《学术界》(月刊)
总第307期,2023.12
ACADEMICS
No.12 Dec. 2023

网络无政府状态的诱因与治理〔*〕

赵瑞琦

(中国传媒大学　国家传播创新中心,北京　100024)

〔摘　要〕国际社会因为缺乏超越国家的权力、执法机构与税收,仍处于无政府状态,网络空间尤其如此:由于互联网本身的技术架构缺陷与文化秉性(先天之手)、网络主权的利己主义(有形之手)、科技寡头的垄断竞争(无形之手)等三重因素,叠加创新技术迅速出现与规范滞后的落差,导致全球网络空间较物理空间的无政府状态更为严重和普遍。由此导致的治理赤字较物理空间更严重,其缺乏物理隔绝的特点会使风险和威胁往往一点突破就全网流散且影响持久。为此,要通过资本驯化、政治制衡与技术向善等路径来减轻无政府状态的弊病。

〔关键词〕网络无政府状态;技术禀赋;网络主权;数字资本主义;治理合作

DOI:10.3969/j.issn.1002-1698.2023.12.010

现实当中运转的信息空间、经济空间和政治空间已经高度分离:无论是互联网的虚拟经济还是制造业的实体经济,都在穿透国界运行。多数国家网络治理都是全球场景与本地现实的博弈:资本主导穿透国界的经济空间与国家主导本国经济秩序和全球经济组织的现实,会使得全球数字治理必然处于一种规范缺失和错位的状态。

由于缺乏可以强力执法和进行税收的更高裁判者,持久的无政府状态就成为由国家构成的国际社会的特质。[1]互联网基于本身的技术架构缺陷与文化秉性、网络主权的利己主义、科技寡头的垄断竞争及创新技术迅速出现导致规范滞后等四大因素影响,使得全球网络空间的无政府状态较物理空间更为深层化,从而对网络空间治理形成持久的挑战。

一、先天之手:技术架构与文化秉性

由互联网设计者和技术规范创立者构成的技术社群所建立的促进而非控制不同节点之间数据传输效率的互联网技术规范与原则,构成了互联网运行的认知基础。由此,网络空间的原初技术架构和操作逻辑,天生就缺乏自上而下的科层制、集中式的权威管辖与治理,从而形成了网络空间无政府状态的极具韧性的关键基因。无政府主义基因,叠加传统无政府主义的当代复归、后现代主义文化的激进驱动、网络政治的迅

作者简介:赵瑞琦,传播学博士,中国传媒大学国家传播创新中心研究员、教授,主要从事网络空间治理、区域国别学研究。

〔*〕本文系教育部人文社会科学重点研究基地重大项目"国际传播的理论与规律研究"(22JJD860012)、中国传媒大学中央高校基本科研业务费专项资金资助(CUC200M01013)的阶段性成果。

猛发展以及草根阶层社会心理中反抗情绪的爆发,都促成了网络无政府主义的生成。[2]

1. 信息化的无政府主义

以首席执行官身份深度参与 Google 从硅谷创业公司到全球科技巨头过程的埃里克·爱默生·施密特(Eric Emerson Schmidt)曾表示:互联网是第一个由人类创造而人类又无法理解的事物,是迄今为止最大规模的无政府状态的实验。互联网与无政府主义的结合产生两种形态:一是传统无政府主义团体、个人运用互联网作为信息传播和活动组织的工具,即无政府主义的信息化;二是与互联网相伴相生的新式无政府主义,它强调虚拟空间的独立性,反对法律和/或技术管制,即信息化的无政府主义。

网络无政府主义基因,具有复杂而深刻的文化诱因和历史背景。治理结构反映了诞生时刻和地点的特征,互联网初期的无政府主义放任发展和技术先驱们的乌托邦思想,鼓励了早期的黑客、GNU 和 Rinux 或开放源代码运动的活动。[3]在阿帕网(Advanced Research Projects Agency Network,ARPANET)建立的 1960 年代,一些计算机先驱人物深受当时席卷西方的后工业时代的反传统、反权威的后现代激进文化浪潮的影响,形成了互联网的无政府主义文化基因。一些技术决定论者更强调:信息技术具有克服时间和空间限制的潜力,可促进信息和知识的爆炸性生产、带来社会团结,因此强烈建议自由使用互联网。

当克林顿政府在 1990 年代试图在加密技术中加入后门(即允许政府通过特定方法访问)时,赛博朋克们(the cyberpunks)领导了一场成功的战斗,[4]击败了政府的政策从而帮助建立了不受监管的密码学——一系列能够挫败政府监控的在线隐私技术。[5]赛博朋克是 1990 年代的数字活动家,大部分是自由主义者,受到了黑客伦理和反乌托邦科幻小说的影响,渗透着无政府主义,其意识形态现在影响着新一代的数字隐私活动家。不过,彼时的互联网仍"被视为'日常生活'的一部分——仅仅是现有社会系统的延伸,而不是超越线下政治和经济限制的革命媒介"。[6]

1995 年,马克·斯劳卡最早提出了"网络民主"一词,将网络与民主联系起来加以研究。约翰·巴罗在《赛博空间的独立宣言》中宣称,虚拟网络空间独立于现实空间,国家权力不能越界干预互联网。以黑客和闪客为代表的无政府主义情绪在众多网民中也都有程度不同的表现。黑客是无政府主义的极端代表,具有极大的网络和现实破坏性。闪客虽然多数只是制造恶作剧,但也带有无政府主义倾向。

这种网络自由主义思潮与文化形成以后,成为较架构与技术更深层次也更持久的影响互联网规制方向的观念因素。一切已死的先辈们的传统,像梦魇一样纠缠着活人的头脑:[7]新式的网络无政府主义秉承传统无政府主义的基本理念,强调虚拟空间的独立性,反对来自政府或其他集团的法律和技术管制。

2. 非中心化的设计架构

信息领域有很多原创性重大发明,如计算机、互联网和卫星导航等,都因投资巨大但无法确保成功而直接或间接出自政府之手:在原型设计证明可行之后,通过市场检验逐步做大并形成全球性规模和普遍性应用。

互联网的前身阿帕网,是美国国防部高级研究计划局(Defense Advanced Research Projects Agency,DARPA)推动的产物。美军在 1960 年代建设计算机网络的原因,其一是前线军队与后方计算机联网以更快、更准确地进行决策。彼时,受商业性组织、大学和研究中心希望电脑互联以共享数据思想的影响,美国军方希望能把前线的信息传输到后方的电脑中以优化决策与行动,从而可以用最迅速的行动、最有效的形式和最小的伤亡获得最大的成果。其二是期望在传统通信方式失效时,确保后方决策可以到达最前线。时值冷战高峰,为了全流程应对苏联日益庞大核武库的威胁,确保在遭受设想中的苏联第一次核打

击之后的通讯有效性，DARPA 就资助了这项可以直接或间接联系的无中心节点、去中心化的通信技术的研究。[8]

