ISOC 并非科层制的结构，而更像一个松散的有机结合体，其互联网技术社群成员跨越 NGO 与私营企业，并在行动上声称其为“跨国立场”，诚如 ISOC 对外宗

旨是“为全人类服务”。因为成员的重叠关系，ISOC 与 ICANN 存在诸多互动，并共同以技术标准的影响力控制“关键互联网资源”，因此 ISOC 的立场实质上是倾向 ICANN 的，或者更具体地讲，倾向于美国的立场。

对 ISOC 支持于否，展现出前述的两种主义张力，即“多边主义”与“多方主义”之争。前者强调国际政府主体，自当反对 ISOC 等非政府行为体的主导，并对现状进行抨击。后者强调多方利益者参与，则支持 ISOC 的治理现状。而 ISOC 的治理方式也与“多边主义”对国际公法的依赖存有很大不同，因为 ISOC 更偏向标准、协议、组织、流程以及指导原则的治理。

2.10 跨国互联网企业（MIEs）

随着互联网全球化发展，出现有跨国经营业务的互联网企业（Multinational Internet Enterprises, MIEs）。例如，美国的“GAFA”与中国的“BAT”[45]，虽然设立于中美两国，但服务的网络用户位于全球各国。作为 ICP，MIE 在内容层上建构出国际“用户网络”。因此，这就涉及到国际法律合规的问题，即“入乡随俗”，遵守业务所在地的法律。问题在于，网络治理场景下围绕主权国家边界所搭建的国际法面临“失范危机”，从而让 MIEs 无所适从，更不得不直面美国单边主义。

例如“微软案”中，美国微软公司收到美国政府的搜查令，要求搜查微软公司的非美国公民用户存储在爱尔兰服务器的电子邮件，并要求微软公司不得向该用户披露搜查的情况。基于传统国际法的管辖权原理，微软公司主张美国政府应适用与爱尔兰的双边协议《司法互助协议》（MLAT）[46]来搜查，而不能单边主义地陉行要求微软公司配合搜查。为此，微软公司在美国法院起诉美国政府，争议点在于美国政府根据《SCA 法案》[47]是否可对存储在爱尔兰服务器的内容进行搜查。初审法院认为可以，因为美国政府的的域外搜查行为是传票（subpoenas）而非搜查令（warrant），所以可域外适用。上诉法院认为不可以，搜查令违反美国法律的域外适用推定。[48]最高法院决定提审，并开庭审理。但是，因为微软公司与美国司法部调解，而撤案终结。[49]

调解的结果是什么呢？那就是国会通过《澄清域外合法使用数据法》（CLOUD 法案）。这是互联网企业与美国政府妥协的产物。[50]一方面，法案明确搜查令可域外适用。另一方面，法案允许互联网企业可以将外国法规定义务作为

抗辩执行美国搜查令的理由。例如，微软公司可以爱尔兰法律禁止美国搜查令调查为由抗辩，向法院申请拒绝执行美国搜查令。

“微软案”反映出美国 MIEs 与美国单边主义的分歧。从《CLOUD 法案》的“抗辩理由”条款可以看出，基于国家主权建构的“多边主义”更受 MIEs 青睐。因为 MIEs 可在“主权斗争”中获得义务的解脱。这似乎可解释为何“谷歌不再坚持将服务器搬到公海”，因为积极管辖冲突而非消极管辖冲突才能使 MIEs 合规。ICP 网络越发重要，吸引国家的关切（尤其是涉及国家安全），公海上之物不是“国家都不来管”，而是“国家都来管”。恰如公海上的鲜美血肉吸引万千鲨鱼虎视眈眈。可行的选择，是 MIEs 通过一国的主权庇护，来遮蔽他国主权单边主义的主张。这不仅是被动，还是主动的考虑。例如，微软公司将服务器设立于爱尔兰，其中原因在于爱尔兰政府对数字经济、隐私保护上的强有力支持政策，从而吸引 MIEs 营商。而基于云服务技术，跨国搭建服务器来提供跨国服务是可行的。

此外，随着用户的网络效应指数叠加，“马太效应”下 MIEs 运营的平台可能被国家视为关键基础设施，并要求其承担公共义务。这不限于美国政府的视野，其他国家政府亦是如此。例如，中国《网络安全法》明确“关键基础设施”的界定标准。为此，MIEs 在“多方利益相关主义”下，积极参与多方治理。例如，MIEs 参与《巴黎倡议》[51]与《基督城行动协议》[52]的“消除网络恐怖主义和暴力极端主义”。这反映出 MIEs 以行动打破政府监管的担忧，另一方面展现出 MIEs 参与对传统上“恐怖主义”国际治理限于政府多边主义的变革。

然而，这涉及到“群己权界”（严复译密尔《论自由》语）与“公私权界”。例如，2021 年 1 月 8 日，美国互联网公司“推特”（Twitter）永久暂停美国总统特朗普使用的推特账号“@realDonaldTrump”，理由在于该账户所发布消息违反了《推特规则》（Twitter Rules）、《公共利益架构》（public interest framework）、《反宣扬暴力政策》（Glorification of Violence policy）。对比此前案例——美国法院裁判特朗普推特账号无权随意拉黑其他推特用户账户，这反映出互联网平台不能简单地用传统“公私权界”的二元范式解释。原因在于，公职人员的私人社交账号，具有公私复合性。此外，德国总理默克尔表态，认为推特关闭特朗普账户存在问题。该表态获得俄罗斯媒体与中国媒体转发。可见，国际社会对该议题的关注。这引申出 MIEs 治理的一些问题：

其一，MIEs 行使审查公权力的合法性何在？对于公主体用户而言，MIEs 是否可基于“契约自由”像管理私人用户一样规制？公主体用户是否可以公共利益确保公民知情权、言论市场自由竞争抗辩 MIEs 管理？对于私主体用户而言，其是否可以“言论自由”抗辩 MIEs 的管理，尤其是当 MIEs 已具有基础平台的公共性时，该等抗辩是否成立？

其二，MIEs 是否有能力界定规制标准？尤其是，当 MIEs 服务用户来自于不同主权国家、不同意思形态、不同文化观念，是否能在同一平台找到一个标准尺度？假如同一平台对于不同群体的标准尺度不同，是否会造成数字鸿沟与不平等？

其三，MIEs 是否应当接受公权规制？当 MIEs 发挥公权力作用时，相对应地，是否应当接受公权规制，尤其是传统法律范式对公权力的规范，例如“比例原则”等？这种监管力度加强，是否会影响 MIEs 的企业发展，以及整体上的数字经济发展？

就问题一，美国《通讯规范法》第 230 节提供一个参考，那就是基于“好撒玛利亚人”原则，原则上互联网平台免于承担因用户发布内容导致的法律责任，但触犯刑法、知识产权法、通信隐私、性交易等除外。此外，互联网平台有权使用任何技术手段限制前述用户内容，即使前述内容受宪法保护。这被誉为美国互联网企业的法律“基石”，一方面免除责任，另一方面赋予规制权利。例如，Twitter 暂停特朗普账户，可能援引的法理就在于第 230 节。

比较有趣地是，特朗普总统与美国互联网企业早因第 230 节而“扛上”。2020 年 5 月 28 日，特朗普行政当局就发布《阻止在线审查报告》，指出“在线平台正在从事选择性审查制度，这正在损害我们的民族言论。除其他令人不安的行为外，成千上万的美国人报告说，在线平台“标记”内容为不当行为，即使它没有违反任何规定的服务条款；对公司政策进行未经事先通知和无法解释的更改，从而不利于某些观点；并删除内容和整个帐户，而不会发出警告，没有理由也没有追索权……所有执行部门和机构应确保其适用第 230（c）节正确地反映了本节的狭义目的，并在这方面采取了所有适当的措施。此外，在此命令发出之日起 60 天内，商务部长（秘书）应与美国总检察长协商，并通过美国国家电信和信息管理局（NTIA）采取行动，向联邦政府提出制定规则的请愿书。通讯委员会（FCC）要求 FCC 迅速提出法规以澄清……”[53]

可见，特朗普反对互联网平台“滥用”规制权利。此外，斯时的美国候任总统拜登也对第 230 节表态，但着眼点于特朗普不同，关注在互联网平台是否“滥用”免除责任。

就问题二、三，在“哥伦比亚大学诉特朗普案”中，美国联邦第三巡回法院认为“总统将@realDonaldTrump Twitter 帐户用作其官方通讯的主要工具。他利用这个帐户对各种主题发表了正式的声明，其中许多主题在全国都具有重要意义。公众反过来可以在 Twitter 上回应总统和其他用户并与之互动.....我们认为这种对话创建了一个公共论坛.....当总统创建这样一个公共论坛时，他将他人排除在对话之外，因为他们表达了总统不同意的观点，因此违反了宪法第一修正案。”[54]可见，这是对国家行为和公共论坛理论的直接适用。换言之，@realDonaldTrump 有公权性质。在该案中，三巡法院援引最高法判例进行论证。

该最高法判例是什么呢？在“Packingham 诉北卡罗来纳州案”中，美国联邦最高法院讨论了 Twitter 与第一修正案的关系，肯尼迪大法官认为：“社交媒体用户利用这些网站从事涉及人类思想等主题的各种活动，应受第一修正案保护。”[55]此外，就“公共论坛”原则，最高法在“福布斯电视台案”中认为，“公众论坛原则首先是在街道和公园的背景下出现的，警告不要将其‘机械’地扩展到电视广播”。[56]“可见，“福布斯电视台案”确定了电视广播不具有公园和街道的两个特征：“开放访问”和“观点中立”。法院认为，由于电视频道创建并发布了自己的内容，因此“不仅允许，而且确实要求电视频道在选择和播放节目时行使实质性的编辑自由裁量权”。

美国联邦第三巡回法院拾起“福布斯电视台案”先例，继而认为“Twitter 具有最高法在‘福布斯案’中确定的两个关键属性，而公共广播缺乏这些属性。首先，Twitter 向公众开放。Twitter 开设帐户的唯一限制是基于年龄的：13 岁以下的人可能不使用其服务。其次，Twitter 在观点方面是中立的；它是用户发布其意见的平台。”因此，三巡法院认为@realDonaldTrump 构成公共论坛。

当然，三巡合议并非一致，存在法官异议。Michael H. Park 等法官认为，“当公职人员使用个人社交媒体帐户表达意见时，他们不会参与“国家行为”。第一修正案对言论自由的保证，不包括在他人的个人社交媒体帐户上发帖的权利，即使这些人碰巧是政府官员……该决定背离了我们的先例，将第一修正案的范围扩大

到涵盖政府官员的个人社交媒体活动，因此值得司法审查。”“由于 Twitter 是私人拥有和控制的，因此公职人员对其功能的使用不会涉及国家权力的行使。Twitter 公司（不是特朗普总统或美国）控制着该平台，并监管每个人的使用。在‘阻止’原告方面，总统使用了推特功能，其他所有用户都可以使用该推特功能，因此，他的行为不能‘公平地归因于国家’。因此，当总统阻止用户使用其个人帐户时，他不是国家行为者。他可以在上任之前阻止该用户访问该帐户，也可以在离开白宫后继续这样做。在阻止用户使用时，他‘没有行使任何法律赋予的特别权力’，“仅由于他穿着法律的权威，他的行为也才使之成为可能。”

综上，跨国互联网企业（MIEs）激荡起与传统主权治理冲突矛盾的火花。尤其是现代互联网场景中，互联网社交媒体账户成为人的“第二身份”，因此如何界定“第二身份”的公私属性，以及其与本人身份在现实世界的关系，成为治理关键。这延伸出互联网平台是否享有豁免权以及规制权利，以及相应地如何从私法遁入公法，接受治理监督的问题。

3. 用什么治理

3.1 知识产权规范

两个“IP”有关联。那么知识产权（Intellectual Property, IP）与互联网（其核心技术 IP）在规范上是否可以相互镶嵌。 2005 年，互联网治理工作组（WGIG）将“知识产权”列入 13 个“与互联网治理相关的公共政策议题”中的第 9 个，但继而表示“其影响不限于互联网，现有的组织机构应对此负责”。“现有组织”的说法在于维护知识产权国际治理的既定利益者（如 WIPO 与 WTO）与优势地位国家（如美国），避免归入“互联网治理”而受“多方利益相关主义”的颠覆。因此，知识产权议题往往有意地区别于网络议题。但在现实中，ISP 面临着是否承担知识产权侵权责任的问题，以及“知识无界”运动与 CRIS 合流从而冲击知识产权范式。

网络中的知识产权保护

从历史看，如前文所述，美国互联网兴起来源于电信自由化。而美国在推动全球电信自由化时，遇到 ITU 代表传统电信利益集团的阻碍。美国的方法，是将议程权力由

ITU 转移到美国主导建构的 WTO，使用“服务贸易”概念来支持国际电信市场，促进电信领域竞争。同时，美国也将知识产权议程与 WTO 捆绑起来，并通过《与贸易有关的知识产权协定》（TRIPS）实现，从而像对付 ITU 一样颠覆 WIPO 的传统职责。可见，美国主导 WTO，将网络议题与知识产权议题归于同一自由贸易机制中。但是，两者在实然上存在冲突，互联网场景下的知识产权面临“失范”风险。例如，数字化版权作品的拥有者怎样使用才算“合理使用”，才算“版权权利用尽”。互联网降低数字作品的复制成本，媒介与作品内容不再泾渭分明。此外，“数字爆棚”下互联网用户制造大量内容（UGC），该内容一旦侵犯知识产权，则牵连到 ICP 与 ISP 是否要承担侵权责任，以及如何承担的问题。

为此，美国于 1998 年通过《数字千年著作权法》（DMCA），其“反规避条款”产生域外效力。这展现出规范的域外倾向，通过单边主义迫使他国提升网络治理中知识产权的保护能力。美国商务部与 WIPO 联合，将“知识产权保护”确立为网络治理的优先议题。其背后动机，在于美国大量的知识产权需要在他国的网络治理中获得充分保护。例如，P2P 技术给传统版权保护带来危机，而技术开发者与参与者遍布全球。为此，美国 2004 年《诱使著作权侵权行为法》也加强技术开发者的责任。

此外，商标问题与 ICANN 勾连在一起。这展现出内容层与逻辑层的联系。ICANN 建立《统一域名争议解决政策》（UDPR），为商标权人在诉讼制度外提供快捷廉价的域名异议程序，并强制要求每个顶级域名、次级域名注册机构遵守 UDPR。尽管 ICANN 直接权力仅限于“通用顶级域名”（.com 等），但 UDPR 的范式已为各国与地区域名注册机构所效仿。作为交换，ICANN 将“地理名称”和“特定种类的国家级以下的地点名称”的资源分配权授予各国政府，这展现出网络空间的“先占”国际公法规制由 ICANN 加以贯彻。

这反映出公共政策（注册商标的强政策性）的私营化解决路径。好处在于，程序统一有利于规避各方（尤其是主权国家）的实体分歧，从而降低制度成本。风险在于，公共政策的私营化缺乏正当程序的保障，而这种政策性议题在传统内国法治理中受到宪法与法律的“限制公权”规制，在传统国际公法中也受到各国立法机构批准或转化的“二次检验”。除了 UDPR，Whois 服务也是一种回应。Whois 服务可甄别 DNS 注册者的姓名、联系方式，从而有利于知识产权人对前者主张

责任。

这衍生出一个问题，就是如果网络治理的知识产权保护私营化的话，那么这些非政府主体应履行何种监管义务，承担何种法律责任？波义耳（Boyle）提出“先发制人”利用技术与市场进行监管，而非交易事后进行监管。[57]这与莱斯格提出的“多元规制”相切合[58]。美国电影协会则呼吁 ISP 采用过滤技术或深度数据包检测技术（DPI）来检查版权侵权行为。在 P2P 问题上，版权人（如美国电影协会代表的利益）与 ISP 存有共同的反对立场，就前者是版权问题，就后者是 P2P 流媒体对 ISP 提供带宽的大量消耗。后者问题引发“网络中立性”（network neutrality），并引发 ISP 与 ICP 的冲突，即 ISP 可否按照 ICP 内容性质分配带宽，是否构成歧视。而 ICP 内部也有分歧，取决于其业务内容，如果偏向 UGC 则对版权侵权更隐忍，如果偏向 PGC、OGC 则更接近版权人一端的零容忍立场。可见，在网络治理场景下，知识产权人、ISP、ICP 各有不同的取向，难以协调成一致的监管义务与法律责任。而利用网络技术的“破坏性创新”就在夹缝中生存壮大。