基于这种确保极端条件下通讯畅通的初衷，也由于初期用户仅限于国防机构和少数研究部门，相关技术架构研究者考虑的主要是如何促进而非控制不同节点间的数据传输，由此导致技术架构缺乏自上而下的威权式的集中管辖。于是，互联网在组织架构上是对传统集权型中央等级式组织的解构：没有传统的星型结构的中央控制中心，而是一种非中心式的分布结构。在这种结构中，所有子网在地位上都是平等的，经由互联网社区控制的开放性协议连接形成网络互联。

在 1980 年代互联网发展的初期，互联网运行的原则是“代码即法律”：代码在实践中成为规范用户行为的主要手段。此一时期，互联网的技术规范和技术标准就是网络空间的法律：因为互联网的新兴和高科技的特点，国家法律始则沉默继而滞后，使市场机制得以主导互联网的发展并塑造网络空间的秩序。此后，代码与法律的关系一直争议不断。不过，数字技术也并未从根本上挑战法律；两者关系的关键问题在于细节和场景。[9]而且，1990 年代形成的互联网群聚效应（Critical mass）带来的网络效应（Network Effect）远大于采用新网络形式所能够带来的新好处，再加之大量用户、企业不断加入现有网络形成的从众效应（Bandwagon Effect）加持，使得从技术上改革或分裂互联网的成本变得非常高昂。[10]

3. 技术与理念惯性叠加

网络无政府主义理念能够经久不衰，实际上深深根植于互联网的技术结构之中。网络技术所具有的非中心、颠覆性功能，使得这一技术所推动的并在与人类活动的交互中快速形成的虚拟空间兼具动态性与复杂性的双重特征，并由此增加了各类行为体内部及相互之间就网络空间应否达成及达成何种秩序形成共识的难度，从而对网络治理形成极大挑战。最终，人类之间的象征性沟通，人与社会的生产、经验和权力，因技术而改变并不断在网络空间扩张、延伸和映射。二战后形成的试图缓解无政府状态的国际秩序和治理体系的建章立制（尽管并非十分有效）无法直接映射至网络架构和现实操作层面。甚至，因为大规模网络监听、网络作战部队急速发展、网络渗透等国家行为的挑战，网络空间的和平与发展面临着较物理空间更为巨大的危险。

技术之弊总是要通过技术创新来解决。在加密经济网络（比特币首次引入该概念）支持下，当前核心的互联网服务有可能重新构建。加密网络结合了前两个互联网时代的最佳特征：社区管理的、去中心化的网络，这决定了它们最终将超越目前最先进的以头部互联网平台为代表的中心化服务。在这种加密网络里，管理策略与治理决策是由社区以公开透明的机制做出的。这是一种建立社区所有权网络的有力武器，它将为第三方开发者、创造者和企业提供一个公平的竞争环境。在现实中，各加密网络会使用多种机制来确保在发展过程的中立性，从而防止中心化平台可能采用的渗透与诱购手段。

由此，一种可能性是：从 web1.0 到 web2.0，起于去中心化的互联网，在发展到成熟而中心化后，最终会被创新的去中心化所取代：去中心化的网络可以赢得第三个互联网时代，就像企业家赢得第二个时代、开发者赢得第一个时代那样。当然，这个过程会涉及大量重复的反馈循环，能否共存、何者上位是个动态过程，主角涉及核心协议的开发人员、加密网络的开发人员、第三方应用程序的开发人员以及提供服务的运营商。

不过，当前加密网络受到许多制约，尚无法真正挑战中心化平台。其中，最严重的制约当属其自身的性能和未来的可扩展性。再次去中心化网络虽然提供了比中心化系统更好的解决思路与可能方法，它并不是解决现在互联网所有问题的灵丹妙药。而且，人类行为中的路径依赖，也使互联网的无政府主义技术架构无法彻底改变。路径依赖最直接的例子是电脑键盘改革。目前普遍使用的“QWERTY”式键盘，成形于 19

世纪,是一种把最常用字母安置在相反方向的按键布局排列方式。这种键盘设计之初“在不会卡死的情况下尽力提高打字速度”的目的,现在早就不必考虑了。然而,因为成本和习惯的原因,新式布局键盘的市场推广很不顺利。改变一个键盘布局尚且如此困难,更遑论互联网架构这样的系统工程。

代码不能成为法律,互联网不是法外之地。网络空间法治化是民族国家政府的大致共识、现实政策与实践追求。尤其是,随着互联网日益成为现实社会的框架和平台,深度规制网络空间势在必行。

二、有形之手:网络主权与国家执法

在构成现代国际社会的根本性原则之中,国家主权是最根本、最核心的要素。当一国主权在网络空间中进行自然延伸时,作为一个极具争议性的概念,网络主权通常被用来主张对数字内容和/或基础设施的某种形式的集体控制,但包括民族国家在内的不同行为主体对主权的精确解释、主体为谁、含义和定义可能有很大不同。[11]

网络主权(Internet sovereignty, cyber sovereignty)大略是指:对内要独立自主地发展、监督、管理本国互联网事务;对外要防止外部势力入侵、攻击和非法利用本国互联网。介于互联网的无界性,主权国家在网络空间获取权力与影响力的规则制定权和话语权的争夺非常激烈。

1. 概念演变与观念博弈

关于是应该提倡更严格的互联网控制还是更自由的网络自治,是网络主权广泛辩论的一部分。学术探讨是形成行为规则的思想基础。1997 年吴修铭(Timothy S. Wu)提出基于民族国家利益的“网络主权”概念[12]后,在世界范围内日益受到广泛深入的研究和探讨,虽历经变迁、饱受争议,影响却越来越广。对于网络主权与“国家主权”之间的张力与互动,目前存在立场敌对、侧重点差异或诉求重叠等多种对应关系的四种不同的观点。

第一种观点完全反对网络空间的国家主权,强调自身不受干扰的互联网主权。1996 年,约翰·佩里·巴罗在《赛博空间独立宣言》中提出基于网民利益的网络主权:“你们(包括网络巨头与政治力量——作者注)没有任何道义上的权力来统治网络空间,你们也没有任何使我们惧怕的方法来执行,……网络空间不存在于你们的领域之内”。[13]2020 年,弥尔顿·L·穆勒(Milian L. Mucller)提出:主权是排他性的最高权威,因此,国家网络主权就要求互联网管理与领土边界重合;若想真正实现网络主权,则要或者建立隔绝与外界数字联系的数字孤岛式的局域网——这将牺牲本国互联网的全球兼容性和信息服务贸易,或者导致所有国家之间进行全球网络空间唯一主权的争夺,这种全有或全无式的主权,即便不是完全无可能,也会遭到所有其他国家和民族的强烈反弹,从而扼杀全球互联网的互通性。由于网络空间的非领土性影响,部分研究者认为基于国家主权的网络治理方法是进入了一个死胡同。不过,既有的过程和现实表明,某些全球化倡议者和技术乌托邦主义者对国家弱化甚至是放弃网络空间权力的建议只能是空想;主权国家只会更加借助信息技术来增强国家在网络空间治理中的能力与话语权。

第二种观点强调国家主权原则适用于一国的网络活动。2019 年英国皇家国际事务研究所发布《国际法对国家网络攻击主权的适用和不干涉原则》报告指出:因为一国能够对其领土内的网络基础设施、领土内外的公民行使独立的国家主权,所以,主权原则可以适用于网络活动暨一国可以在其领土范围内就网络事务管理行使独立的国家权力。实际上“主权”一词所暗含的利益和斗争高于合作与理性的原则,并没有加剧网络冲突。一项针对包括 110 个网络事件和 45 个网络争端数据集的研究显示,竞争对手之间的网络争端的实际规模和速度与大众的看法不一致;126 个活跃的竞争对手中只有 20 个参与了网络冲突;而且,所发现的互动在规模和频率上都是

有限的,这表明网络上的克制;此外,大多数被发现的网络争端都是区域性的,违背了网络力量的无边界性质。[14]导致这种现象的原因在于,虽然民族国家基于主权和利益会进行有甄别、可选择的自主互联网连接,但是,网络空间要发挥最大的聚合效能以保证国家发展不掉队,就需要无障碍、全时空的全域连接与畅通。

第三种观点强调国家主权的主导地位,网络主权必须以此为基础来界定和延展。中国相关机构联合发布的、定义了网络主权及其原则和具体体现的《网络主权:理论与实践》(2.0 版)认为:其一,一国未经许可不得入侵他国网络系统进行网络监控、窃密或破坏活动;其二,网络主权义务要求一国提升网络治理的透明度、规范性和稳定性,以保障其管辖范围内别国网络主体的合法权益,促进网络空间的开放与自由;其三,网络主权义务要求一国作为国际共同体成员,积极参与网络主权治理,在联合国框架下推动网络空间国际公约和准则的制定,建立网络空间的争端解决机制。不过,网络技术挑战了基于第三次工业革命基础上的传统国际规则——比如,威斯特伐利亚条约认为国家的垄断权是以暴力为基础的;但面对代码武器化和技术平民化的现实,控制的概念与内涵需要重新界定或很难界定。通常情况下,最强大的国家会提倡自由,而其他国家则强调游戏规则。

第四种观点强调以“最低限度的合作”来构建网络主权。国家拥有网络空间的“核心主权”,但互联网作为全球公共产品的特征和全球公域的性质以及通信基础设施的全球范围覆盖等特点,使得监管框架必须转移到国际层面,以国家为责任主体在国际层面施行“合作主权”。

目前,全球权力转移、全球性问题出现、全球政治觉醒和全球新边疆的出现等趋势,对网络主权概念的演变形成了重大影响:其一,因为欧洲、北美和东亚在经济层面出现的三足鼎立,使网络霸权失去了物质基础,网络主权在实践中应是合作的而非单边的;其二,基于互联、互通和互动才能发挥功能的网络空间,不应、不能也不该走向封闭;其三,要解决全球政治觉醒导致的动荡、全球新边疆出现的挑战,就需要以开放的网络主权作为互联网全球治理的基础,不断丰富和完善网络主权的观念和实践,打造一个和平、安全、开放、合作、有序的全球网络新空间。

这些关于网络主权的内容、方式和边界的界定,既有所差异又环环相扣,反映出在维护网络空间和谐发展目标下,对网络主权不同向度的系统认识和动态权衡会处于长期博弈的过程中。网络空间构成了一个全球分歧的空间,作为构成主体的国家和互联网在其间的联系是有争议且持续的。[15]

2. 民族国家的立场博弈

国家不断增强针对互联网的权力以打开发展空间并得到最大的赋能,不少国家更是用相关技术加强在国内控制和国际网络战中的胜算,[16]这导致了网络空间正在或应该恢复到威斯特伐利亚模式的论断:[17]各国在建设信息基础设施、塑造信息基础权力上的博弈愈演愈烈。大国地缘战略竞争已延伸至网络空间,互联网被视为传播信息战的战场,以牺牲对方为代价来增强自己的全球影响力:利用网络空间向全球受众宣传自己世界观的同时,反驳对方的信息叙事。[18]

民族国家实践网络主权的理念依据有三:一是认为主权本身是不断演进发展的概念,其内涵、外延和实践无疑会随着时代环境、社会变迁和世界格局的变化而进行相应的调整;国家权利会自然延伸,进而通过国家主体间共有观念的博弈形成国际规范。二是网络空间的可规制性为国家在网络空间行使主权提供了现实可行性和必要性——与现实空间一样,在很大程度上只有政府才有能力合法地来采取所需的各种安全保障措施。毕竟,无论是互联网的基础设施还是终端用户,都无法脱离国家地缘政治主权管辖的边界。同时,随着实践与技术的演进,民族国家政府管理信息流动和网络行为的现实手段在不断

充实和丰富。这些事实为国家主权介入提供了可能。三是网络秩序的缺失和网络威胁的加大,使民族国家政府通过网络治理和主权管理以化害为利塑造秩序,具有了现实理由与理念正当性。

联合国就在2013年首次明确《联合国宪章》下的主权平等原则适用于网络空间的立场。主权叙事确实对许多新兴网络大国以及中小型网络参与者具有吸引力。例如,继中国在2014年第53届亚非法律协商组织年会上提出"网络空间国际法"议题后,该组织成立了一个工作组来讨论网络空间的国家主权和国际合作。包括部分西方国家在内的许多国家,在制定其互联网政策时,越来越强调政府参与和数据主权。在这其中,一些发展中国家不愿接受以西方为中心的做法,因为他们的声音在西方阵营中很少被听到,他们将网络主权视为制衡或削弱美国在网络空间霸权的一种方式。例如,津巴布韦、吉布提和乌干达担心接入互联网只是一个让美国科技公司殖民其数字空间的门户,他们更喜欢基于非西方标准和价值观的互联网。

2019年的第74届联合国大会第一委员会,通过了两个各有拥趸却在网络空间治理路径上存在基于地缘政治分歧的决议草案:一个是获得美国、欧盟支持但遭到中国和俄罗斯等国反对的《从国际安全角度促进网络空间国家负责任行为》的草案;另一个是获得中国和俄罗斯等国支持却遭美国和欧盟反对的《从国际安全角度看信息和电信领域的发展》的草案。这直接反映出以美国为中心的现有多利益相关方模式与希望通过联合国或其他多边、以国家为基础的主权治理模式之间的对抗和博弈。这其中的典型是美国与中国在竞争性技术(5G、尖端芯片)和竞争性网络规范(网络自由主义与网络主权)上的互动,西方有学者用数字本地主义来解释这种日益紧张的关系,[19]认为这种东西方之间的分歧将导致合作的可能性有限。西方集团国家一直批评和抑制中国为追求对网络空间的更多控制而采取的网络治理方式。[20]不过,在美国连续发生的网络恐怖主义事件也使更广泛的政治社会的态度从优先考虑隐私保护转变为承认政府对私人—公共信息共享系统的不可避免的使用,这导致了相关法案的立法。[21]