进一步而言，DPI 模糊了逻辑层与内容层的界限。诚如 ISP 与 ICP 本身对应于逻辑层与内容层的二分。但假如要求 ISP 实施 DPI 来打开数据包检测内容，那就改变了 ISP 过去仅仅运送数据包的逻辑层身份。

综上，知识产权范式与网络治理的镶嵌关键，在于 ISP、ICP 对知识产权保护的监管义务。例如，美国特朗普政府在与加拿大，墨西哥和日本的贸易协定中，强迫纳入《通信规范法》第 230 节，这是一项有争议的法律，保护互联网公司免于对其平台上发布的第三方内容承担责任。白宫称与这些国家的交易为“数字贸易规则的黄金标准”。但是众议院能源和商业委员会的民主党和共和党领导人均不同意，说“美国不适合出口反映第 230 条的语言”。该法律是美国激烈政策辩论的主题。[59]

“知识无界”运动(A2K)与CRIS 的合流

“知识无界”运动（Access to Knowledge, A2K）滥觞于开源软件的实践，其反对数字版权管理（DRM）、软件专利、传统媒体垄断，支持 P2P、网络中立性。A2K 分为三阶段：一是免费/开源软件运动（F/OSS）；二是反美国 DMCA；三是围绕药品专利导致药价高企而对

TRIPS 挑战。

在意识形态上，A2K 展现出与 CRIS 相似的面相，并捡起政治经济学作为斗争武器。CRIS 是 A2K 的先驱，A2K 不能限于知识产权议题，还要涉及信息基础设施、政府等多个方向。这在特定国家发生了政治关联。例如，瑞典的“海盗党”诉求通过“海盗湾”给 P2P 提供庇护，并参与欧洲议会选举。

此外，A2K 将版权制度异化，“为我所用”。其通过开放通用公共许可证（GPC），以版权法的“许可”范式来规范被许可人行为及软件迭代保持在“非独占”的公共道路上。

3.2 安全规范

“安全”是国际政治新现实主义的核心词，对应于传统现实主义的“实力”。网络治理的议题越来越关注“安全化”。原因在于，网络场景的安全问题有其特殊性。例如，传统执法手段不足以打击网络犯罪，因为网络犯罪与传统犯罪相比，其规模有外溢可能、范围有跨国可能、行为有分散可能。然而从技术中立性角度来看，难以将这种特殊性归咎于网络本身。相反，这种特殊问题更像是人性犯罪问题在网络空间的延伸。

与传统政府多边治理不同的是，网络的安全治理展现出多方主义的倾向，尤其是 ISP 在其中发挥关键作用。例如，北美网络运营商集团（NANOG）联合规制垃圾邮件黑名单。而国家政府倾向于通过 ISP 进行合作。原因在于，ISP 对服务器、带宽、域名进行直接管控，与国家监管方相比，更能快速地地对安全风险进行反映。例如，“伦敦行动计划”（LAP）中，各国执法机构松散地合作并界定安全问题，通过国际条约加以明确，但是日常的鉴别、拦截、应变工作则是由 ISP 组成的跨国网络完成。可见“公私合作”下的政府监管处于隐秘的地位。但这并不代表国家政府对监管的放弃，因为国家安全正是政府关注的焦点。例如，美国的“无授权窃听方案”（warrantless wiretap program），授权国家安全局（NSA）与 ISP 合谋对互联网通信进行监听，并免除 ISP 侵害用户隐私的法律责任。再例如，欧盟委员会于 2006 年通过数据保留动议，要求 ISP 保留用户活动信息并将该数据对欧盟的执法机构开放。　引而言之，政府的监管存在冲突。例如，美国政府向位于欧洲布鲁塞尔的金融电文交换机构“环球银行金融电信协会”（SWIFT）发出

传票，要求 SWIFT 提供金融数据及民航航班乘客数据。美国政府的单边行为违反欧盟的个人数据保护政策。除了政府外，ICANN 推动的 Whois 服务也与欧盟的个人数据保护政策相冲突。值得玩味的是，国家政府内部司法机关与执法机关间对 Whois 的态度也是微妙的。这反映国际治理对国内政治的牵连。例如，澳大利亚法院判决拒绝给予执法机关在".au"域名内任意获取 Whois 数据的权利，但是澳大利亚在 ICANN 的政府代表仍支持"开放获取"的原则。实质上，Whois 服务反映网络治理的"身份证问题"——谁有权发"身份证"，谁有权检查"身份证"，谁有权驱逐"无证之人"。这里的权力是如此之大，虽然现行留存于 ICANN 的技术职能下，但"问鼎天下"，引起国家政府的利益关心与安全担忧。

这揭示的问题，在于莱斯格所谓的市场、规范、架构可否代替国家法律或国际公法？这反映出国家与互联网安全的关系。国家政府并非没有努力。例如，欧洲委员会主导的《网络犯罪公约》（the Convention on Cybercrime）要求各国执法机构设立一个"联络点"，承诺每周 7 天，24 小时工作，从而确保快速提供帮助与协作。此外，国际刑警组织也运营类似的"国家中央参照点"（National Central Reference Points）的网络。可见，当国家政府尝试采取网络化治理，并仿照 ISP 建立 24 小时应急架构的时候，那么形式上法律吸收架构，但在实际上架构代替法律存在。换言之，这反映传统规范（国家法律、国际公法）与市场、规范、架构的双向适应。运用安全规范治理网络，那么"网络空间"的真空必将引起国家安全的担忧。"以其人之道，还治其人之身"网络化治理，是填补真空、治理网络的可行之道。

此外，网络攻击也在挑战网络安全。最新一轮与冠状病毒相关的网络攻击可能会为编纂网络规范的运动提供新动力。其中一项举措，即"网络安全技术协议"，是微软和诺基亚等全球技术公司之间的一项共同努力，旨在就抵御网络威胁的方式进行合作。该协议的发言人在一封电子邮件中说：" COVID-19 证明了就网络空间中负责任的行为的规则和期望达成国际共识的重要性。"[60]

3.3 内容规范

英国互联网观察基金会 (IWF) 的内容规制

内容层治理是极强公共政策性的命题，其与各国的政策取向、公共利益相关联。西方国家面临内容治理的困境。这不仅因为内容的困境，还在于方法的困境。举“儿童色情内容”为例，各国对其执法入罪化已达成较大共识，但在方法论上仍存在困境。例如，英国互联网观察基金会（IWF）参与网络“儿童色情内容”的规制，其创始任务有二：一是提供非法内容的举报热线；二是开发帮助用户管制互联网内容获取权的评级系统。评级系统受万维网联盟（W3C）支持，诚如 W3C 开发自己的“网络内容筛选平台”（PICS）。这种共识制度化为互联网内容评级协会（the Internet Content Rating Association），原理与电影评级类似。问题在于，“数据爆发”时代，大量内容涌现，上述评级制度难以应对，资源付出成本过高。

为此，IWF 改变策略，“发动群众”利用热线举报来“通知并取缔”潜在违法的内容。与此类似，IWF 的模式在各国推广，如美国国家失踪与受虐儿童虐待中心（NCMEC）也开通“网络匿名举报热线”。这为国际化提供可能。各国负责的举报热线围绕国际互联网检举热线联盟（Inhope）组织起来，美国 NCMEC 也将业务国际化为“全球失踪于受虐儿童援助中心”（ICMEC）。这种国际化带来功能的变化，即 IWF 组织不再满足于在其国内（如英国）取缔国内违法内容，还旨于阻止国内用户对国外违法内容的访问。例如，IWF 为了“阻止访问”，实施“洁净网络”（Cleanfeed），汇集一个禁止访问网站的列表，并将其发给各 ISP 与国内执法机构，同时发给 Inhope。通过 Inhope，加拿大的举报热线“Cybertip.ca”可能会将 Cleanfeed 的列表列入其“阻止访问”列表，从而产生“一处受限，处处受限”的效果。值得说明的是，ISP 为免除自身的内容审查责任，偏向对收到的“阻止访问”列表自动执行。

可见，半官方机构（IWF）与私营机构（ISP）联合，在政府之外建立起内容审查与规制知情的机制。实质上，这种拦截内容可能不限于“儿童色情内容”。例如，欧洲和加拿大的热线还将“攻击性言论”加入拦截列表。这反映出的问题，在

于：其一，缺乏正当程序的救济机制。被拦截的网站主体难以申诉与陈述意见，尤其在跨国“阻止访问”场景上面临困境；其二，网络效应缺少安全阀规制。一国热线的错误拦截操作可能因为 ISP 的自动执行机制而产生网络效应的广泛影响，并通过国际 Inhope 共享网络而泛化。例如，IWF 因“维基百科蝎子乐队专辑封面”过度拦截，影响到网络用户对维基百科的正常使用；其三，难以界定法律责任。半官方机构与私营机构的日常配合混淆了彼此的法律责任，隐身在后的国家政府监管又难以被施于国际公法上的国家责任。

ICANN 的内容规制

ICANN 强调其在逻辑层的技术性。但在 DNS 问题上，逻辑层的技术性与内容层的政策性相联系。自 2006 年起，ICANN 制定常规性扩产顶级域名（TLDs）的政策与程序。问题在于“有些 TLD 不应被使用”。那么，禁止的标准是什么呢？ICANN 在国际公法中寻求答案，参考国际公法对商标的规范，强调 TLD“必须不违背普遍接受的涉及道德与公共秩序的法律规范。这些规范依据国际法律准则认定”，因此禁止“暴力非法行为”“歧视行为”“儿童色情行为”有关的顶级域名注册。可见，当 ICANN 脱离逻辑层技术性，而参与内容层治理的时候，不得不在国际法的渊源中寻求治理正当性。这也离不开政府咨询委员会（GAC）的推动。2007 年，GAC 制定了正式的“建议”，要求授予新名称时应尊重具有“国家，文化，地理和宗教意义”的单词周围的“敏感性”。 GAC 原则的早期版本甚至授权单个政府以任何理由否决任何它认为令人反感的拟议 TLD。

既然 ICANN 与美国关系微妙，那么美国对 ICANN 的 DNS 管制采取的是什么立场？这与前述 ICANN 与美国政府的“XXX 事件”关联，那就是美国政府不可避免受国内政治影响而对 ICANN 施加影响，从而并不支持“XXX”作为成人网站的顶级域名。但另一方面，应当考虑到受美国宪法第一修正案保障的“言论自由”与第十四修正案的“正当程序”。 ICANN 的 DNS 管制，以私营机构身份进行治理，实质上规避了“言论自由”与“正当程序”对公共权力的规制。首先，不得不承认，ICANN 虽以私营机构存在，但其在实质上发挥着公共权力，尤其当 ICANN 介入 DNS 内容管制议题时更是如此。其次，如果将 ICANN 所谓“暴力非法行为”“歧视行为”“儿童色情行为”的禁止领域放在美国司法系统进行“言论自由”的

裁判，那么在具体场景中的 TLD 可能会受法院支持获得“言论自由”庇护，但在 ICANN 程序中不可能如此。此外，如果以国际条约的方式订立，则美国国会可能以“言论自由”为理由而未予通过。再者，ICANN 的机制也显示出当事人在正当程序中的乏力。但是，考虑到美国政府在“XXX 事件”的取向，ICANN 的 DNS 管制可能与美国政府有暗合的默契，从而“绕开固若金汤的马奇诺防线”。这可用来批判美国的“良善霸权”，因为美国政府借用 ICANN 渠道来规避美国宪法对“利维坦”的限制。诚如穆勒指出，在 ICANN 中，GAC 的政府代表可以提供“建议”，而无需正式谈判条约或未得到国家立法机关的批准。[61]

为此，德里克·巴姆鲍尔（Derek Bambauer）提出一种适用于网络治理的审查标准，共有四个方面：其一，审查是否公开，限制的理由是否充分；其二，过滤的内容是否保持透明；其三，过滤的范围有多大，执行的实效有多强；其四，公民是否可参与审查标准的政策咨询。概言之，即公开、透明、精准、民主。穆勒则指出巴姆鲍尔的第四方面实质就是公共政策议题，因此公共政策与技术是难以割裂的，此外巴姆鲍尔是“国家中心主义”的，忽视了网络治理的多方参与。[62]

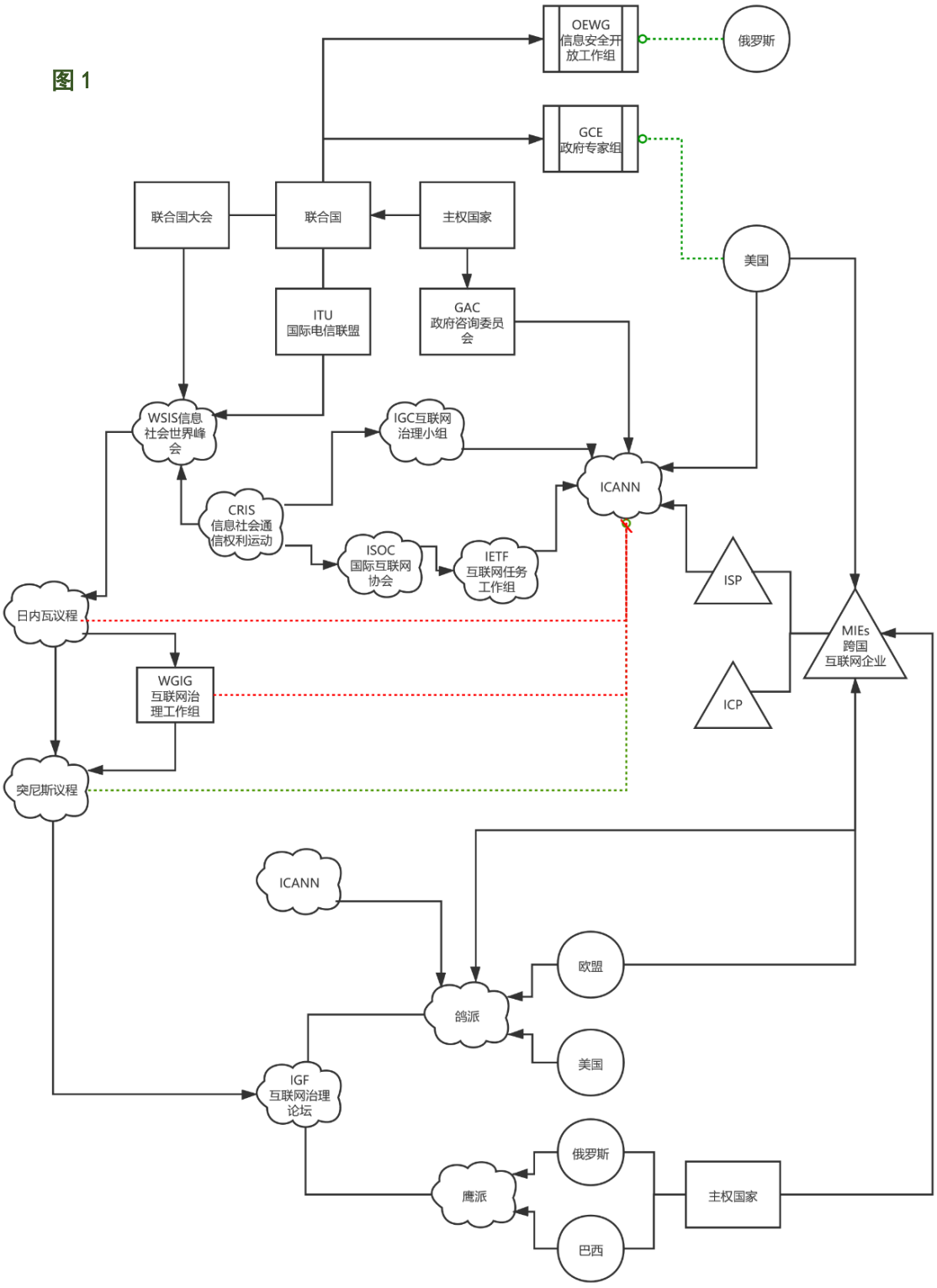
Bradshaw 与 DeNardis 也指出，DNS 管理有时被描述为“文书”或仅是“技术”任务，但它也牵涉到许多公共政策问题，例如商标纠纷，基础设施稳定性和安全性，资源分配以及言论自由。一种并行现象涉及政府和私人力量，出于政治和经济目的，它们越来越多地更改或采用 DNS，这与其将互联网名称解析为数字的核心功能有所不同。[63]