欧盟与美国的治理观念也有分歧,它认为数字主权是保护其自身市场不受美国和中国技术巨头影响、确保主权政府作用、平衡美国在网络空间的霸权及获得数字自治的必要条件。这导致欧盟更有可能接受与中国接近的网络规范。[22]当然,欧盟和中国在网络主权的含义上存在争议:中国推动网络主权更多是出于国家安全考虑,而欧盟追求网络空间主权的动机是保护数据隐私等公共权利以及欧洲数字经济的发展。此外,虽然欧盟强调政府参与的重要性,但它支持多方利益相关者模式,而不是多边模式。乐观而言,欧盟与中美的差异或许可以使其在中美网络争端中充当调解人,确保网络治理斗而不破。

在全球化进入国与国相互依赖的网络空间时代,简单或一味照搬绝对的和排他性的传统主权原则,根本无法适应网络空间秩序建构与维护正义的要求。此前,美国互联网管理的全球开放政策,帮助了美国成为互联网巨头主宰世界。美国利用网络安全审查制度,禁止TikTok等针对中国挑起事端的"霸凌行径",预示了一种更具侵略性的技术监管哲学。这种做法的显然错误在于:一是将所有数据视为国有资源,而不考虑数据的流动特征与禀赋,导致管辖权向别国不当拓展;二是恣意行使网络霸权,违反法治的可预期性和正当程序原则。如果更多国家跟随特朗普,以外交顺从、保护主义目的或是以公民安全的新顾虑为由进行数字控制,互联网会变得更像一个由许许多多封地拼凑起来的地方,由此可能造成的"分裂(或碎片)网"(Splinternet)违背互联网的初衷,违背互联网全球互联、开放、去中心化的本质,违背技术架构的公平普适性,严重威胁互联网为人类带来更广泛合作互利、全球覆盖和经济增长的能力。

关于网络主权的国际斗争仍将持续,因为线上行为与线下行为已经完全叠加与混合而绝非虚拟主权,未来具体的形态和内容构成仍在塑造之中,一个可能的趋势是网络主权的着眼点开始从主要是政治考虑转向更多的商业考虑:通过跨境资本、数据贸易和服务贸易的控制,确保本国用户数据非经允许不得跨境流动更不被境外利用。未来,强调网络主权在网络安全建设中的作用,也许是设想为全球数字资本主义的实践建立护栏,并不意味着关闭网络以将一个国家与外界隔绝。

3. 网络空间的地缘政治

当代环境的某些独特方面,对国家控制提出了挑战,[23] 尤其是数字时代网络空间与现实空间高度融合,成为了人类生产生活新空间、民族国家新疆域和全球治理新对象。尽管各国对网络主权的公开立场不同,但都在以立法、执法和司法管辖的形式行使管辖权,为本国网络空间建章立制,并试图影响国际规则以建构本国在全球治理中的话语权和行动力。网权论(制网权)也与海权论、陆权论、空权论和天权论等经典流派一起共同构成地缘政治理论。世界各国军队在采用数字、电子和网络设备和技术后不久,网络空间就开始军事化,并成为第五战场。大国的军队在通信、作战和计划方面都严重依赖网络空间,它们针对不同目标发起的网络攻势引发了国际社会的网络军备竞赛和持续的网络空间战略竞争。

这显著地助推了网络空间的无政府状态。地缘政治的权力架构已经大比率地蔓延、复制和映射到了全球网络空间,成为国家行动的现实基础:网络空间组成架构的地缘属性、网络空间活动主体的地缘属性以及主权国家在网络空间日益上升的权力,都促成了网络空间的地缘政治属性。[24]

其一,国家的地缘政治结构决定互联网的物理结构。互联网的物理层,是由传输数据的光纤电缆、互联网交换中心(IXP)和互联网服务供应商(ISP)的数据中心等具有机械的、电子的、功能的和规范的硬件组成。目前近 80% 的互联网流量是通过光缆传输的,由于光缆大多铺设于海底,且为跨国铺设,故而海底光缆会为各国的网络安全带来脆弱性。比如,非友好国家在某国家网络光缆附近所进行的海洋军事行动,会带来网络切断和信息监听的威胁和风险。对此,需要通过国家间的协议、协调和谈判来进行预先安排和事后解决,以保证互联网的物理结构顺畅。各种形式的网络化和数字化活动,包括实体(physical)网络、逻辑(logic)网络、数据(data)网络和社会(social)网络等,尽管可以使公民社会之间绕过政府进行直接接触,非国家行为体也可以更方便地参与到国际事务中,但网络并没有弱化国家边界,反而使政府在网络空间中的作用更加明显起来。互联网体系结构的各个层面及相互之间与国家的互动,使地缘政治以自己的方式和特征在网络空间发挥最大的作用。

其二,国家的地缘政治实力决定网络结构。人造的网络结构大多是规则的,但网络连接的集散中心却与地缘政治结构吻合。在随机的互联网结构中,节点与其他节点连接的数量应该呈正态分布,即某个节点与其他节点的连接数量是固定的,是有尺度的网络。不过,现实是部分节点会与其他大量节点进行连结,进而形成一个个的集散中心和节点,从而使互联网形成无尺度网络(scale - free network)。这种自由网络节点的实体位置与现实地缘政治完美对应:因为互联网的诞生和发展均源于美国,因此美国的互联网交换中心数量最多,而且,大部分集散中心和节点都位于美国;在趋势上,中国迅速发展的大型互联网公司使得这些节点有东移的趋势。这既是由美中的地缘政治实力决定的,也推动了双方地缘政治实力的增长。

其三,地缘政治权力结构的变化会影响互联网发展。一项国际制度的形成,是基于对彼时世界关切的回应,也是彼刻地缘政治力量的实力对比。随着权力架构因位移而失衡、关切问题因时

势变化而发生变化,这项制度安排就不再适合彼时彼此的目标和诉求。在互联网产生的时代,实力处于巅峰状态的某些大国塑造了互联网样态及其治理。当前,某些大国作为霸权国家的制度否决能力在明显下降,叠加全球性问题的挑战、风险社会的环境和全球权力格局的变化,全球治理制度改革的窗口已经打开。网络空间亦复如此:全球权力从西方向东方转移的趋势,在网络空间治理方面产生了一个日益对抗和竞争的多极系统:面对非西方世界不断上升的影响力,西方不得不面对其衰落的真实可能性——这一点在2020年慕尼黑安全会议上对"无西方"(Westlessness)的密集讨论中有所体现。[25]

在这种情况下,国家系统正试图修改互联网,以使其更好地符合国家利益,无论这些是一个更负责任的网络(防止和阻止不可接受的行为);一个不太负责任的网络(赋予活动家和持不同政见者权力);一个拥有更好的工具来规范对特定内容的访问(删除破坏稳定的言论或侵犯版权的材料);或者是一个普遍可用、更容易使用、不受约束的创新和商业平台的网络,[26]均会导致网络空间的激烈博弈。