4. 本篇小结

图 1 简要总结了各治理主体间的关系，可见，网络空间的国际治理场景中，“谁用什么治理网络空间”面临着诸多挑战。国际治理可为网络空间中的行为创造“道路规则”，同时为物理层的“关键基础设施”、逻辑层的“关键互联网资源”与内容层的大数据与个人信息提供保护。就“谁来治理”的问题，“网络自由主义”与“网络现实主义”，“多边主义”与“多方主义”存在张力，美国与 ICANN 的微妙关系，欧盟与中国、俄罗斯等国家的“合纵连横”，以及 WSIS 孕育的 WGIG，CRIS 对传统的解构，技术集群组织 ISOC 与跨国互联网企业的治理互动。就“用什么治理”的问题，知识产权、安全与内容的规范视野折射出“是否用旧瓶装新酒的问题”。

[64]总之，网络空间展现出“合纵连横”的意向，“春秋一霸”美国主导 ICANN，欧盟“模棱两可”，其余诸国通过 WSIS 希望改变，在 WGIG、IGF 发酵，通过“联合国”会盟，或以 OEWG 合纵，或以 GGE 连横。除此单边主义、多边主义张力外，多方主义还邀请 CRIS、IGC、ISOC、MIEs 参与网络空间治理。

图 1



第二篇 网络安全

各国在“何为国际网络安全治理的主导理念”这一问题上有较大冲突，因而无法形成统一的国际规则。在国际网络安全的治理问题上，主导理念的差异所应回归的最原始的问题依旧是“主权与人权孰高”的问题，典型体现在 “网络主权”与“网络信息自由”治理理念之争。[65]除不同国家在网络治理方面的主导理

念不同，在网络安全治理的不同层面，同一国家的治理主导理念也不尽相同。

1. 布达佩斯网络犯罪公约

1.1 概况

在涉及网络安全的治理网络犯罪与恐怖主义维度，国际合作是各国政府的普遍选择。但是由于治理理念无法达成一致，传统的政府间国际合作平台——联合国，在治理网络犯罪和网络恐怖主义上并没有做出太多的实质性贡献。网络技术先发国家由于技术发展较为成熟，在制度创设中掌握话语权，在国际舆论引领上也处于主导地位。因此，美欧创制的网络犯罪治理规则即为现行国际通行规则。欧洲委员会 2001 年通过的《布达佩斯网络犯罪公约》（下称《布达佩斯公约》）被美欧视为成熟的国际规则，也被大多数国家认为是“已有网络犯罪治理规范中最完善、最成熟的代表”。[66]

截至 2020 年 9 月，已有 65 个国家签署并批准了《布达佩斯公约》。[67]在未加入该公约的国家中，也有一些国家在本国立法中吸收了公约的相关规定。由于成员国覆盖世界多个区域《布达佩斯公约》也在全球范围形成了一定的辐射效力，其法律框架也深刻影响了世界不同区域打击网络犯罪和网络恐怖主义的规范体系。《布达佩斯公约》的加入条件，规定在公约第 37 条：非欧委会成员国加入公约须由部长委员会征得缔约国的一致同意，然后在部长委员会的投票中获得 2/3 以上多数的支持，并取得列席委员会投票的缔约国代表的一致支持，方可获邀加入公约。[68]

《布达佩斯公约》规定了四类犯罪：侵犯计算机数据和系统可信性、完整性和可用性的犯罪，计算机相关犯罪，与内容相关的犯罪如儿童色情等，与侵犯著

作权及相关权利有关的犯罪。[69]此外，由于参与《布达佩斯公约》谈判的各方未能就种族主义和排外主义言论定罪的通用条款达成一致，该公约中并未规定言论犯罪，而是将有关条款集成到了一个单独的 《附加议定书》之中。[70]从《布达佩斯公约》和附加协定的关系来看，《附加协定》实质上是在《布达佩斯公约》规定的网络犯罪类型之外，增加的一类网络犯罪类型。

此外，在打击网络犯罪的组织构架上，《布达佩斯公约》建构了网络犯罪公约委员会（T-CY）[71]以及网络犯罪项目办公室（C-PROC）[72]。网络公共委员会是公约体系的专门负责机构，负责跟进和评估通用标准的运行。网络犯罪项目办公室是专门的技术支持机构，通过技术的培训和升级完善公约体系的治理，主要负责能力建设。这种组织构架与《布达佩斯公约》规定的相关规制之间形成了一种稳定的互动关系。

《布达佩斯公约》也涉及网络恐怖主义的规制。从公约规定的这 9 种罪行来看，公约并没有直接规制网络恐怖主义。但是，从犯罪构成要件上分析，公约规定的 9 种犯罪的行为要件为规制网络恐怖主义罪行提供了依据。从公约使用的“计算机系统”和计算机数据等信息技术中立语言上可以推断，公约规定的实体罪行适用所有的技术性犯罪。例如，在恐怖分子以网络为攻击对象，侵入、干扰计算机网络的正常运行，引起社会恐慌的情形下，公约显然是适用的。

1.2 《合作打击信息犯罪公约（草案）》

达成一个全球层面具有普适性的打击网络犯罪的国际合作机制符合国际社会的期待，这一期待日益严峻的网络犯罪挑战相匹配。在美欧主张的以“信息自由”为主导理念的《布达佩斯网络犯罪公约》治理体系未来发展受限的背景下，中俄等网络技术发展中国家提出了新的治理路径——以“网络主权”为主导理念，在联合国框架下构建主体更多元、适用更广泛的国际性公约。2019 年 10 月，俄罗斯在第 74 届联大三委提交新的“打击为犯罪目的利用信息通信技术”决议草案，包括我国、南非、印度等在内的 40 个国家参与共提。[73] 俄罗斯提交联大审议并通过了《合作打击信息犯罪公约(草案)》（下称《草案》），旨在对抗网络犯罪《布达佩斯公约》体系，以在联合国框架下解决国际网络犯罪问题。这一网络犯罪的全球治理体系能够较好的解决《布达佩斯公约》规制网络犯罪体系中产生

的问题。

首先，“网络主权”治理理念并不拒绝新的国际规则的出现。该治理理念没有否定全球性打击网络犯罪规则创制的必要性，而是要求将联合国视为构建全球性网络犯罪公约的主体。联合国的规则创制模式与“网络主权”理念更匹配——联合国采取“一国一票”平均分配制度而非“加权分配制度”，意味着任何问题一旦进入讨论议程，理论上各个参与国对被讨论议程的话语权基本一致，由此网络弱势国家在规则创制上的话语权能够得到保障。相对而言，发达国家并未因自身实力强硬而获得更大话语权。《草案》决议在联合国设立一个代表所有区域的、不限成员名额的特设政府间专家委员会，并由该委员会拟定打击网络犯罪全球性公约。这一专家委员会保障了所有国家的话语权，不再使网络犯罪的治理存在于“发达国家俱乐部”之中。

其次，在《草案》中俄罗斯提出的草案适用罪行范围更大。《布达佩斯公约》适用对象是明确的网络犯罪,而俄罗斯草案的适用对象是信息犯罪和其他违法行为,后者的适用范围更具有拓展性和解释空间。《草案》规定了针对网络空间的 14 种主要罪行，将此前《布达佩斯公约》未曾纳入的网络钓鱼、发送垃圾邮件、违反国内数据保护规范罪行以及通过网络实施的违反国际法的罪行等全部纳入公规制射程，这使《草案》更加适应当前以“传统犯罪的网络化”为主要特色的罪行发展趋势。

1.3 问题

《布达佩斯公约》虽然是当前最具影响力的国际网络犯罪治理机制，但是从主体范围、犯罪类型、加入条件等方面来看，其不可能发展为全球化的网络犯罪治理标准。

首先，《布达佩斯公约》是由欧委会区域性治理发展出来的一种国际合作治理模式，其参与起草和制定的主体都不具代表性——仅有 26 个欧洲委员会成员国及 4 个观察员国参与其中。而对于网络后发国家而言，他们在同一领域内的利益需求与美欧迥异，接受美欧的治理理念与既定规则必然意味着将处于被动与不利地位，因此《布达佩斯公约》不易被认同和接受为全球标准。

其次，公约中对网络犯罪的类型界定完全以美欧等发达国家的价值取向和关

注重点为主，不具有全球拓展性。《布达佩斯公约》主要规制技术性网络犯罪，即以网络为犯罪对象的犯罪。这些都是网络技术较为发达的国家关注的犯罪罪行，规制这些罪行是因为网络技术犯罪会对经济安全造成威胁，打击犯罪的目的也在于保障私营企业获利、促进数字经济的繁荣发展。此外，《布达佩斯公约》规定的网络儿童色情和侵犯著作权及相关权利有关的犯罪也与跨国媒体、跨国公司以及流行文化产品等经济领域的利益切实相关。《布达佩斯公约》并未将发展中国家所关注的网络犯罪问题——如对破坏国家安全和稳定的信息内容的监管和处理纳入其中。与此相反，发展中国家更重视“网络主权”，强调网络犯罪信息内容对国家和社会的危害，经济危害相对居于次要地位。相应地，发展中国家关注的国际网络犯罪集中在“传统犯罪网络化”问题上，这种网络犯罪的治理更需要在国家政府的主导下完成。一言以蔽之，在发展中国家的观念里，打击网络犯罪与网络恐怖主义的主要目的是为了维护国家主权、保障国家政治安全以及维持社会的稳定。正是因为网络技术发达国家和网络技术发展中国家治理理念的不同，网络技术发达国家就会以“信息自由”之名否认“网络主权”的正当性，在打击网络犯罪和恐怖主义过程中，与“信息自由”理念契合的《布达佩斯网络犯罪公约》不易被网络技术发展中的国家认同和接受，从而使该公约成为全球标准。

最后，非欧洲委员会成员的国家加入《布达佩斯公约》的条件过于繁琐和严苛。“获得缔约国全体一致同意”这一要求对于网络发展后发国家过于严苛，并不容易得到满足，因此《公约》缔约国的数量增加极为缓慢。欧委会也曾就简化加入程序提出相关方案。但该方案虽然取消了取得缔约国一致同意的要求，却又增加了公约委员会的审议或犯罪问题委员会审议的环节，仍然没有解决非欧洲委员会成员国家加入条件严苛和程序繁琐的根本问题。由此，《布达佩斯公约》不易被网络技术发展中国家认同和接受，从而使该公约成为全球标准。

2. 数据跨境流动

与网络犯罪和网络恐怖主义相似，在数据跨境流动的治理问题上，当前的治理理念依旧停留在美欧等网络发达国家提倡的“信息自由”之上。由于对数据的保护更加偏于商业价值，因此欧美等国支持数据的跨境流动。也正是由于这个原因，当前数据跨境流动的规制主要集中在国际贸易领域之中。但是对于网络

技术后发国家来说，数字贸易并不发达，对网络信息的关注更集中在信息主权与信息安全的层面。因此，网络技术后发国家更加积极的限制数据的跨境流动，以便将数据控制在更容易行使管辖权的国内地区。近些年来，欧美等国也对数据的跨境流动进行了一定的制约，但是其限制并非建立在数据主权之上，主张对数据的属地管辖权，而是建立在所谓的人权之上，强调公民的隐私权保障，其根本目的还是为了促进数据更好地跨境流动。

2.1 现存治理模式

内容层面的网络安全问题主要集中在数据跨境流动上。最初，数据跨境流动问题受到重视仅因其商业价值。世界贸易组织（WTO）在过去近 30 年里成长为全球最具影响力的国际组织之一，其基本功能就包含了国际贸易规则的创制和实施。WTO 作为全球唯一有权处理国家间贸易规则的国际组织，其规则体系对于支持全球数字贸易具有重要作用。主要体现在两个方面：

第一，《服务贸易总协定》（General Agreement on Trade in Services，下称 GATS）通过“技术中立原则”扩展到数据贸易领域后，数据流动与数据本地化的选择将受到影响。GATS 项下的《具体承诺表》中规定，原则上 WTO 成员国的数据是应当开放跨境流动的，但同时该项也规定了宽泛的安全例外条款，为数据本地主义提供了可能性。

GATS 将“服务贸易”界定为通过跨境提供、境外消费、商业存在和自然人存在四种方式提供服务。[74]由于 WTO 成员国在技术中立原则上达成普遍共识，一般认为，如果成员未明确表示排除适用，则 GATS 的相关规则也同样适用于通过网络进行的跨境服务。跨境服务往往需要客户和企业数据的跨境流动，这意味着 WTO 规则在一定程度上准许了数据的跨境流动。

与此同时，GATS 中也设置了安全例外条款，允许成员基于维护自身安全目的获得数据跨境流动义务免除，即在一定程度上准许了数据本地化。[75]数据本地化措施是否违背国民待遇原则取决于成员方的具体承诺。GATS 第 14 条之 2a 款规定：“本协定不得解释为要求任何缔约方提供其公开后会违背其基本安全利益的任何资料”。此外，GATT1994 第 21 条也明确规定了安全例外，其中 a 款规定更是直接关系跨境数据流动问题。GATT 第 21 条 a 款规定：“本协定不得解释为

要求任何缔约方提供其根据国家基本安全利益认为不能公布的资料”。这一条款给予了成员根据自身根本利益限制或禁止数据跨境流动的自由裁量权。当成员因数据本地化措施出现争议时，WTO 专家组/上诉机构首先应对该措施涉及的贸易类型进行界定，以确定应适用 GATT 规则或 GATS 规则。虽然对成员国的数据本地化措施通常需要经过必要性检查，但是在解决跨境数据流动问题上难以判断数据本地化措施是否符合比例原则。[76]

第二，在 WTO 项下开展诸边谈判，制定各个成员方之间的数据流动规则。WTO 成员于 2019 年 1 月发起“电子商务诸边谈判”，旨在制订电子商务/数字贸易领域的国际规则，以适应经济的全球化和数字化发展。目前数字贸易在 WTO 项下展开主要是依靠此种机制，即成员国之间的区域贸易协定。根据 WTO 的相关规则，区域贸易协定可以成为最惠国待遇的例外。也就是说不同的成员方可以按照各自的立场，确定数据流动的基本原则。[77]

WTO 旨在促进数字贸易发展，也在规则上支持数据的跨境流动。但是，GATS 也从根本上确认了隐私的重要性，并将其作为一项基本政策目标在各成员之间达成共识。由此，在 GATS 框架下，跨境数据流动面临法律上的双重规制：一是跨境数据自由流动并非原则，而是具体承诺，需要专家组个案认定。GATS 第 14 条保障的核心内容是成员在数据和隐私保护方面享有施加措施以便达到保护机密性和安全性目的的权利，而并不保证所有成员都在数据和隐私保护方面采用统一和相同标准的具体承诺。二是任何涉及数据隐私的法律和法规均可能限制跨境数据的自由流动。但是这种限制也应当有一定的限度。根据 GATS 第 6 条第 5 款的规定，对于已经对数据服务作出承诺的成员方，是不能再通过国内法规减损其所作承诺的，除非这种国内法是在实施“国际标准”，否则认为这种减损是违反承诺义务的。