涉互联网技术的革命性发展不会改变这种地缘政治态势。基于5G技术的机器学习、人工智能及区块链等颠覆性技术,就像当初的铁路和电报一样,可能会改变地缘政治的计算,但新兴技术还不足以改变既往的技术—经济范式,更不会改变地缘政治的结构和逻辑。而且,网络空间的光纤电缆网络、数据处理模块、内容构成、语言使用及互联网用户,仍会直接反映民族国家的架构。网络空间尽管容纳包括跨国公司、非政府组织、民间社会及个人行为者等诸多非国家行为参与者,民族国家仍将是地缘政治行为体中影响力最大的有机体。在很大程度上,只有民族国家政府才有能力且合法地来采取各种措施保障安全,包括攻击性行动等。不过,面对非国家主体影响的增强以及网络攻击、侵犯隐私和安全威胁的普遍与频密发生,包括美国、中国和俄罗斯在内的大国政府已经被锁定在关于未来网络主权如何治理网络空间的辩论之中。[27]

进入2020年代,随着全球化进程和全球秩序的动摇,民族国家的影响力在上升:对国家的角色和功能应该不断弱化,甚至让位于全球治理和全球善治的理论期待在退场之中,网络空间尤其如此。能否在网络主权这个复杂概念之下,处理好网络设施与运行、网络数据与信息、社会与人三组范畴的平衡,将反映全球网络治理的成败。

三、无形之手:数字资本主义的监控

互联网企业是全球数据、网络安全、隐私等的拥有者或控制者,是海量信息时代的新闻入口,互联网经济已经开始主导世界经济:苹果、微软和Alphabet近年冲上或接近3万亿美元的市值;美股科技企业前十家的市值总和已经远超多数国家股市总市值;在全球范围内有互联网属性科技企业的市值也呈爆炸性增长,传统的能源巨头和优质企业的上升幅度与节奏已不可同日而语;大型科技公司在网络空间治理中扮演着极为重要的角色。

伴随科学革命和技术创新,以科技公司为主导的数字秩序有可能在某些领域与政府共同行使规则制定权。比如,尽管中国的网络治理主要是由保护国家主权和增加政府参与的愿望所驱动,但强化无线局域网认证和隐私基础设施(WAPI)流产的案例意味着中国企业并不总是支持政府的观点,企业对国家的某些互联网科技政策形成有决定性影响。[28]

1. 科技平台的中心化

作为技术系统的互联网,一开始会被既有的社会结构所塑造。但随着对数字基础设施依赖增加而导致的物质条件变化,会改变过去的权力结构和监管动态。[29]

在Web 1.0阶段,互联网用户取得了巨大的成功,此时的互联网是由一组特定的想法所主导的:互联网消除了守门人,为创新开辟了新的空

间,允许自下而上的对话,使沟通民主化等。[30]在网络全面商业化阶段,原本的网络管理模式在一定程度上得以延续,非政府行为体在网络空间治理中占据主导地位。[31]

在2005年左右进入Web 2.0阶段后,出现了可以通过让用户生产内容来降低成本的想法和以平台核心的商业模式。此后,尽管将以美国为中心的硅谷视作所有在线生活之母只是神话,[32]但美国互联网平台一直呈现压倒性影响并形成全球垄断地位。而在美国国内,曾是新经济时代最著名网络公司的美国在线(AOL)等新媒体公司,在信息传递、共识建构和舆论发动上的重要性呈断崖式下跌。

2010年代是商业互联网发展的新阶段。在手机日益成为超级电脑的技术背景下,在智能手机的爆炸式增长的助力下,移动应用成为互联网的核心。同时,科技平台超越开放协议能力的软件与服务的快速建立,导致用户最终从开放服务态势转向更复杂、更集中的服务;在国际互联网市场,引领着数字经济发展与技术应用创新,成为企业创新的引擎,并在数字技术的显著进步所撬动的生态系统中建立互补的产品和服务。[33]

背负这些功能的平台已经成为特定网络活动的标志,Google、Twitter、YouTube、MSN和Skype等已经成为搜索、微博客、视频分享、聊天和视频会议的同义词,并且实现了"名词动用":无疑,一个公司在渗透社交活动方面取得成功的顶点,是使一个品牌名称变为动词。当前,GAFA(Google、Amazon、Facebook和Apple)作为美国科技界的四大巨头,垄断着美国乃至全世界的技术版图,任何初创企业和投资者想要有所作为都绕不开这四大巨头。作为数字经济方面唯一可以媲美美国的国家,中国也存在类似情况。B(百度、字节跳动)A(阿里巴巴)T(腾讯)J(京东)等顶级互联网企业,急剧地聚合流量:它们到2020年左右,控制了整个中国互联网超过70%的流量。不过,除了字节跳动旗下的TikTok,中国平台的营收主要来自国内,国际影响力不足。

2. 资本系统的规训控制

这些科技平台,运用数字技术发现、利用和创造差异获取利润,追求持续不断的资本积累,会形成新的数字资本主义体系,使数字化信息处理、数字化商品生产等数字劳动成为价值和剩余价值的主要源泉之一。这是资本主义发展在经历商业资本主义和工业资本主义后的新历史形态。劳动形式的变化使数字资本主义作为一种新型模式,继承了商业和工业资本主义的实质,成为资本主义体系的重要发展阶段,是在数字空间中对过往资本主义历史的一次重演。[34]

在前途路径上,数字资本主义时代的利益冲动会战胜对未知科技的担忧。2023年11月,OpenAI的董事会来回换将的博弈显示,在希望人工智能更快发展与更安全发展之间,资本赢了。在这个案例中,为了利用人工智能开启一个繁荣新时代为企业赚取财富,那种认为超前的人工智能是从神经网络的数字深处召唤出来的怪兽,必须极其谨慎地加以限制和部署以防止它跨越"奇点"(singularity)以接管并杀死所有人的顾虑,被忽视了。作为一项有可能引领第四次工业革命的技术,人工智能不太可能长期被那些想要减缓其发展的人所控制——尤其是在事关巨额投资回报的情况下。民族国家或许也会担忧能否驾驭尖端人工智能,但不能让对手超过自己的安全困境会让它们站在资本一边。

在现实场景中,数字资本主义的负面影响不能无视。这些基于西方理念的现代技术在很多场景下是资本主义的一种系统规训和控制,如同消费主义一样,蕴含价值定位、文化同化和边界渗透的功能。比如,在数十亿用户获得惊人的且多半是免费技术的同时,这些并非不作恶的"科技暴君"收集的信息包含从健康记录、法庭文件到地图和购物记录等几乎所有类型的数据。这些占据人们大多数注意力的中心化技术平台,凭借海量的用户基础,通过主观排列和过滤信息,决定了用户能看到什么和不能看到什么。它们还能作出其他重要的互联网治理决策,甚至是突

然改变规则来掌控流量与数据以实现利益最大化。这会导致一系列市场失灵,无法实现自发性纠偏。面对可以改变规则、垄断客户、利润第一的平台,初创公司、创业人员的生态环境会举步维艰。而缺乏后来者竞争,创新便遭到抑制和压制,互联网的趣味与活力会被阉割。

利用科技平台的数据进行精准营销和精准打压的事件屡见不鲜。类似脸书等社交媒体平台一直通过默认设置来收集用户的直接与核心应用之外的信息,比如在人们点击智能手机上的程序会被归纳和引导上网习惯,进而将用户困在其生态系统中,以攫取大量商业利益。通过数据叠加在给用户画像后,脸书就可以把精心策划的在线广告精准传播给潜在购买者和目标用户以实现盈利。这其中最典型的就是剑桥分析公司(Cambridge Analytica)在未经用户许可的情况下收集、使用超过 5000 万脸书用户信息,通过结合微定向与心理学,在精心分析选民的数据和预测选民动向的基础上,针对犹豫选民有针对性地投放有利于雇主或捣毁对手的信息,从而在美国总统大选、英国脱欧公决等事件中为雇主服务。对于从利用技术对个人行为进行无限追踪并因之获得商业利润的角度看,这种将在线平台掌握的个人数据应用于政治操纵目的的现象,可称为"监视资本主义"。[35]

在社会资本下降、经济不平等加剧、群体极化显著、对科学的信任度下降以及媒体环境日益分化等趋势下,[36]伴随科技平台中心化的不断加强,再辅以国家赞助的机器人审查和算法偏差等问题,已经导致了所谓"后真相(post - truth)"时代的到来。这会损害个人隐私和数据安全,对特定的核心价值观、生活方式和政治制度形成挑战。

3. 互联网成为外交工具

民族国家在网络(in cyberspace)和经由网络(through cyberspace)的斗争很激烈。在这种斗争中,美国的资本和政治力量可以实质性地控制着科技平台,进行信息流操纵,包括利用网络空间注入错误信息、蓄意有偏见的报道、掩盖事实真相和捏造信息等,以影响人们的思想和行为,使之成为谋求全球影响力和地缘战略目标的新型武器。

从一开始,社交媒体公司就被美国资本主义和帝国主义的强大霸权所吸引,并与之结盟以巩固垄断地位。同时,在资本的操纵之下,美国的科技服务商与美国国家安全局广泛监控计划之间就存在密切的联系。而进入第四次工业革命的智能时代,美国硅谷科技力量的超强与领先地位和优势,是美国全球独大的数据和情报收集能力的保障,也日益成为美国保持其超强国际影响、军事力量、资本力量和文化力量的平台和基石。尤其是自美国奥巴马政府开始,互联网与社交平台就开始成为美国外交的"袋中之箭"。随之,"互联网自由"从一种个人理念演化成一种积极推行的外交政策。比如,美国利用社交媒体的"真相武器化"(weaponized truth)功能,在伊朗大选和阿拉伯之春中,通过推特和脸书等干预当地的局势,试图颠覆当地政权。同时,利用网络、信息和传媒优势展开"公众传播战"(public - communication warfare),在受众中大力塑造在西方叙事框架下的"真相",主动压制对美国不利的消息,从而在信息领域中迅速剥夺对手的话语权和叙事能力,实现对信息环境的统治。

同时,各大科技平台都主动或被地参与了类似"梭镜计划"等美国对全球的监视:美国政府在服务器上直接进行相关内容收集,让情报机构能对实时通信和存储在服务器上的信息进行深入监视并利用。[37]当然,很多其他国家也都试图如此行事,只是没有美国的实力,也没有美国如此娴熟和典型。美国科技平台所主宰的社交媒体,虽非简单的美国国际政策的传声筒,但在社会认知、价值判断和好恶立场上与政府非常接近,其所塑造的环境基本上成为"自由民主世界"政治正确的背书。这是对其自诩的监督、引领和沟通功能与意义的消解。

四、无政府状态下的治理合作

国际社会若无法通过引导技术向善、加强国际团结和进行资本驯化等方式建立一个有弹性和友好的网络空间以减少交易成本,全球福利将遭到掣肘和破坏。

1. 技术向善

针对互联网无政府主义的技术架构与文化秉性,首先,要使互联网从“代码即法律”的过去进入结合“法律即代码”的未来,以新型制度结构和政策实践引导代码配合国家和资本进行监管并规范互联网行为:建构法律条例、社会规范、市场供给和科学规范四位一体式的互联网行为规则,以鼓励或阻碍特定的市场行为,通过朋辈压力规范用户的社会行为等。

其次,技术创新都是以成群的形式出现的。要协同治理与互联网发展密切相关的人工智能、尖端芯片和致命自主武器系统等领域,否则技术系统的两极分化导致两套或多套系统将不可避免。创建更完善的高技术系统,需要所有主要参与者进行密切的科学互动,并制定统一的国际规范来管理类似人工智能在现实生活中的应用等。

再次,强化组织治理以加强对网络安全认知共同体的引导。网络安全认知共同体是指计算机领域科学家和工程师群体在网络安全治理领域中具备的以专业知识为核心的权威网络,[38]在一些科技平台,尤其是人工智能领域,许多巨头主要是研究人员而不是企业家。Alphabet、微软、OpenAI 和 Meta 等公司的研究人员仍然像教授那样通过发表研究论文的方式相互交流,但这远远不够。在依靠天才和直觉驱动的高科技领域,通过价值协调、强化因果认知和提升价值标准等,[39]认知共同体能够通过业务知识和政策知识形成的权威推动规范的形成。

最后,要鼓励科技发展与市场营利进行区分。目前,一个活跃的开源人工智能运动主张人工智能不受企业控制。OpenAI 的竞争对手 Anthropic 是由一群前 OpenAI 员工创建的,它将自己定位为一家公益公司,这种法律结构旨在使其免受市场压力影响。这样的定位和声音,可以中和科技公司只是为推出产品、创造收入和成为第一而快速行动、打破陈规的竞争,有助于对尖端人工智能极其谨慎地加以限制和部署,以防止做出对人类整体不利的行为。

面对科技革命,人类只能看到前方很短的距离,但人类应该知道有很多事情需要做,以确保公司文化和使命导向是最终获致技术向善,以避免人类被控制而不是去控制。

2. 共同治理

由主权确定的国际秩序,仅仅是价值与状态的结构化承载,在伦理道德上是无法通过是非判断来说服他国的;除非实现主权让渡,否则没有任何国家愿意牺牲本国利益以成全整体利益,更不用说他国利益。因此,尽管网络主权过度声索的刚性会损害其秩序性功能,但在总体国际无政府状态之下,首先需要自保以生存的国家的这种基于私利的行为模式是非道德的(amoral)而不是“不道德”的(immoral)。在目前国际无政府权力结构所决定的国际政治实践中,利益追求仍然超越价值判断。每个国家的行为都有基于主权利益的理由,即便该行为并不符合普遍的道德判断。