由于 WTO 规制对于数据跨境流动的规制需要根据各国的具体承诺进行个案判断，因此在客观上并没有建立起一个统一的国际数据跨境流动规则。因此，现阶段数据跨境流动规则主要是以双边协定和国内立法的模式进行的。由于网络技术发达国家与网络技术后发国家在治理主导思想上相差较大，目前国际上关于跨境数据流通的规制存在以下三种主要模式。

俄罗斯：数据本地化

俄罗斯要求数据的存储与处理均在国内进行，强烈排斥数据的跨境自由流动。采取与此相类似规制模式的国家还有马来西亚、巴西及印度等。

俄罗斯于 2014 年 5 月和 2014 年 7 月先后进行了两次立法修改。[78]通过这两次修改，可以看出俄罗斯对数据跨境流动的态度:(1) 公民个人信息应存储于俄罗斯境内;(2) 处理公民个人信息应在俄罗斯境内进行;(3) 数据相关主体应积极配合国家监管工作。[79]

俄罗斯在网络安全治理问题上一直坚持“网络主权”保障理念，其所倡导的数据本地化规制路径通过严控数据流动，试图将侵犯数据安全和威胁国家网络主权的风险扼杀在摇篮里。数据本地化的根本目的在于对数据所承载的安全和价值进行直接控制以实现强化国家网络主权战略。对于正在快速发展的新兴国家来说，在面临相对较高的网络风险和相对较弱的国内信息技术产业竞争力条件下，优先保障发展和安全是首要目标。

美国：数据自由跨境流动

美国规制路径是在保证跨境数据自由流动的基础上，由数据控制者或数据处理者以合法、合理的方式对数据的安全性负责，否则将被数据监管机构问责。

与欧盟自上而下统一立法的事前预防模式不同，美国行业默认数据控制者或者处理者在商业活动中应自觉遵守相关规则，仅在事后对违法行为进行惩罚。因此，该规制方式能够最低限度地避免跨境数据滞留，同时也降低了行政机关的监管压力。美国规制路径一方面强调企业对相关规则的遵守，另一方面又对违规企业进行事后问责。该规范体系的建构旨在为数字经济产业创设最低标准，让跨境数据流动的限制机制回归市场。

可见，在美国看来，数据跨境流动完全是一个商业问题，仅依靠市场可以规制，监管问题也仅仅依靠行业自律和行业协会。亚洲太平洋经济合作组织(APEC)在制定数据跨境流动规则时，处处体现着促进自由流动的思想，这显然是美国起主导作用的结果，也是美国推广自身模式最重要的一次实践。

APEC《跨境隐私规则体系》(Cross Border Privacy Rules system，CBPRs)

是“规范 APEC 成员经济体企业个人信息跨境传输活动的、自愿的多边数据隐私保护计划”。[80]CBPR 由隐私执法机构、问责代理机构和企业三方共同参与。问责代理机构（Accountability Agent）的性质是一个行业自律组织，监督企业达到上述组织机构标准，对认证企业的行为进行监督和处罚；违规企业所在国的隐私执法机构对违规企业进行法律制裁。[81]符合 APEC 隐私框架提出的 9 项个人信息保护原则、50 条具体要求的企业将获得认证，并可以在亚太地区收集、传输和利用信息资源。

CBPRs 体系下问责制运行的流程是：企业自评是否可以达到标准，如果自认不能，则修改自身的隐私政策；修改后提交问责代理机构审查，审查通过后获得 CBPRs 认可的隐私保护信赖标章。CBPRs 体系内的公司经认证获得信赖标章后即被认为在隐私保护领域是值得信赖的企业，企业之间的个人数据可以在得到充分保护的基础上自由流通，不受成员方经济体国内法的限制。[82]但是，如果违反 CBPRs 相关安全保障条款或承诺，则该企业要受各国隐私执法机构问责处罚。

CBPRs 体系下设各国隐私执法机构，这些机构具有执法权力。那么执法权的权力来源以及依据是什么呢？是缔约国国内法对于隐私权的保护。但是涉及国内法问题就必然会出现管辖权冲突，为了解决这个问题，CBPRs 设置了准入的一个门槛——缔约国必须加入 APEC 跨境隐私执行合作安排（cross-border privacy enforcement arrangement，CPEA），以协调数据流通领域的执法合作。

欧盟：附条件的数据跨境流动

欧盟规制路径采用双重标准：对于欧盟成员国，禁止以数据保护为由阻碍跨境数据的自由流动；而对于其他第三国，则需以欧盟事先审查确认第三国可以充分保护其数据安全，并认可其资质为前提。[83]

欧盟成员国在向第三国转移个人数据时需要第三国达到充分保护水平。GDPR 规定，在评估保护水平是否充分时，应特别考虑到下列因素：（1）法治、尊重人权和基本自由、一般和部门性相关立法。它包括关于公共安全、国防、国家安全和刑法以及公共当局获取个人数据的立法，以及关于此类立法、数据保护规则、专业规则和安全措施的实施规定，如将个人数据传输到第三国或国际组织所遵循的规则、判例法以及有效和可执行的数据主体权利和保障数据主体权利的

有效行政和司法补救；（2）存在独立监督机构并有效运作，负责确保数据保护规则的强制执行。包括充分的执法权，以协助数据主体行使其权利并向其提供建议、意见，并与成员国的监管当局合作；（3）已加入的国际承诺，或具有法律约束力的公约、文书以及因参与多边或区域体系而产生的其他义务，特别是在个人数据保护方面。[84]

此外，为了事先确保数据的隐私安全，欧盟对“特殊数据”进行细化分类，并按种类确定安全保障标准。根据 GDPR 第 9 条的规定，个人最为隐私、最不愿被人得知的数据（如，个人的健康数据、性取向、生理需求等），不论目的和用途，都受到最严格的安全保护。个人基因数据、生物特征数据在不用于对人的识别的情况下可以适当降低安全保护标准。哲学、政治、宗教相关的个人数据保护强度更弱，仅要求不得泄露。

强化数据控制者的责任体现了对事前防范的强调。GDPR 规定了数据控制者应当承担的义务。（1）报告数据泄露义务。GDPR 第 33 条规定，当发生数据泄露时，数据控制者应当及时向数据监管机构报告数据泄露。GDPR 第 34 条规定，当个人数据泄露可能对自然人的权利和自由产生较高的风险时，数据控制者应当将数据泄露事故及时告知数据主体。（2）数据保护影响评估和事先咨询义务。GDPR 第 35 条规定，当数据处理由于运用了新技术等可能会对数据主体的权利和自由造成较大风险时，数据控制者在进行数据处理前应当评估处理行为对个人数据保护的影响。GDPR 第 36 条规定，当数据控制者进行评估之后表明数据控制者无力减少该风险，数据控制者应当在数据处理前向监管机构咨询。

2.2 现存治理模式存在的问题

利用国际贸易规则规制数据跨境流动存在着天然的不足。国际贸易规则仅适用于数字贸易领域的数据化境流动，对数据跨境流动的风险防范不足。数据的跨境流动主要涉及到以下风险：第一，数据隐私风险。个人数据被恶意利用和买卖，将对个人隐私、财产甚至人身安全造成严重威胁。第二，数据安全风险。数据被泄露、监听和盗取，不仅数据主体权利无法得到保护，企业商业机密、知识产权等也会被侵犯，整个国家的数字产业竞争力也将受到威胁。第三，国家基础数据安全风险。关于国家基础设施的敏感数据涉及国家安全，一旦泄露或被窃取，

将带来严重的不可控风险。作为一个经济组织，WTO 对跨境数据流动的规制局限于对个人数据和个人隐私的保护，没有重视数据流动过程中涉及到的其他风险。

信息本地化模式则仅关注了数据安全风险，忽视了数据在数字贸易领域的巨大经济价值。要求信息本土化这一做法过于绝对，存在很大的缺陷。首先，数字贸易和数字经济发展需要数据流动，数据绝对的本地化会造成经济与贸易的停滞。同时，严苛的数据本地化要求有可能会引起国外对等性保护主义，即，一国企业走出去很有可能受到其他国家的同等限制。其次，数字安全在国内范围无法保障。数据本地化会使国家掌握所有公民的所有信息，甚至沦为国内政府监视公民行为的借口。[85]最后，数据本地化所采取的措施需要经过合目的性和必要性的论证，但是由于论证的科学性和认可程度存疑，因此采取何种本地化措施成为了数据本地化实施中的又一大阻碍。

美国的事后问责制也存在明显缺陷：第一，一旦造成损害，结果不可逆转。由于不存在任何事前限制，数据完全自由流通一旦出现问题，庞大流量造成的损失无法估量。第二，要求企业自我监管和自我审查，由此带来的成本让大量中小企业无法承受。此外，涉及到信息跨境流动的企业自律水平也参差不齐，行业监管也很难达到较为理想的效果。第三，事后监管无法使数据恢复原状，处罚仅仅体现在货币金额上。且美国不同于欧洲，对企业侵害公民隐私权的处罚力度较低，对大型企业威慑力十分有限。

欧盟的问题在于，赋予第三国数据跨境流通资质的考察充分性保护认证报告，基本上只遵循形式审查原则，而对于各个国家的实施效果并未给予足够关注。而且，审查程序冗杂，形式审查时标准过高，客观上阻碍了数据的跨境流动，与欧盟本身网络自由的主导治理理念相悖。

3. 域名地址资源分配

在尤查·本克勒提出的网络空间系统分层理论中，逻辑层指控制和维持硬件运转的软件和协议所在的层级。逻辑层将散布在全球各地、数以亿万计的物理基础设施通过各种通信标准和协议连接，形成了真正“互联、互通”的网络。其中，域名系统（Domain Name System，简称 DNS）是构筑域名、IP 地址的相互

映射与互联网信息查询互通的基础系统。故而在逻辑层，全球网络治理的聚焦点与争论点落足于域名分配系统的控制权争夺上。引而言之，DNS 的安全治理与其控制权争夺密不可分。为保障互联网的正常运行，域名安全在网络安全问题中是“牵一发而动全身”的机要议题。为弥补 DNS 协议自身的脆弱性、抵抗层出不穷的 DNS 攻击，部署域名安全保障体系是全球网络治理的重要任务。

3.1 概况

ICANN 是目前域名分配的治理主体，其运营模式为“多利益相关模式”(Multi-stakeholders)。“多利益相关模式”早在 1997 年就出现于由美国政府发表的“有关互联网名称和地址管理”的白皮书中，该文件对 1998 年 ICANN 的成立影响颇深。尽管如此，ICANN 仍长期被看作是美国在全球域名治理上的单边控制之工具。虽名为非营利私有组织，但 ICANN 下属负责操持 DNS 系统的 IANA 曾长期受美国商务部下属的国家电讯局(NTIA)的技术监管。控制“.com”和“.net”域名的管理者 VeriSign 公司也与美国商务部有合约关系，受其指令。[86] 美国政府的单边垄断既不符合互联网群体对去主权化自治的期待，也不符合各国对网络主权的期待，长期受到来自各界的呼吁改革的压力。[87] 对 ICANN 改革模式的争论依然体现出网络安全治理与传统政府事务治理方式的二分，即“多方主义”与“多边主义”的对立。两种治理方式分别对应了两种 ICANN 改革的方案，即强调国家间联合治理的“联合国模式”，与“多方利益相关方模式”，或称“公司模式”。[88] 其争议重点在于参与治理的主体与政府的角色。中国、俄罗斯和许多中东国家倾向于“联合国模式”，支持政府在网络空间治理中发挥更明显的功用；而美国、欧洲、日本等国家政府支持“多方利益相关模式”，强调政府、民间社会、商业力量和学术界的平等参与。

联合国模式的基本诉求是在 ICANN 之外，重新打造一个政府间域名治理机构，由各国联合治理。联合国模式的重点是将治理主体限制在国家政府层面，要求各成员国都享有一票表决权。一些国家也提倡将 ICANN 的职能转移到现存的、可以实现这一目标的国际组织下辖机构中，如国际电信联盟（ITU）。ITU 主要负责协调无线电频谱的全球共用，不仅是世界上最古老的政府间组织，且自成立以来一直以“政府间公私伙伴关系组织”的形式制定全球标准、改善发展中国家电

信基础设施建设。[89] 2005 年，欧盟在突尼斯“信息社会世界峰会”上首次提出将域名管制权转移到联合国的国际电信联盟所领导的“互联网工作组”（Working Group on Internet Governance，WGIG）。[90] 然而，这仅是欧盟试图打破美国域名控制垄断的尝试之一，其后期对“联合国模式”的态度较为暧昧。目前支持在国际电信联盟职能中囊括域名分配权与管理权的，主要是发展中国家、新兴经济体等网络技术后发国家。2011 年 9 月，印度、巴西和南非联合建议将 ICANN 纳入国际电联下管理。同年，上海合作组织向第 66 届联合国大会提交“信息安全国际行为准则”，旨在推动以各国政府为主体的多边主义互联网治理规则的制定。[91] 2012 年的国际电信世界大会(World Conference on International Telecommunications, WCIT-12)修订了 1988 年的《国际电信条约》，采纳了俄罗斯、中国、沙特阿拉伯等国的提案，增大了 ITU 在网络空间治理方面的法律权重。然而，美国和大多数欧洲国家拒绝签署修订后的条约，旗帜鲜明地反对多边机制的扩张。[92] 2014 年的国际电联全权代表大会（ITU Plenipotentiary Conference 2014）上，各国撤回了多边主义扩张提案，转而妥协于吸纳更多利益相关方参与决策。[93] 这证明了在美国依然保持着域名治理中的强大优势、并且坚持 ICANN 现有治理框架的现状下，通过修订更改现存的代表全球共识的条约向国际政府间多边组织让渡部分网络管理权力，尚且难以成功；实现网络治理更大范围的“联合国模式”，更是道阻且长。

与之相对，摒却国际各界的实际观感，“多方利益相关主义”则一直是 ICANN 所宣称的、贯穿始终的原则。吸纳鼓励更多元的利益相关方参与到域名管理的决策中，符合 ICANN 成立之初的价值导向。ICANN 进一步拥抱多方利益相关制度的转型是自然的、且已经发生的。这一点与域名管理系统本身处于互联网“逻辑层”，强调技术主导与“去主权化”是密不可分的。在互联网发展早期，域名管理系统便由技术社群所统领的 IANA 所管理，在技术社群痛失 Jon Postel 后，美国政府才主导了管理权的私有化，将 IANA 归入加州的私有非盈利公司 ICANN 下。但私有化后，美国商务部却对互联网域名长期保有行政监管权，ICANN 下 IANA 的域名管控权是由商务部“授权”的。这被看成是政府“通过行政干预对全球互联网基础资源实施幕后操控”的明证之一。[94] 2014 年，美国商务部宣布将互联网域名管理权（stewardship）让渡给 ICANN。2016 年正式签署文件，ICANN 自此作为

IANA 的唯一成员，拥有对 DNS 的全部监管权限。从移交时间上看，此举是为了平复在“棱镜门”事件后美国政府无法再忽视的国际压力：将行政管理权让渡给一个奉行“多方利益相关主义”的非盈利性组织，无疑让重视网络国家主权的国家失去了一个批评“单边垄断”的有力论点。这次让渡对“多方利益相关主义”的进一步强调也体现在美国商务部下辖的国家电讯局（NTIA）在让渡声明中。NTIA 提出了管理权转移四大原则：1. 支持和增强多方利益相关主义模型；2. 维持网络 DNS 系统的安全性、稳定性和强韧性；3. 满足 IANA 服务的全球消费者和合作伙伴的需求与期待；4. 维持网络的开放性。[95] 根据让渡的目的和原则，监管职能自然应该交予“多方利益相关者”。[96]

在 IANA 管理权让渡的同时，ICANN 启动了一个“多方利益相关者”参与决策的正式机制，称为“赋权社群”（Empowered Community）。“赋权社群”的成立被看作 ICANN “迈向真正的多利益相关方治理模式的里程碑”。[97]赋权社群（Empowered Community）是根据美国加州法律设定的非盈利联合体，具体由五个组织构成：地址支持组织(ASO)、国家代码域名支持组织(ccNSO)、通用名称支持组织(GNSO)、一般会员咨询委员会(ALAC)和政府咨询委员会(GAC)。[98] 概括来说，赋权组织可以通过一套自下而上的流程（escalation process）与 ICANN 董事会讨论解决方案，对董事会的“作为”与“不作为”表达担忧。[99] 具体来说，通过赋权组织，多利益相关方对 ICANN 的控制体现在三个方面：实质控制、日常治理、与问责监督。[100] 在实质控制方面，剔除了美国商务部的参与，ICANN 成为 IANA 的唯一成员，这意味着 IANA 对域名分配系统的管理权来源于赋权社群的授权，这也是让渡事件的关键改变；在日常治理方面，赋权社群拥有包括对 ICANN 董事会进行任命与移除（除总裁外）、拒绝《标准章程》的修订内容、拒接接受 ICANN 运营和战略规划等权力；在问责监督方面，赋权社群有权要求董事会复审复议、启动调解或独立审核流程。[101]

3.2 问题

多利益相关方模式

美国对“多利益相关方”模式的推崇无外乎两点考量：一是域名管理权一旦移交给政府间国际组织，满足“联合国模式”的一国一票的诉求，美国必须面临国际协作问题。

而美国所代表的信息发达国家与信息发展中国家在网络空间属性是“全球公域”还是“主权领域”的问题上发生了严重分歧，很难达到共识[102]。二是“多利益相关方”模式可以放大美国互联网产业优势。

针对 2014 年的 IANA 主权让渡，NTIA 曾一再强调美国商务部一直以来仅对 DNS 管控行使“行政监督权”，这一权力的转移将带来的改变是微小的。这种说法固然出于美国政府强调 ICANN 的私营性与其运营独立公正性的主观意图，实际上在与其意图相反的层面上，ICANN 的“多方利益相关模式”的确颇具讽刺意味体现了改革前后一致性：ICANN 固然通过“赋权社群”确立了更完善的各利益相关方参与决策与监管的机制，但其强调的“多方利益相关模式”，毋宁说是围绕美国国家整体利益的“多方利益相关模式”。

虽然每个赋权社群的成员理论上都是决策者，不同赋权社群的参与者在重要事项上的决策权却有显著不同。在董事会提名上，代表互联网域名注册机构、互联网服务提供商等的通用名称支持组织和代表一般网络用户的一般会员咨询会拥有比余下社群更多的提名席位；而政府咨询委员会（GAC）却不被赋予提名权。这无疑体现了对互联网行业权利的放大、对各国政府权力的限制。[103] 除此之外，ICANN 对 GAC 的限制还体现在两方面。第一，ICANN 董事会仅承诺会将 GAC 的意见纳入考量，但没有义务贯彻实施（ICANN 2016，Section 12.2）；第二，2016 年 ICANN 改革的同时，其章程规定，GAC 在公共政策方面的提议必须达到“无一反对”、“全体认同”的共识才可通过（ICANN 2016，Section 12.2）。[104] 然而在实际决策中，各国政府代表的分歧，很难达到全体认同，ICANN 的这一规定实际上高度限制了 GAC 的功用。[105] 总结来说，同为赋权社群，ICANN 明显偏向保障互联网行业利益，着力于削弱政府方的决策参与，这明显有悖于其平等接纳各方意见的宣称。这种体制下美国对 ICANN 机制的影响力并未减弱。作为互联网发展的起源地，私人部门与商业力量正是美国强大信息产业的主力军。但从技术话语权与商业影响上来说，发展中国家属于技术后发方，与美国、日本等技术先发方的差距短时间内无法弥补。通过“多方利益相关制度”，美国既有组织法作为其运营合理性的背书，又维持了信息技术资源上其旧有的优势，进一步扩大了其与发展中国家在网络治理话语权上的差距。

联合国模式的问题

支持“联合国模式”的大多为发展中国家。他们倾向于将互联网治理与国家和国际安全与经济发展相联系，将其与信息安全和信息环境等议题结合在一起。互联网及信息通信技术（ICT）对全球经济的重要性以及战略价值日益突显，把互联网治理置于国际机构保护之下的想法也日益得到重视。但“多方利益攸关者”模式的支持者们认为一旦将互联网国际治理转入联合国掌中，互联网的开放性和免许可（permission-free）的商业自由度将不可避免地受到侵蚀，互联网一直以来的创新性将受重创。联合国自身的集中化、官僚主义、与决策机制带来的话语权偏移使拥护 ICANN 非政府、非营利性质的互联网社群感到恐慌。

目前联合国模式在全球网络空间治理上面临着如下三个困境。其一，在保证多利益相关方群体的治理模式下，IGF 等联合国空间治理机制强调会议的开放与宽松，为了尊重多方观点，避免涉及敏感议题。这导致了 IGF 等论坛往往只能输出仅能作为建议的文件，而非指导性的、有具体规划的实施方案。而即使协议通过，由于非政府组织的利益相关方的缺席，计划缺乏落实的必要工具，无法实施。[106]

其二，负责网络空间治理的联合国部门中，非政府行为体多利益相关方不具备投票权，也就是在治理机制的正式文件的决策过程中是缺位的。如前所述，这样通过的文件无法得到非政府组织利益相关方的认可，也就阻碍了文件的落实。一些联合国采取“专家组”的形式负责相关治理议题，但其决议过程不透明，成了易受大国博弈影响的“烟雾缭绕的后室”，无法反应多方利益的平衡。负责网络空间治理的联合国部门与 ICANN 的多利益相关方制度中政府与非政府方的缺位，是机制代表性不足的一体两面，都无法达到全球互联网共治的诉求。

其三，网络技术先发国家与后发国家利益矛盾尖锐。正如在 ICANN 多利益相关方制度下，不同背景的多元利益方的内部博弈，使得达成共识尤为艰难。联合国成员内部发达国家与发展中国家对于国际制度规范的诉求是相矛盾的。美国作为占优者寻求如欧盟、日本等技术先发国以互联网行业间的“连横”方式进行守成；而发展中国家希求“发展空间”和“补偿”，寻找盟友政府以“合纵”方式试图打破技术垄断。两种求变方式存在根本性冲突。

域名安全与 DESSEC 部署现状

DNS 系统的安全是互联网正常运营的前提。DNS 的主要功用是把域名解析，即把域名转换为 IP。电脑、手机等终端发送域名请求（如 baidu.com）之后，DNS 服务器将其转换为对应的 IP（如 39.156.66.18），与该 IP 建立通信，并向用户展示交互网页数据。在家中、咖啡馆、企业的 DNS 服务器和一些公用 DNS，依据其工作方式称为“递归 DNS”（或本地 DNS，LDNS）。LDNS 对于第一次接收到的域名查询并没有直接的对应 IP 信息，这时候就会询问“权威 DNS”，即掌握一定范围内对应 IP 信息的服务器。权威域名体系的构造呈“反向树形结构”[107]，顶层为根域名，其下为顶级域名，顶级域下又进一步注册二级、二级以下的域名。域名由各层级名称中间由“.”串连而成。域名的层级树形构成一个域名空间，而储存域名的数据结构叫做资源记录（resource record，RR）。当接到本地 DNS 的域名查询请求后，根域名区（zone）负责返回处在第二层的顶级域名，顶级域名区负责返回第三层域名。域名查询会在层级服务器上不断递归，直到达到存有与域名相对应的 IP 地址的域名区，最后返回 IP 地址。

域名安全是互联网治理领域的焦点，在域名安全保障的技术标准制定上，存在政治、经纪、法律等纠纷。作为互联网早期协议，DNS 系统在设计时却缺乏信息保护和认证安全机制，是“建立在互信模型基础之上的开放体系结构”。[108] 在实际运用过程中，DNS 系统在多个环节都有具有脆弱性。随着互联网产业的蓬勃发展，针对 DNS 的蓄意攻击手段层出不穷，根据互联网工程任务组 IETF 规定的 RFC 3833，DNS 系统的安全威胁可以分为三方面：一是服务器与解析器之间的安全通信威胁；二是利用已有服务构造拒绝服务攻击(DoS/DDoS)；三是利用软件实现上存在的漏洞或者错误控制提升权限，控制 DNS 服务器。[109] 具体攻击形式有：DDoS、缓存污染、链路劫持、流量窃听、偷窃用户隐私信息等。[110] 其中，DNS 域名缓存污染（又称 DNS 投毒）仍是主要的攻击方式。

DNS 域名缓存污染主要利用了用户数据保护协议 User Datagram Protocol（UDP）的传输方式与本地服务器（LDNS）的 IP 信息缓存（cache）机制。UDP 的重要特点是“无连接、不可靠”。UDP 模式下用于通信的 IP 报头包含申请查询终端的 IP、DNS 数据报文、与应由权威 DNS 回应的响应包 IP。由于无连接，攻

击者可以伪造成权威 DNS 的 IP，并掉包其中的 DNS 数据报文，将用户的域名申请转到一个错误的网页，这就是 DNS 攻击。攻击者一般会迅速发出多个伪造响应包，让 LDNS 接受其中一个。一旦成功，UDP 协议会自动终止通信，迟来的真正响应包无法传输到 LDNS 上。本地 DNS 服务器（LDNS）是有“缓存”（cache）的，它会将已经查过的 IP 信息储存下来。LDNS 下一次接收到同样的域名查询，就会直接从缓存给出答案，只要不过期，就不会再到互联网上进行递归查询。这就意味着一旦攻击者在第一次查询将正确的 IP 掉包，以后每次查询都将引向错误的网址，这就是 DNS 缓存污染。

针对 DNS 污染，目前最有保障性的机制是由 IETF 开发的域名系统安全扩展（domain name system security extension, DNSSEC）。DESSEC 在原有的 DNS 协议之上“扩展”的部分，是通过公钥基础设施（public key infrastructure, PKI）在其之上添加了域名注册人的数字签名(digital signature)的功能，以此来提供权限认证、验证数据完整性。[111] “注册人”是指有权控制域名相关信息(即，名称转换为地址的映射以及其他数据)的个人或组织。DNSSEC 准许注册人对他们存放在 DNS 中的信息进行数字签名，这样一来，客户端(例如， Web 浏览器)就能够验证所接收的内容与发送前进行数字签名时是否一致、是否遭到了恶意篡改。[112]在 DNSSEC 的实际运行中，每个服务器区需要双重密钥 [113]：对 DNS 资源子路本身进行签名的“签名密钥”（ZSK），和对包含 ZSK 密钥的资源记录进行签名的“密钥签名密钥”（KSK）。而每一个域通过 RSA/SHA-1 密码算法为下级域产生一个公钥/私钥对。下发私钥、密码互相核对的过程称为安全授权。[114] DNS 的层级结构使得“根区”的 KSK 公钥成为了最顶端的、所有区的信任锚（trust anchor）。

如今 DNSSEC 作为保障域名体系安全的技术在国际上获得了越来越广泛的认可和应用，但从部署率、认证率上来说仍不乐观。2010 年，ICANN 针对 DNS 的顶层(即“根”)实施 DNSSEC 签名。2014 年 ICAAN 的报告称，根区域超过 50%的顶级域名均已部署了 DNSSEC。然而，在 2020 年的报告中，ICANN 承认，“2010 年根区签名十年后的今天，DESSEC 的部署仍然滞后”[115]。2018 年和 2019 年发生的一系列国际 DNS 劫持事件[116]，导致美国网络安全和基础设施安全局 (US- CERT) 首次发布紧急指令，敦促 ICANN 再次呼吁所有 DNS 利益相关方全面部署 DNSSEC。

[117] 但推进 DNSSEC 全面部署面临着双重困难：技术挑战与政治风险。

在技术层面上，DNSSEC 部署在技术上仅能较为有效地防止域名污染的问题，仍存在至少为五点技术限制。其一，DNSSEC 会降低域名/IP 互通的响应效率。密钥认证系统使得每一步 DNS 查询/应答中报文所包括的密钥长度层级增长，会占用大量的网络带宽资源，不仅会使得日常查询/返还的时间变长，更会使 DNSSEC 更容易受到放大攻击的威胁；其二，DESSEC 不能保证密钥的传输通信安全，即无法保证密钥不会泄露。其三，DNSSEC 的部署对 CPU、DNS 服务器配置及管理系统的性能都有更高要求。换言之，DNSSEC 提高了部署运营成本；其四，DNSSEC 可以做到“验伪”，但无法解决隐私泄露问题，需要额外的加密技术。更高的加密技术要求又进一步提高了技术门槛和运营成本。总之，DNSSEC 的部署对于 DNS 服务器持有组织、所在国家都存在天然的加入门槛。这引出了 DNSSEC 的第五个技术挑战，即渐进式部署的缺陷。由于各地区与各利益相关方的技术资源差距，DNSSEC 无法在短时间内在全球范围内完成部署，只能采用渐进式部署。但 DNSSEC 的核心，即认证人签名，并不适合渐进式部署。要从认证体系中获益，必须确保负责“发布”的注册人和负责“查询”的解析方双方都进行了 DNSSEC 部署。否则未部署的一方无法解析数字签名，而部署的一方也无从验证信息的真伪。换言之，DNSSEC 无法与传统 DNS 系统兼容。这对不同域之间的互操作与信息引用造成了巨大挑战。[118]由目前的进度来看，DNS 与 DNSSEC 并用的时期仍会延续。有学者认为，率先部署 DNSSEC 的区，为真正受益于信任链，会形成一个个“安全孤岛”[119]。DNSSEC 部署区或是选择为了隔绝错误信息，将来自大量未部署 DNSSEC 地区的信息隔绝在外；或是只能承受与未签名区互通信息时混入错误信息的风险。

在政治层面上，DNSSEC 的部署带来的最显著风险便是在其体制下根区密钥管理权所代表的政治势能。一旦全球 DNSSEC 部署完毕，根区信任锚就会成为全球 DNS 安全的切入点。而根区密钥的管理权，根据与美国签署的合同，皆被 ICANN 与 VeriSign 公司掌握。全球绝大多数根域名服务器也处于美国境内。如上所述，即使美国商务部已不再对 ICANN 进行监管，ICANN 的现存框架仍使得网络治理资源向美国技术商业公司及组织倾斜，使得美方“利益相关方”对决策的影响力更大。而 DNSSEC 的技术门槛、部署运营成本与渐进式部署的“安全孤岛效应”极有可能放大这种倾斜，造成互联网关键资源控制权的严重不平等。在各国在数据

流动、信息安全方面的利益冲突升级时，不排除掌控大多数根区密钥的美国借提高 DNSSEC 安全性之名，进一步保持美方对数据信息的掌控和网络空间行为话语权，进而重建实质“单边控制”的可能。

4. 本篇小结

图 2 简要勾勒了本篇内容。可见，欧美等发达国家以“网络自由”为主导理念治理网络犯罪与网络恐怖主义，现行国际规则由此侧重经济问题。[120]由于欧美国家的经济主导地位，一旦国际社会将网络犯罪问题限定于经济维度（而非涉及国家安全的政治维度），就可以保证网络发达国家在网络安全领域的霸权地位，限制发展中国家拥有规则创制的话语权。

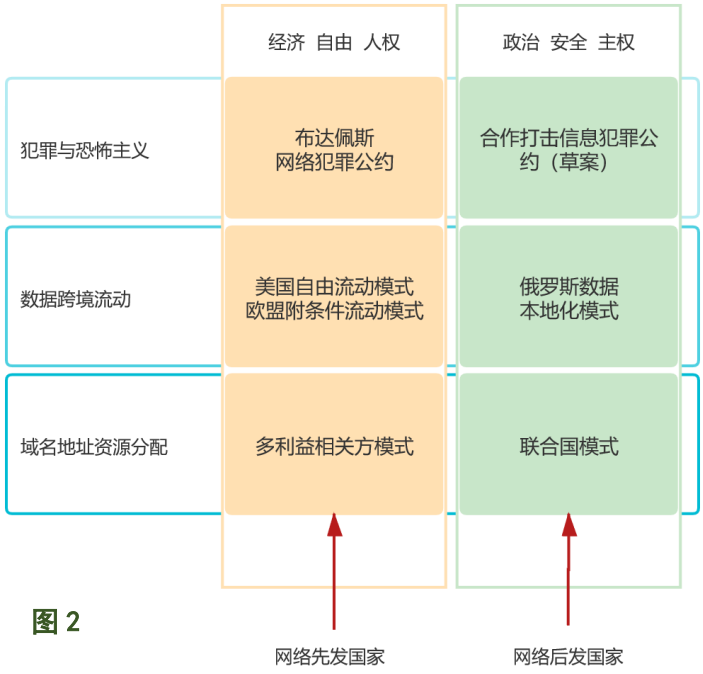


图 2

无独有偶，数据跨境流动的治理问题上，当前的话语权依旧掌握在美欧等网络发达国家手中，他们主导“网络信息自由”的理念也更偏重于使用数据的商业价值，从而支持数据的跨境流动。但是对于网络技术后发国家来说，数字贸易并不发达，他们更关注信息主权与信息安全，以及由此引发的国家安全问题。