现有的网络治理协议和国际法,无疑无法获得所有国家的全部同意和维护,因此,其必然是部分失效的。仅仅通过不造成实际制约的舆论谴责是无法改变国家行为的;而在多数情况下缺乏制裁民族国家能力的国际法,也只能有条件地生效。[40]对抗承受能力与控制互联网能力方面,是保证和实现网络主权的前提。

不过,网络主权的刚性行使,并非完全符合国家利益,更无助于网络空间的稳定与有效。在国家彼此依赖的当今世界中,国际秩序的脆弱性和敏感性已经明白无误地显示:人类生活在一个风险共担的命运共同体中,在全球性挑战面前,没有哪个国家能够置身事外、独善其身;主权不只是权利,更是义务,国际和平及国家福利的维

护,是以各国在特定场景下交出一部分主权为条件的。可以说,对主权的自愿让渡和自我限制并未贬损主权,相反,它通过广泛而有效地履行国际义务恰恰可以提升主权国家的行动能力。一旦深刻理解各国相互依存、休戚与共的信念和原则并将其融入网络主权的理解和实施中,是否承担对其他国家的主权义务便是判断网络主权边界与好坏的主要原则。在这种实践不断形成惯习的情况下,共同治理有可能成为网络主权的未来。

搭便车理论认为,当群体成员数量增加时,把该群体成员组织起来参加一个集体行动的成本会大大提高,即大群体需要付出更大的代价才能发起一场集体行动。[41] 鉴于网络治理主体的多元与巨量,治理议题的庞大和复杂,建构基于新思维、新模式、新做法和新技术的符合人类整体利益的治理模式,注定是充满艰辛和不断反复的。

3. 资本驯化

自平台化成型以来,互联网公司巨大而高度集中经济权力、控制权力与传播权力的三重叠加就引发了社会责任问题并推升了监管的必要。[42] 这种状况在工业革命初期有一个有趣的平行线:工业力量对社会秩序的挑战,促使国家和社会采取控制措施,从而形成了工会、劳动法和消费者保护法等治理规范。同时,平台化本身也证明了互联网监管的可行:之前,极度分散化的互联网导致监管就像试图监管空气或烟雾一样困难;之后,互联网流量大部分集中于较少的平台,治理和监管平台就可以引导互联网发展。

在寻求平台治理的新方向,通过监管以促进平台合理发展的过程中,没有"一刀切"(one - size - fits - all)的解决方案:谷歌与苹果达成的排他性默认搜索协议引发的针对互联网平台企业垄断行为的审查,并不适合所有其他中小互联网企业。较为合理的方案至少应包括三个相互关联的战略:利用数字技术创造更多社区驱动的组织形式;建立一个开放和可访问的平台文化;促进有意义内容的创造、策划和消费。[43]

各国都在以前所未有的紧迫性和广度采取行动,以限制平台的野蛮发展。全球性的强化反垄断监管已成趋势。面对人工智能的快速发展,以抵制监管著称的超大型平台也主动呼吁加强政府监管,以分担平台自我治理的成本:脸书首席执行官扎克伯格表示,社交媒体公司需要政府提供更多监管,以解决日益严重的有害在线内容问题;谷歌首席执行官桑达尔·皮查伊称人工智能太重要了,不能不进行监管,只是需要采取"合理的方法";微软总裁布拉德·史密斯称世界"不应等待技术成熟"才对人工智能进行监管。[44]

不同国家的治理动机是不同的:美欧担心科技企业正在阻挠竞争、传播虚假信息并侵蚀隐私;俄罗斯等则是试图控制敌对运动,加强政治统一、维护稳定。不同的动机也导致了不同的监管模式。中美两国针对内容的平台治理,分别以国家和市场为主导,形成了"以内容监管为主的国家主义"和"以技术治理为主的市场主义"两种模式。这两种不同甚至冲突的治理背景虽然差别巨大,但并非全然是企业走出国门、获得全球成功的障碍:遵循内容治理和技术治理分离原则的字节跳动公司,分别打造了两种模式下最为成功的抖音和 TikTok 短视频平台即是明证。[45] 不过,互联网企业凭借一国注册、全球运作的技术优点而大获成功的案例并不多。

要解决民族国家与全球市场之间的矛盾,平衡通信技术与法律之间的失序,从现实效果看,各国应采取更综合的治理战略,以避免治疗措施的不良后果比弊病本身的危害更大。目前,建立平台控制与国家监管之外的"第三条道路"的倡议很多。[46]

五、结　论

网络空间治理规范的缺失,很难单靠一方获得更大话语权来弥补和链接。综合而言,当前全球互联网治理有五种模式。一是早期开放互联网(the open web)的理论与实践遗存;二是头部科技平台主导的公司主义互联网(corporatist In-

ternet)；三是科技公司和政府融合；四是受规制互联网(the regulated Internet)；五是混乱代理人模式。这种出现在不同司法监管区的不同治理实践，存在三种问题：一是标准化欠缺——没有经过验证的模范做法和程序供全球借鉴；二是有出现“分裂网”的风险——在不同的司法管辖区以不同的方式运作，但在一个司法管辖区的事情会影响到其他地方的事情；三是监管的代价——国家有自主选择权，但若阉割掉平台运营和组织优点，将导致国内收益和国际竞争力降低。

其实，导致互联网无政府状态的先天之手、有形之手和无形之手，背后都是人性在起决定作用。任由人类天性中以牺牲集体利益为代价来最大化个人效用的倾向发展，人类注定要盲目地开发世界资源，从而形成公地悲剧。但身处危机时刻，人类的社会性和理性也会纠正天性的盲目与冲动，会聚集在一起制定规则和制度、甚至做出个人牺牲来管理公共资源、保全集体利益。在化解网络风险、获致网络善治的过程中，人类要负责任地行动起来，以兼济天下的安排和久久为功的心态，发挥灵性与潜能，超越现实的锱铢必较，在伦理、道德等更恒久的领域处理好相互的关系。如此，增强治理民主以约束权力来源、运用法治以约束权力运行、通过信息透明以约束暗箱操作，就有可能经由网络空间国际合作达到网络善治。

注释：

〔1〕Kenneth Oye ed., *Cooperation under Anarchy*, Princeton: Princeton University Press, 1986, p. 11.

〔2〕刘力波：《网络无政府主义的意涵及发生探源》，《思想战线》2017 年第 1 期。

〔3〕Woon, Shin Chang, “Libertarian Dimensions of Information Society”, *Society and Theory*, 2012, (21), pp. 535 – 567.