而在逻辑层，全球网络治理的聚焦点与争论点落足于域名分配系统的控制权争夺上。推进域名安全保障的目标，除了对各界提出技术上的挑战以外，也延续了在域名治理主体上政治、经济利益的博弈。不同的安全技术部署方案，意味着不同的技术门槛、部署与运营成本，以及在技术优势国与后发国中互联网治理资源的不同倾斜。无论是 DNS 的控制权还是安全治理，都能看到“多利益相关制度”

与“多边主义”的权衡对抗，究其根本，也映射了对网络治理属于“国家主权”还是“全球公域”的不同想象。

第三篇 数字发展

信息技术发展为全球经济发展注入动力，但是全球范围内利用信息技术的能力存在差异，并由此带来一系列的影响。受 2020 年疫情影响，全球数字化经济发展加快，解决数字鸿沟问题，帮助各个国家抓住数字化转型机遇显得尤为迫切。

1. 全球数字鸿沟现象概述

1.1 全球数字鸿沟现象定义及分类

数字鸿沟指不同区域获取或者使用信息通信技术（ICT）的能力存在差距的现象，不同区域在数字化技术的获取与使用上产生了鸿沟，这种鸿沟主要表现在各个国家以及各个国家内部不同区域之间。全球数字鸿沟现象则是从世界范围来看，不同国家之间获取及利用信息通信技术的能力存在差距，这一现象在发达国家与发展中国家之间十分突出，部分发展中国家信息通信设备稀缺且技术水平落后而部分发达国家在信息技术领域占有优势地位，例如美国不仅掌握网络领域重要资源，且其信息通信技术发展迅速，垄断了领域内的重要产品，因而在全球信息通信领域中处于优势地位。[121]此外，发达国家之间、发展中国家之间也存在获取或者使用信息通信技术（ICT）能力的差距。[122]

随着社会的发展，不同区域之间获取及利用 ICT 的能力不断变化，同时随着这一领域的研究不断深入，数字鸿沟的概念也在逐步加深。目前，数字鸿沟涵盖了获取信息通信技术能力的差距、使用信息技术能力差距以及由于信息技术不平等使用带来的一系列社会影响的三道鸿沟。[123]

第一道沟：接入沟

第一道鸿沟指的是接入沟，即获取信息通信技术能力的差距。不同的国家或地区之间获取信息通信技术的能力存在差距，这也是数字鸿沟一开始的含义。针对第一道鸿沟，国际电信联盟认为经济水平差距较大的国家之间获取 ICT 技术的不平等是接入沟的重要表现。[124]近年来，随着社会生产力的发展与技术的进步，网络基础设施持续扩建，接入沟的差距已经渐渐削弱，[125]

因而第一道沟不再是数字鸿沟领域关注的重点。但是接入沟的差距并没有随着网络设施的扩建而被消除，尤其是在发达国家与发展中国家之间这一鸿沟仍然十分明显。根据统计数据显示，发达国家互联网的普及率已经超过了 70%，然而部分发展中国家网络普及率仍低于 10%，[126]仅仅在互联网普及率这一方面发展中国家就严重落后于发达国家，可见在全球范围内，接入沟问题仍然不容忽视。

第二道沟：使用沟

数字鸿沟中第二道鸿沟指的是不同国家或地区的不同使用者使用信息通信技术能力存在差异，拥有不同知识背景、不同学历水平的使用者掌握信息通信技术的能力不同并且利用互联网的方式不同。研究显示，受教育程度低、收入水平低的用户更偏好仅仅通过互联网进行娱乐项目，然而受教育程度更高、收入水平更高的用户则倾向于通过更加丰富、广泛的方式使用互联网。[127]从这一研究表现出的基本事实出发，考虑到发达国家与发展中国家之间经济水平、教育水平等多个方面存在着巨大差异，发达国家与发展中国家之间在如何使用信息通信技术技术、如何利用互联网等问题上存在着很大不同。随着网络基础设施的不断扩建，如何使用利用信息通信技术，缩小第二道鸿沟成为数字鸿沟领域另一重要议题。

第三道沟：知识沟/能力沟

数字鸿沟的第三道鸿沟是指不同的国家或地区在获取并使用信息通信技术之后对其产生的社会影响存在差异。[128]从民主政治角度而言，不同国家或地区利用信息影响公众生活的程度存在较大区别。[129]从信息内容和经济发展角度而言，第三道鸿沟囊括了信息内容层面的差异以及信息通信技术对社会经济发展的差异。[130]在数字经济快速发展的背景下，各国之间试图将信息通信技术与本国产业相结合实现数字化转型从而发展数字经济，但是国家间利用信息通信技术发展经济的能力存在差距。此外，在信息通信技术的研发投入方面，发达国家投入的支出占 GDP 比重超 2%，而部分发达国家支出比例低于 2%。[131]发达国家与发展中国家在知识沟层面差距十分明显。随着全球数字化程度的不断加深，第三道鸿沟成为复杂的社会现象，逐渐引起重视。

1.2 全球数字鸿沟现象趋势

随着信息技术的不断发展，信息通信技术在全球的应用反而有加剧数字鸿沟的趋势。从基础设施来看，5G 时代来临，根据国际电信联盟报告显示，不同区域 5G 网络覆盖率差异较大。在参与了经合组织的国家中 5G 网络覆盖率已经达到 34%，然而在亚太地区这一指标则下降至 15%，在拉丁美洲这一指标继续下降至 3.2%，更为鲜明的对比是，在撒哈拉以南非洲地区这一指标数据为零。显然，虽然 5G 基础设施还没有全面铺开，目前在不同发展水平的国家里 5G 基础设施的覆盖率已经开始出现较大的差距。[132]

此外，受 2020 年新冠疫情影响，数字经济迎来重大的发展机遇，全球数字化程度不断加深。根据国际电信联盟发布的《衡量数字化发展：2020 年事实与数字》报告中显示：由于疫情的影响，在疫情防控期间，数字化进程加快，民众行为发生改变，线上消费次数显著增加，但与此同时全球数字鸿沟现象并没有得到改善，发达国家与不发达国家之间的差距更为明显。[133]由于经济水平存在较大差距，获取和使用信息通信技术水平差距大等多方面因素综合作用，数字化进程帮助有效抗击疫情的同时也加剧了数字化不平等的现象，南北国家之间的差距进一步加深。

因此，为了促进国际社会的友好协作和全球数字经济的协调发展，帮助全球处于各个发展阶段的国家抓住数字经济发展机遇，促进不同国家平等发展，全球数字鸿沟现象亟待解决。

2. 当前全球数字鸿沟治理

2.1 当前全球数字鸿沟治理目标

经济目标

从经济层面而言，全球数字鸿沟治理的首要目标在于消除各国获取以及使用信息通信技术的差距。首先，为了消除各国获取信息通信技术的差距须保障全球范围内各个国家或者地区能够获得普遍的信息接入。从 20 世纪 80 年代开始，国际经济合作开发组织提出“普遍

服务”的概念，这一概念指的是在全球范围内的任何地点，公众都应该得到依据其经济条件能够负担得起的电信服务，从而实现信息通信技术的接入层面的公平。[134]其次，为了消除各国使用信息通信技术的差距须促进全球范围内不同使用者使用信息通信技术水平提高。国际组织积极呼吁提高人们使用 ICT 的技能水平，各国政府也积极响应号召，例如 2020 年欧盟推出《欧洲技能议程》旨在为成年人提供信息通信技术的培训，[135]新加坡政府也提出了再教育计划为人们提供相关培训。[136]此外，全球数字鸿沟治理的目标不仅仅在于技术本身，而是要利用技术促进经济的和谐发展，2020 年国际电信联盟就曾经提出“连通目标 2030：利用 ICT 促进可持续发展目标(SDG)的实现”，[137]建议各个国家利用信息通信技术实现和谐发展。

民主目标

从民主层面而言，全球数字鸿沟治理的目标主要在于通过扩大信息通信技术的应用范围帮助发展中国家实现民主政治。由于网络空间的不断扩张及其传播的内容具有多样性、可访问性、用户积极创造内容等多个方面的特征，国际社会认为广泛应用信息通信技术能够帮助充分保障民众的知情权、促进政府部门的信息公开。[138]总而言之，全球数字鸿沟治理在民主政治层面致力于充分利用网络传播的特性，改良政府与民众之间信息不对称问题，进而帮助对抗独裁与专政实现民主政治。

2.2 当前治理体制

目前现有的全球数字鸿沟治理尚不完善，不能够真正弥合全球数字鸿沟。从国际层面而言，当前全球数字鸿沟治理主要是通过国际组织的积极倡议来推进，而国际层面全球数字鸿沟治理聚焦于提高发展中国家获取和使用 ICT 水平，同时关注加强发达国家与发展中国家之间的合作。从国家层面而言，首先各个国家积极尝试通过多种途径提高本国信息技术水平，但是各国发展 ICT 的能力存在差异，各国发展国内信息技术产业的措施反而可能扩大了国际数字鸿沟。其次，以西方发达国家为主的国家层面的对外技术援助并没有真正解决发展中国家的技术落后、信息化水平不高等问题。

国际组织的积极尝试

一直以来国际组织都在进行促进数字鸿沟问题的国际治理的积极尝试，早在二十一世纪初日本冲绳八国会议召开时，会议发表的《全球信息社会冲绳宪章》就提出发展信息社会，缩小信息技术差距。[139]继而，在八国集团首脑会议上世界经济论坛组织提出主题为《从全球数字鸿沟到全球数字机遇》的建议书，提出要缩小国家之间以及国家内部获取和使用信息技术水平，消除数字鸿沟。[140] 区域组织也进行了一些积极尝试，例如 2001 年上海 APEC 年会的部长级会议通过了《数字 APEC 战略》，文件中提出 APEC 成员国之间应增加合作，进一步提高信息通信技术水平，促进数字鸿沟治理。

联合国也关注到数字鸿沟的问题。早在 2001 年联合国就成立了联合国信息和通信技术工作组，尝试利用全球力量协助治理数字鸿沟，为全球经济发展提供基础的信息技术条件。[141]之后在国际电信联盟的积极倡议下，2003 年联合国召开了首届信息社会首脑峰会，会议总共分为日内瓦峰会与突尼斯峰会两个阶段。之后在世界信息社会首脑峰会中提出了“消除数字鸿沟作为人类构建和谐信息社会的最终目标”，日内瓦会议最终形成日内瓦《原则宣言》《行动计划》文件，主旨在于提高各国信息技术水平，进而消除数字鸿沟。[142]在 2005 年的突尼斯阶段会议上，各成员国在“全球数字团结基金”上达成一致，但最终为缩小国际数字鸿沟募集资金主要来自于发展中国家。突尼斯峰会最后通过了《突尼斯承诺》和《突尼斯信息社会议程》，重点探讨了解决数字鸿沟问题面临的挑战。[143]

现有的数字鸿沟治理的国际社会规则在国际法层面通常不具备法律约束力，没有约定具体的权利义务内容。以日内瓦《原则宣言》《行动计划》以及《突尼斯承诺》和《突尼斯信息社会议程》为典型代表，这些规则不具备法律约束力，但是显示了解决数字鸿沟问题的一般方向，对于数字鸿沟问题引起广泛重视，促进信息通信技术的使用具有重要意义，是解决这些问题的良好开端。国际组织通过发布报告提出信息技术使用具体的衡量指标，成立特别工作小组落实各国政府的行动，国际组织的成员国之间加强战略合作以及成立专项基金募集资金等多种方式积极促进数字鸿沟问题的解决。但是显而易见，国际社会并没有就数字鸿沟问题达成一致意见，没有强有力的完整体系化治理框架推进问题解决。

国家内部提高信息化水平的尝试

各国消除国内数字鸿沟的努力反而进一步扩大数字鸿沟。各个国家提高信息化水平的能力有所差别，在原有的不同信息化水平基础上，各国尝试改善国内数字鸿沟的努力可能进一步扩大国家之间的信息化差距。以发达国家为例，欧盟发布“数字欧洲计划”“创建数字社会”等计划措施旨在消除欧盟地区内部的数字鸿沟，提高欧盟信息化水平，建设信息化社会；日本政府提出“建设高速信息通信网络社会基本法案”促进国内信息网络建设；韩国则发布网络韩国 21 世纪”战略加强国内网络建设。与此同时，发展中国家也在作出改善信息通信技术水平的努力，例如印度大力发展软件业、墨西哥政府投入 200 亿墨西哥比索改善基层地区金融和电信业务服务以及 100 亿比索加强电信基础设施的建设改善国内偏远地区的电信服务[144]。然而，数字经济产业具有资本密集和技术密集型的特征，相比于发达国家，受到资金短缺和技术水平制约发展中国家消除数字鸿沟的努力大打折扣。因此，各国消除国内数字鸿沟的努力反而造成全球数字鸿沟更加严重。[145]

此外，国家内部积极提高信息化水平的尝试可能对国际社会产生辐射影响，美国是其中的典型代表。90 年代开始，美国对信息基础设施建设提出了一系列的倡议并采取了一系列的行动。90 年代初期克林顿政府提倡建设国家信息基础设施（NII），随后开始号召各国共同建设全球信息基础设施（GII），之后西方七国集团在北约总部确定成立了“全球信息基础设施委员会”。[146]在国内法律层面，1996 年克林顿采取措施，签署了《电信法》利用法律手段支持国家信息基础设施建设。紧接着，美国陆续提出一系列发展信息技术和信息基础设施建设的战略与计划，例如“数字地球”战略、“下一代互联网计划”、“宽带技术技术机遇计划”、“国家宽带计划”以及“数字素养行动”等。除此以外，美国还综合利用税收、财政、金融等多种经济方面手段全面帮助壮大信息基础设施市场，促进其发展。[147]通过一系列国际倡议与国内政策，美国提高了发展信息基础设施建设的战略意义，大力提高了国内信息基础设施建设水平。同时由于美国掌握信息通信领域的先进科技，美国占据了与信息技术相关的国际市场上制定规则、标准制定主导权，实际上成为了全球范围内信息基础设施领域的领导者。

国家层面弥合全球数字鸿沟措施

1.美国对外技术援助

国际技术援助是国家对外援助中一种特殊形式。在美国历史上曾经多次实施对外援助计划，其中最有名的是对欧洲进行援助的马歇尔计划。国际技术援助是南北关系中重要议题，美国长期掌握着先进的信息通信技术，国际技术援助的重要性也在不断提高。[148]为解决全球数字鸿沟问题，信息通信技术的援助包含在美国对外技术援助中。

美国对非洲的技术援助是美国对外提供技术援助的重要代表。美国对非洲的援助开始于 1949 年杜鲁门总统提出《援助落后地区经济开发计划》，之后肯尼迪总统签署了《对外援助法案》，初步构建起美国对外援助的法律框架。[149]二十世纪八十年代初期，在该法案的指导下，美国成立了美国贸易发展署，在信息通信领域与非洲开展合作。2003 年美国通过了《千年挑战法》，依据该法成立了“千年挑战公司”，对非洲提供技术援助，具体合作内容中涉及信息化建设领域。[150]此外，1961 年美国还通过《和平队法》，该法案促进了美国与非洲地区国家在非政府层面的国家合作，并通过信息技术知识传播与培训提高非洲地区使用信息通信技术的能力。

美国帮助治理全球数字鸿沟现象的手段主要是通过对外提供技术援助，而这种技术援助通常通过国际经济贸易的合作以及科技文化知识传播与培训实现。整体而言，美国对外技术援助呈现规范化、法制化、体系化的特点，美国对外提供技术援助通常通过法案构建初步框架。另一方面，美国对外技术援助通常采取与市场相结合的方式，通过经贸合作往来实现，或组建公司或推动跨国公司与发展中国家开展业务往来，例如在“数字化领导计划”推动下，微软公司在印度、韩国等国家出资以促进全球数字鸿沟问题消弥。[151]

2.中国“数字丝路”的提出

2015 年，第二届世界互联网大会分论坛提出“ 数字丝路·合作共赢”，多家机构共同签署“数字丝路”建设联盟意向书。2017 年，习近平书记在“一带一路”高峰合作论坛上首次正式提出“数字丝绸之路”。同年在第四届世界互联网大会上，中国与老挝、沙特、塞尔维亚、泰国、土耳其、阿联酋等多个国家共同发起《“一

带一路”数字经济国际合作倡议》，倡议中明确提出各国要采取多种政策措施和技术手段来缩小数字鸿沟，包括各国之间和各国之内的数字鸿沟，大力推进互联网普及。2019 年第二届“一带一路”高峰合作论坛上，习近平总书记再次强调建设“数字丝绸之路”。

“数字丝路”依托“一带一路”政策，在中国政府大力支持鼓励下，以信息网络技术为抓手，中国国内电信运营商以及互联网高新技术企业为主力，从基础设施建设、电子商务平台建设以及智慧城市工程三条路径开展与“一带一路”沿线国家开展广泛的合作，积极促进数字鸿沟问题解决，开展数字经济，促进经贸往来且为文化交流奠定基础。[152]“数字丝路”不仅仅有助于提高发展中国家信息通信水平落后，对于突破南北国家之间的信息发展水平差距具有重要意义，有助于缩小全球发展差距。[153]“数字丝路”以信息通信技术为基础，发展数字经济为依托，是沿线国家真正实现可持续发展重要路径。

2.3 全球数字鸿沟治理难题

全球数字鸿沟治理的难题存在于多方面。首先，因各国发展能力有异，各国消除国内数字鸿沟的努力反而进一步扩大数字鸿沟。其次，ICT 水平关系到国际之间的综合国力竞争。信息网络技术是经济发展的重要动力，数字经济是信息社会国与国之间主要竞争内容。2019 年中美之间开展贸战，美国对华科技公司进行限制，其中焦点在于 5G 基础设施建设。作为新一代信息基础设施建设的核心，5G 建设面临激烈的国际竞争。[154]最后，由于知识产权问题以及技术进出口壁垒对于技术在不同国家地区之间流动的限制，影响了国家间信息通信技术合作。以中美为例，美国逐步开展与中国之间高新技术领域科技脱钩[155]，同时在知识产权领域加强管控信息通信技术[156]。

综上，各国依靠自身力量难以消除数字鸿沟，在国际竞争与合作壁垒甚至加剧了全球数字鸿沟治理。当前的国际格局下难以实现全球正义，真正解决全球数字鸿沟问题。

3. 本篇小结

自20世纪80年代提出数字鸿沟的概念以来，国际社会一直号召各国积极采取行动消除全球数字鸿沟以促进全球平衡发展，但是实际效果并未达到预期。随着经济和技术不断发展，全球信息基础设施建设水平不断提高，但数字鸿沟现象不但没有减轻反而逐步产生使用能力差距，与各国产业结合程度差距等更深层级的鸿沟。信息通信技术及数字经济是当前国家间关键竞争领域，数字鸿沟现象关系到国家政治经济影响力，依靠西方资本主义国家出于自身利益考量的对外技术援助不可能真正有效治理数字鸿沟。中国提出的人类命运共同体理念是实现全球正义新方案，同时加强数字经济合作促进发展中国家数字化转型，是推动全球数字鸿沟问题解决重要路径。

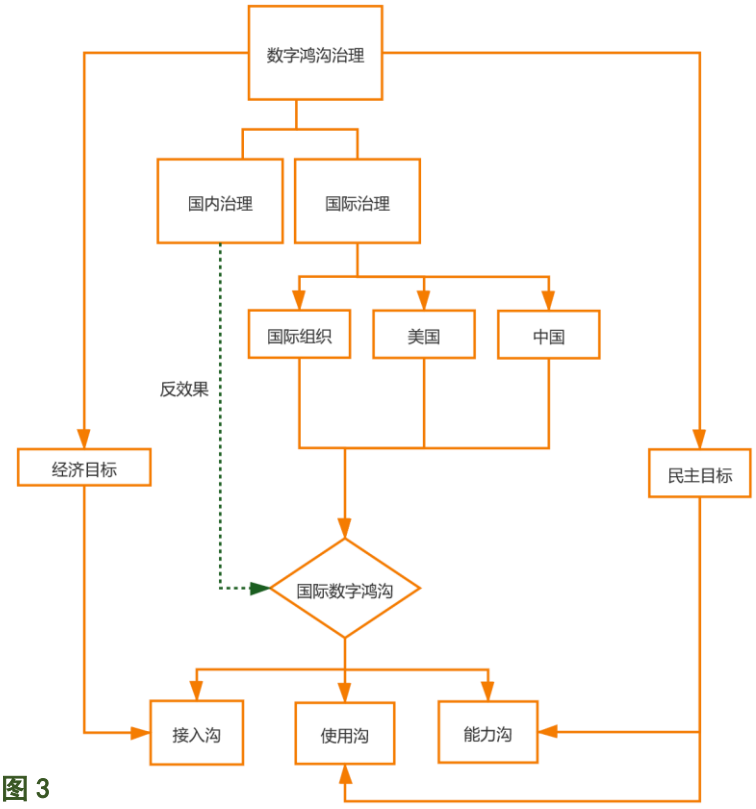


图3

结语

网络空间国际治理是一个重大而复杂的课题。谁来治理，治理什么，用什么治理，在政治、经济、文化、法律、技术等多维度呈现出不同面向。后疫情时代，国际社会各个领域面临前所未有之变局，网络空间谱写人类社会与科学技术的双重变奏，显得尤为复杂。如何搁置争议，促进网络空间安全和谐有序发展，让全人类共享技术发展的福祉，是全人类面对的共同问题，也是网络空间国际治理研究的方向。

希望本报告的梳理，能为以此为志业的同仁们提供有益参考，为网络空间国际治理的“推陈出新”和“吐故纳新”贡献微薄力量！

面向 IPv6 的网络空间国际治理联合研发与示范课题组发布

清华大学法学院子课题组撰写

二〇二一年 七月

地址：北京市海淀区清华园
邮编：10001
电话：010－62782800
邮箱：wangye20@mails.tinghua.edu.cn

参考文献

[1]参见新华社："中共中央印发《法治社会建设实施纲要（2020－2025 年）》"，中国政府门户网站，<http://www.gov.cn/zhenGGE/2020-12/07/content_5567791.htm>，最后访问日期 2020 年 12 月 14 日。
[2] "四项原则"和"五点主张"，参见"习近平在第二届世界互联网大会开幕式上的讲话（全文）"，中国政府门户网站，<http://www.gov.cn/xinwen/2015-12/16/content_5024712.htm>，最后访问日期 2020 年 11 月 30 日。
[3] "《倡议》文件"指《携手构建网络空间命运共同体行动倡议》。"四个共同理念"指"发展共同推进、安全共同维护、治理共同参与、成果共同分享"的理念。"五个共同体"指"把网络空间建设成为造福全人类的发展共同体、安全共同体、责任共同体、利益共同体"。参见"世界互联网大会组委会发布《携手构建网络空间命运共同体行动倡议》"，中国国家互联网信息办公室网站，<http://www.cac.gov.cn/2020-11/18/c_1607269080744230.htm>，最后访问日期 2020 年 11 月 30 日。
[4] 刘晗,叶开儒："网络主权的分层法律形态"，《华东政法大学学报》，2020 年第 4 期，第 67-82 页。
[5] [美]劳伦斯·莱斯格：《代码 2.0》，李旭等译，清华大学出版社，2009 年第 1 版，第 10 页。
[6] Powell, Walter W., B. Staw, and L. L. Cummings. "Neither market nor hierarchy." (1990): 104-117.
[7] Benkler, Yochai. *The wealth of networks: How social production transforms markets and freedom*. Yale University Press, 2006.
[8] [美]弥尔顿·穆勒：《网络与国家：互联网治理的全球政治学》，周程等译，上海交通大学出版社，2015 年第 1 版，第 44 页。
[9] ISP 与 ICP 二分，前者指互联网服务提供方（Internet Service Provider），后者指互联网内容提供方（Internet Content Provider）。
[10] 如上，第 52 页。
[11] Visner, S. S. (2009). Information Technology's Challenges to Global Governance. *World Politics Review (19446284)*, 6-6.
[12] 李丹："互联网技术漫谈（三）：互联网与电信网有什么不同"，"亚太网络研究 APNet"微信公众号，2020 年 4 月 12 日，<https://mp.weixin.qq.com/s/GRm0186Cnl-U-2F4k7OUEA>，2020 年 12 月 14 日访问。
[13] 潘龙飞，周程："网络化与全球化——《网络与国家》导读"，载于[美]弥尔顿·穆勒：《网络与国家：互联网治理的全球政治学》，周程等译，上海交通大学出版社，2015 年第 1 版，第 4 页。
[14] 同上，第 3 页。
[15] Benkler, Yochai. The wealth of networks: How social production transforms markets and freedom. Yale University Press, 2006.
[16] Fidler, D. P. (2015). Sidetracked: Obama's Cybersecurity Legacy. *World Politics Review (19446284)*, 1-9. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=wpr&AN=111745327&lang=zh-cn&site=ehost-live.
[17] [美]弥尔顿·穆勒：《网络与国家：互联网治理的全球政治学》，周程等译，上海交通大学出版社，2015 年第 1 版，第 84-88 页。
[18] 如上，第 88 页。
[19] Fidler, D. P. (2015). Sidetracked: Obama's Cybersecurity Legacy. *World Politics Review (19446284)*, 1-9. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=wpr&AN=111745327&lang=zh-cn&site=ehost-live.
[20] Goldberg, C. (2020). To Counter China Online, Regulate Big Tech. *World Politics Review (19446284)*, 1-4. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=wpr&AN=145401978&lang=zh-cn&site=ehost-live.
[21] Rondeaux, C. (2020b). Why Diplomacy Matters as Much as Defense When It Comes to Cybersecurity. *World Politics Review (19446284)*, 1-5. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=wpr&AN=146053369&lang=zh-cn&site=ehost-live.
[22] Ruohonen, J., Hyrynsalmi, S., & Leppänen, V. (2016). An outlook on the institutional evolution of the European Union cyber security apparatus. *Government Information Quarterly, 33*(4), 746-756. doi:10.1016/j.giq.2016.10.003.

[23] “On July 16, 2020, the Court of Justice of the European Union issued a judgment as……the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States.” On privacyshield.gov, accessed on 13 November 2020.

[24] Blinken, A. J. (2001). The false crisis over the Atlantic. *European opinion about, and relations with, United States, 80*(3), 35-48. doi:10.2307/20050149.

[25] Blinken, A. J. (2002). Winning the war of ideas. *Washington Quarterly, 25*(2), 101-114. doi:10.1162/01636600252820162.

[26] Asmus, R. D., Blinken, A., & Gordon, P. H. (2005). Nothing to Fear: Washington Should Embrace the European Union. *Discussion of Jeffrey L. Cimbalo, Saving NATO from Europe, 84*(1), 174-177. doi:10.2307/20034218.

[27] Grigsby, A. (2018). The United nations doubles its workload on cyber norms, and not everyone is pleased. *Council on Foreign Relations*. <https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased> accessed on 3 December 2020.

[28] Ibid.

[29] “中华人民共和国和俄罗斯联邦外交部长联合声明”，中华人民共和国外交部网站，<http://new.fmprc.gov.cn/web/wjbzhd/t1814218.shtml>，最后访问日期为 2020 年 12 月 3 日。

[30] 黄志雄：“2020 年上半年联合国信息安全工作组进程网络空间国际规则博弈”，《中国信息安全》2020 年第 69 期，第 68-71 页。

[31] Ibid.

[32] 英格玛·斯纳比里：“联合国政府专家组 ICT 工作进展概览”，《中国信息安全》2019 年第 9 期，第 42 页。

[33] Klein, Hans. "Understanding WSIS: An institutional analysis of the UN World Summit on the Information Society." *Information Technologies & International Development* 1.3 (2004): pp-3.

[34] 关键互联网资源（CIR）指对域名系统（DNS）以及互联网协议地址（IP）的治理，以及对根区服务器系统、技术标准、对等操作、互联、通信基础设置以及多语话的治理。

[35] Mueller, Milton L. *Ruling the root: Internet governance and the taming of cyberspace.* MIT press, 2009.

[36] [美]弥尔顿·穆勒：《网络与国家：互联网治理的全球政治学》，周程等译，上海交通大学出版社，2015 年第 1 版，第 76 页。

[37] Keane, John. *Global civil society?*. Cambridge University Press, 2003.

[38] [美]弥尔顿·穆勒：《网络与国家：互联网治理的全球政治学》，周程等译，上海交通大学出版社，2015 年第 1 版，第 102-103 页。

[39] 如上，第 129-188 页。

[40] Tarrow, Sidney. "Transnational politics: Contention and institutions in international politics." *Annual review of political science* 4.1 (2001): 1-20.

[41] [美]弥尔顿·穆勒：《网络与国家：互联网治理的全球政治学》，周程等译，上海交通大学出版社，2015 年第 1 版，第 60 页。

[42] 如上，第 132 页。

[43] Dimitrov, Radoslav S. "Hostage to norms: states, institutions and global forest politics." *Global environmental politics* 5.4 (2005): 1-24.

[44] 如上，第 151 页。

[45] “GAFA”是谷歌(Google)、苹果(Apple)、脸书(Facebook)和亚马逊(Amazon)这美国四大互联网巨头企业的缩写。“BAT”是百度（Baidu）、阿里巴巴（Alibaba）和腾讯（Tencent）这中国三大互联网巨头企业的缩写。

[46] Mutual Legal Assistance Treaties (MLAT).

[47] Stored Communication Act (SCA), part of the Electronic Communications Privacy Act.

[48] *Microsoft Corp. v. United States* (In re：A Matter of Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation), 829 F.3d 197 (2016).

[49] U.S. v. Microsoft Corp., 138 S.Ct. 1186 (2018).

[50] [美]布拉德·史密斯，卡罗尔·布朗：《工具，还是武器？》，杨静娴等译，中信出版集团，2020 年第 1 版，第 51-54 页。

[51] 《网络空间信任和安全巴黎倡议》(Paris Call for Trust and Security in Cyberspace，2018)。

[52] “基督城呼吁”峰会上，17 个国家、8 家科技行业巨头加入新西兰主导的“消除网络恐怖主义和暴力极端主义”的行动。Facebook 发布了声明，解决监管机构的担忧，阻止有害内容在其网络上的传播。摘自工业和信息化部网络安全威胁信息共享平台，2019 年 5 月 16 日。

[53] Ex. Or. No. 13925 of May 28, 2020, 85 Fed. Reg. 34079.

[54] Knight First Amendment Inst. at Columbia Univ. v. Trump, 953 F.3d 216, 2020 U.S. App. LEXIS 9025.

[55] Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

[56] Ark. Educ. Tv Comm'n v. Forbes, 523 U.S. 666, 118 S. Ct. 1633 (1998).
[57] Boyle, James. "A politics of intellectual property: Environmentalism for the net." *Duke Law Journal* 47 (1997): 87.
[58] 多元规制分为法律，准则，市场，架构。参见[美]劳伦斯·莱斯格：《代码 2.0：网络空间中的法律》，李旭等译，清华大学出版社，2017 年修订版，第 138 页。
[59] Goldberg, C. (2020). To Counter China Online, Regulate Big Tech. *World Politics Review* (19446284), 1-4. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=wpr&AN=145401978&lang=zh-cn&site=ehost-live.
[60] Meaker, M. (2020). How Hackers Are Seizing on COVID-19 and Hampering the Global Response. *World Politics Review (19446284)*, 1-5. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=wpr&AN=143082287&lang=zh-cn&site=ehost-live.
[61] Mueller, M. (2009). Internet Content Regulation and the Limits of Sovereignty. *World Politics Review* (19446284), 5-5. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=wpr&AN=44065041&lang=zh-cn&site=ehost-live.
[62] Bambauer, Derek E. "Cybersieves." *Duke law journal* (2009): 377-446.
[63] Bradshaw, S., & DeNardis, L. (2018). The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom. *New Media & Society*, 20(1), 332-350. doi:10.1177/1461444816662932
[64] 问题在于，“旧瓶”的国际条约与国际惯例（customary）涉及到缔约方的多边主义是否适用于多方主义的网络治理场景，以及网络发展不对称与数字鸿沟下发展中国家是否享有对网络场景国际惯例的“持续反对”能力与权利。参见 Kittichaisaree, Kriangsak. *Public international law of cyberspace*. Vol. 32. Cham: Springer, 2017.
[65] 刘小燕,崔远航：《网络安全规则与国际话语权角力——基于犯罪与恐怖主义维度的阐释》，载《新闻大学》2019 年第 7 期，第 33 页。
[66] 张豫洁：《评估规范扩散的效果——以〈网络犯罪公约〉为例》，载《世界经济与政治》2019 年第 2 期，第 90 页。
[67] 裴炜：《网络犯罪治理国际合作：机制、主题与展望》，载《中国信息安全》2020 年第 9 期，第 81 页。
[68] 胡健生,黄志雄：《打击网络犯罪国际法机制的困境与前景——以欧洲委员会<网络犯罪公约>为视角》，载《国际法研究》2016 第 6 期。
[69] 《公约》第 2 条至第 10 条进一步列举了四类九种网络犯罪行为，分别是: (1)侵犯计算机数据或系统的机密性、完整性及可用性的犯罪：包括非法访问、非法截获、数据干扰、系统干扰和设备滥用五种犯罪类型; (2)与计算机有关的犯罪：包括与计算机有关的仿造罪、与计算机有关的欺诈罪; (3)与内容有关的犯罪：指与儿童色情有关的犯罪; (4)与侵犯版权和邻接权有关的犯罪。
[70] Council of Europe，Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems，January 28，2003.
[71] Cybercrime Convention Committee（T-CY），http://www.coe.int/en/web/cybercrime/tcy
[72] Cybercrime Programme Office (C-PROC) ，http://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-
[73] 吴海文、张鹏：《打击网络犯罪国际规则的现状、争议和未来》，载《中国应用法学》2020 年第 2 期，第 192 页。
[74] Mexico - Measures Affecting Telecommunications Services, Report of the Panel, para. 7.45.
[75] 石静霞,张舵：《跨境数据流动规制的国家安全问题》，载《广西社会科学》2018 年第 8 期，第 129 页。
[76] 石静霞,张舵：《跨境数据流动规制的国家安全问题》，载《广西社会科学》2018 年第 8 期，第 129 页。
[77] 石静霞：《数字经济背景下的 WTO 电子商务诸边谈判：最新发展及焦点问题》，载《东方法学》2020 年第 2 期，第 172 页。
[78] 就第一次修改而言，《关于信息、信息技术和信息保护法》(第 149 号法令) 在互联网信息传播组织义务项下增加了境内存储的相关要求，文本规定：网民在对文字、图像以及语音等各种信息进行发送、接收以及处理的过程中，互联网信息传播组织者应将上述信息留存于俄罗斯境内。此外，还声明互联网企业在国家机构进行调查时积极配合的义务，否则将处以行政罚款。第二次修改则在第 149 号法令第 16 条第 4 款中增加数据控制者与数据处理者对于存储、处理俄罗斯公民信息的数据库应留存在俄罗斯境内的规定。《俄罗斯联邦个人数据法》(第 152 号法令)第 18 条增加第 5 款，运营商获取信息需要使用俄罗斯本地的数据库，且需确保数据主体的知情权。
[79] 何波：《俄罗斯跨境数据流动立法规则与执法实践》载《大数据》2016 年第 7 期，第 131 页。
[80] 参见 APEC 跨境隐私规则（CBPR）网站。http://cbprs.org/compliance-directory/cbpr-system/。
[81] 史佳颖：《APEC 数字经济合作评估及中国的参与策略》，载《亚太经济》2021 年第 2 期，第 10 页。
[82] 廖雪娟：《跨境个人数据流通规制路径分析及启示》华东政法大学 2017 年硕士生学位论文。
[83] 在实践层面，目前只有 11 个国家和地区获得充分性保护认证：包括加拿大、阿根廷、瑞士、安道尔、法罗群岛、泽西岛、马恩岛、根西岛、新西兰、以色列、乌拉圭东岸共和国。

[84] Article 45 of GDPR, https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en
[85] 马蒂亚斯·鲍尔等：《数据本地化的代价：经济恢复期的自损行为》，载《汕头大学学报（人文社会科学版）》2017 年第 5 期，第 45 页。
[86] 刘晗、叶开儒：《网络主权的分层法律形态》，载《华东政法大学学报》2020 年第 4 期，第 76 页。
[87] 刘晗、叶开儒：《网络主权的分层法律形态》，载《华东政法大学学报》2020 年第 4 期，第 76 页。
[88] 刘晗、叶开儒：《网络主权的分层法律形态》，载《华东政法大学学报》2020 年第 4 期，第 76 页。
[89] 王甜甜：《联合国网络空间治理机制有效性研究》，载《上海社会科学院》2018 年，第 18 页。
[90] 刘晗、叶开儒：《网络主权的分层法律形态》，载《华东政法大学学报》2020 年第 4 期，第 76 页。
Milton Mueller, Networks and States: The Global Politics of Internet Governance, The MIT Press, 2013, p.63.
[91] 刘晗、叶开儒：《网络主权的分层法律形态》，载《华东政法大学学报》2020 年第 4 期，第 77 页。
[92] 王甜甜：《联合国网络空间治理机制有效性研究》，载《上海社会科学院》2018 年，第 19 页。
[93] 王甜甜：《联合国网络空间治理机制有效性研究》，载《上海社会科学院》2018 年。
ITU: Final Facts of Plenipotentiary Conference, 2014，available at
https://www.itu.int/en/plenipotentiary/2014/Documents/final-acts/pp14-final-acts-en.pdf
[94] 罗锦莉：《移交互联网域名管理权或是“虚晃一枪”》，载《金融科技时代》2016 年第 11 期，第 88 页
[95] NTIA：“NTIA Announces Intent to Transition Key Internet Domain Name Functions”（March 14，2014）
https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions
[96] 多方利益相关者：
[97] 王甜甜：《联合国网络空间治理机制有效性研究》，载《上海社会科学院》2018 年。
[98] 参见刘晗、任启明：《简析如何在 ICANN 新机制下维护我国网络主权》，载《中国信息安全》2017 年第 5 期。
[99] ICANN: “Empowered Community”, icann.org/zh/ec.；
其中“escalation process”在中文页面中翻译为“升级流程”，此处理解为与“bottom-up process”同义，译为“自下而上的流程”
[100] 刘晗、任启明：《简析如何在 ICANN 新机制下维护我国网络主权》，载《中国信息安全》2017 年第 5 期，第 44 页
[101] ICANN: “Empowered Community”, icann.org/zh/ec.
[102] 鲁传颖：“国际空间国际规则体系与中美新型大国关系”，上海国际问题研究院全球治理研究所
[103] 刘晗、任启明：《简析如何在 ICANN 新机制下维护我国网络主权》，载《中国信息安全》2017 年第 5 期，第 45 页
[104] Becker, M. (2019), When public principals give up control over private agents: The new independence of ICANN in internet governance. Regulation & Governance, 13: 561-576. available at:
https://doi.org/10.1111/rego.12250
[105] Mueller 2017，p. 146 qtd. in Becker, M.p572.
[106] 王甜甜：“联合国网络空间治理机制有效性研究”，《上海社会科学院》2018 年
[107] 崔淑田、刘越：“DNSSEC 技术发展及影响分析”，《电信科学》，2012 年第 9 期，第 100-105 页
[108] 同前注[106]，崔淑田、刘越书，第 100-105 页
[109] 胡宁、邓文平、姚苏：“互联网 DNS 安全研究现状与挑战”，《网络与信息安全学报》，2017 年 3 月，第 3 期，第 13-21 页
[110] 段海新：2019 年北京网络安全大会宣讲

[111] 同前注[106]，崔淑田、刘越书，100-105 页
[112] David Conrad, ICANN Office of the Chief Technology Officer: “DNSSEC：Securing the DNS”，24 July 2020, available at:
https://www.icann.org/zh/system/files/files/octo-006-24jul20-en.pdf
[113] Chandramouli R， Rose S. Open issues in secure DNS deployment. IEEE Security and Privacy, 2009，7(5):29~35
[114] 张子蛟、高金峰、王炯炜、胡宏伟：《DNSSEC 部署:山雨欲来风满楼》，载《中国教育网络》2010 年 6 月刊。
[115] David Conrad, ICANN Office of the Chief Technology Officer: “DNSSEC：Securing the DNS”，24 July 2020，available at: https://www.icann.org/zh/system/files/files/octo-006-24jul20-en.pdf
[116] 2018 年 11 月，总部位于美国的中国电信公司发布了一系列 Google 地址。报道可见:
https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/;2019 年 5 月，由台湾网络信息中心（TWNIC）运营的公共 DNS 的流量被劫持到巴西的一个实体(AS268869)。报道可见
https://www.manrs.org/2019/05/public-dns-in-taiwan-the-latest-victim-to-bgp-hijack/.
[117] David Conrad, ICANN Office of the Chief Technology Officer: “DNSSEC：Securing the DNS”，24 July

2020,available at:
https://www.icann.org/zh/system/files/files/octo-006-24jul20-en.pdf
[118] 同前注[108]， 胡宁、邓文平、姚苏书，第 13-21 页
[119] 同前注[106]，崔淑田、刘越书，第 100-105 页。
[120] 刘小燕,崔远航:《网络安全规则与国际话语权角力——基于犯罪与恐怖主义维度的阐释》，载《新闻大学》2019 年第 7 期，第 32 页。
[121] 熊光清:《全球互联网治理中的数字鸿沟问题分析》，载《国外理论动态》2016 年第 9 期，第 82 页。
[122] 胡鞍钢、周绍杰:《新的全球贫富差距:日益扩大的"数字鸿沟"》，载《中国社会科学》2002 年第 3 期，第 34 页。
[123] 张正平、卢欢:《数字鸿沟研究进展》，载《武汉金融》2020 年第 3 期，第 64 页。
[124] 国际电信联盟:《2017 年衡量信息社会报告》。
[125] 邱泽奇,张樹沁,刘世定,许英康:《从数字鸿沟到红利差异——互联网资本的视角》，载《中国社会科学》，2016 年第 10 期，第 93 页。
[126] 薛伟贤,王亚文:《弥合数字鸿沟 推动数字经济发展》，载《西安日报》，2020 年第 8 期。
[127] Paul DiMaggio and Eszter Hargitai，" From the' Digital Divide' to Digital Inequality: Studying Internet Use As Penetration Increases，" Working Paper 15，Princeton University，Center for Arts and Cultural Policy Studies，Princeton，NJ，2001.
[128] 韦路,张明新:《第三道数字鸿沟:互联网上的知识沟》，载《新闻与传播研究》，2006 年第 4 期，第 43 页。
[129] NORRIS P. Digital Divide: Civic Engagement，Information Poverty，and the Internet World Wide[M]. New York: Cambridge University Press，2001.
[130] PETYAC，FREDERICOCJ，TIAGOO，et al. Digital Divide at Individual Level: Evidence for Eastern and Western European Countries[J]. Government Information Quarterly，2018，35(3):460-479.
[131] 薛伟贤,王亚文:《弥合数字鸿沟 推动数字经济发展》，载《西安日报》，2020 年第 8 期。
[132] https://baijiahao.baidu.com/s?id=1685468703333340494&wfr=spider&for=pc，最后访问于 2021 年 5 月 18 日。
[133] 国际电信联盟:《衡量数字化发展：2020 年事实与数字》。
[134] 国际经济合作开发组织:《普遍服务和电信资费改革》。
[135] https://www.sohu.com/a/441137952_162522， 最后访问于 2021 年 5 月 18 日。
[136] https://www.sohu.com/a/414060447_670057 ，最后访问于 2021 年 5 月 18 日。
[137] https://itu.foleon.com/itu/connect-2030-agenda/home/ ，最后访问于 2021 年 5 月 18 日。
[138] burrim. Re-conceptualizing the Global Digital Divide[J]. JIPITEC : Journal of Intellectual Property, Information Technology and E-Commerce Law, 2011, 2(3).
[139]八国会议发表《全球信息社会冲绳宪章》[N]. 人民邮电,2000-07-26(004).
[140] 佚名:《从全球数字鸿沟到全球数字机遇——向 2000 年八国集团九州—冲绳峰会提交的建议书》，社会科学文献出版社, 2002。
[141] http://news.eastday.com/epublish/gb/paper148/20020614/class014800014/hwz692352.htm ，最后访问于 2021 年 5 月 18 日。
[142] 唐岚、李艳、高瞻:《信息社会世界峰会简况》，载《国际研究参考》，2004 年第 3 期，第 1-5 页。
[143] 许祎玥、陈帅、方兴东:《信息社会世界峰会的演进历程及发展现状》，载《汕头大学学报(人文社会科学版)》2017 年第 7 期，第 27 页。
[144] https://baijiahao.baidu.com/s?id=1655053349089374905&wfr=spider&for=pc ，最后访问于 2021 年 5 月 18 日。
[145] 王玉柱:《发展中国家难跨新数字鸿沟》，载《环球时报》2018 年第 15 期。
[146] 钟义信:《国家信息基础设施(NII)浪潮与中国高速信息网络行动》，载《金融科技时代》, 1996 年。
[147] 陈文理:《美国信息基础设施发展中的政府行为及其借鉴》，载《湖北社会科学》2011 年第 1 期，第 35 页。
[148] 李萌:《全球化时代的科技外交：理论与实践》，上海交通大学 2009 年硕士生学位论文。
[149] 朱月季:《新援助格局下中国对非洲援助实践的改革路径：美国经验》，载《华中农业大学学报(社会科学版)2017 年第 1 期，第 120 页。
[150] 武涛、张永宏:《美国对非科技合作的特点：法制化、援助化与市场化》，载《亚非纵横》2012 年第 6 期，第 34 页。
[151] 邵艳丽、黄奇、朱庆华 :《国外数字鸿沟问题研究述略》，载《情报资料工作》2003 年第 4 期，第 77 页。
[152] 李海敏:《"数字丝路"与全球网络空间治理重构》，载《社会科学文摘》2020 年第 2 期，第 42 页。
[153] 方芳:《"数字丝绸之路"建设：国际环境与路径选择》，载《国际论坛》2019 年第 2 期，第 56 页。
[154] 袁钟怡、张孟媛:《技术的安全化:特朗普政府 5G 政策与中美战略竞争新态势》，载《长春大学学报》67

2020 年第 3 期，第 76 页。

[155] 李峥：《美国推动中美科技“脱钩”的深层动因及长期趋势》，载《现代国际关系》2020 年第 1 期，第 33 页。

[156] 朱雪忠、徐晨倩：《大国竞争下的美国涉华 337 调查与中国应对之策》，载《科学学研究》2020 年 09 月 22 日出版，第 1 页，https://doi.org/10.16192/j.cnki.1003-2053.20200922.002.