〔4〕不过，2020 年美国国会提出两项法案，规定不包含政府访问方法的加密为非法。

〔5〕这些依赖加密的技术包括：可以将金融交易置于政府监控和征税的能力之外的区块链；能够在促进泄密的同时保护举报人的举报平台；可以混淆公民物理位置的暗网等匿名网络。Jarvis, Craig, “Cypherpunk Ideology: Objectives, Profiles, and Influences(1992—1998)”, *Internet Histories*, 2022, 6(3), pp. 1 – 27。

〔6〕Dahlberg, L., “Cyber – Libertarianism 2. 0: A Discourse Theory/Critical Political Economy Examination”, *Cultural Politics: An International Journal*, 2010, 6(3), pp. 331 – 356.

〔7〕《马克思恩格斯选集》第 1 卷，北京：人民出版社，1995 年，第 585 页。

〔8〕Jayne Rodgers, *Spatializing International Politics: Analyzing Activism on the Internet*, Routledge, 2003.

〔9〕Jan Oster, “Code Is Code and Law Is Law—the Law of Digitalization and the Digitalization of Law”, *International Journal of Law and Information Technology*, Vol. 29, Iss. 2, 2021, pp. 101 – 117.

〔10〕Milton L. Mueller, “Will the Internet Fragment?”, *Polity Press*, 2017.

〔11〕Couture, S., & Toupin, S., “What does the Notion of ‘Sovereignty’ Mean When Referring to the Digital?”, *New Media & Society*, 2019, 21(10), pp. 2305 – 2322.

〔12〕Timothy S. Wu, “Cyberspace Sovereignty? The Internet and the International System”, *Harvard Journal of Law & Technology*, vol. 10, No3, 1997, pp. 647 – 666.

〔13〕BARLOW John Perry, “Declaration of Independence of Cyberspace”, GAYARD L., *Darknet: Geopolitics and Uses*, Vol. 2, UK: wiley, 2018, p. 149.

〔14〕Valeriano, B., &Maness, R. C., “The Dynamics of Cyber Conflict between Rival Antagonists, 2001—11”, *Journal of Peace Research*, 2014, 51(3), pp. 347 – 360.

〔15〕Yu Hong & G. Thomas Goodnight, “How to Think about Cyber Sovereignty: the Case of China”, *Chinese Journal of Communication*, 2020, 13(1), pp. 8 – 26.

〔16〕AKDUMAN, Birol, “From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance”, *International Journal of Social Sciences*, 2023.

〔17〕Demchak, C. C., &Dombrowski, P., “Rise of a Cybered Westphalian Age”, *Strategic Studies Quarterly*, 2011, 5(1), pp. 32 – 61.

〔18〕Tan, Er – Win&Sayankina, Sofiya, “Cyberwarfare and the Weaponization of Information in US – China 21st – Century Geostrategic Rivalry”, *Pacific Focus*, 2023.

〔19〕Moore, G. J., “Huawei, Cyber – Sovereignty and Liberal Norms: China’s Challenge to the West/Democracies”, *Journal of Chinese Political Science*, 2023, SCI(28), pp. 151 – 167.

〔20〕Strickling, Lawrence E., “Internet Governance Progress after ICANN 53: Hearing before Subcommittee on Communications and Technology Committee on Energy and Commerce”, *United States House of Representatives*, 2015.

〔21〕Jho, Whasun, “Cyber – security Governance in South Korea and the United States: A Comparison of Securitization of Cyber – threat”, *Information Society & Media*, 2017, 18(2), pp. 97 – 120.

〔22〕〔28〕Xinchuchu Gao,"An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model", *The International Spectator*,2022,57(3),pp. 15 - 30.

〔23〕Krasner,S. D.,"Abiding Sovereignty", *International Political Science Review*,2001,22(3),pp. 229 - 251.

〔24〕蔡翠红:《网络地缘政治:中美关系分析的新视角》,《国际政治研究》2018 年第 1 期。

〔25〕Xuechen Chen & Yifan Yang,"Contesting Western and Non - Western Approaches to Global Cyber Governance beyond Westlessness", *The International Spectator*,2022,57(3),pp. 1 - 14.

〔26〕Choucri, N., & Clark, D. D.,"Who Controls Cyberspace?", *Bulletin of the Atomic Scientists*,2013,69(5),pp. 21 - 31.

〔27〕Lantis,J. S., & Bloomberg,D. J.,"Changing the Code? Norm Contestation and US Antipreneurism in Cyberspace", *International Relations*,2018,32(2),pp. 149 - 172.

〔29〕Sofie Flensburg & Signe Sophus Lai,"Networks of Power. Analysing the Evolution of the Danish Internet Infrastructure", *Internet Histories*,2021,5(2),pp. 79 - 100.

〔30〕Flew T., *Regulating Platforms*, Cambridge: Polity,2021, pp. 53 - 55.

〔31〕刘杨钺、张旭:《政治秩序与网络空间国家主权的缘起》,《外交评论》2019 年第 1 期。

〔32〕这种说法混淆了 1980 至 1990 年代存在于世界各地的平行在线网络的存在。当时,许多国家发展了全国性的、国营的、由邮政电报和电话公司(PTT)管理的单一网络,著名的例子包括英国(Prestel)、德国(Bildschirmtext,BTX)、巴西(Videotexto)等,其中,法国的 Minitel 是世界上第一个在一国层面上获得大规模渗透的在线系统,2012 年被关闭之前,Minitel 与 Internet 是并存的,法国人都可以选择访问两个网络。Julien Mailland,"Building Internet Policy on History: Lessons of the Forgotten 1981 Network Neutrality Debate", *Internet Histories*,2018,2(1 - 2),pp. 1 - 19;Gillies, J.,& Cailliau,R., *How the Web Was Born*, New York, NY: Oxford University Press,2000,pp. 67 - 70。

〔33〕Jingyao Mei,Gang Zheng,Ling Zhu,"Governance Mechanisms Implementation in the Evolution of Digital Platforms: a Case Study of the Internet of Things Platform", *R&D Management*, 2022, 52(3),pp. 498 - 516.

〔34〕〔日〕森健、〔日〕日户浩之:《数字资本主义》,野村综研(大连)科技有限公司译,上海:复旦大学出版社,2020 年,第 35 页。

〔35〕Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London: Profile Books,2019,pp. 11 - 13.

〔36〕Lewandowsky, S., Ecker, U. K., & Cook, J.,"Beyond Misinformation: Understanding and Coping with the Post - truth Era", *Journal of Applied Research in Memory and Cognition*,2017(6),pp. 353 - 369.

〔37〕Greenwald,Glenn,"NSA taps in to Internet Giants´Systems to Mine User Data, Secret Files Reveal", *The Guardian*,2013(6).

〔38〕Ernst B. Hass, *When Knowledge Is Power: Three Models of Change in International Organizations*, Berkeley: University of California Press,1990,p. 57.

〔39〕赵瑞琦:《面向 2035 年的全球网络安全治理:认知共同体的建构》,《中国科技论坛》2020 年第 11 期。

〔40〕〔德〕贝克:《全球化时代民主怎样才是可行的》,《全球化与政治》,北京:中央编译出版社,2000 年,第 11 - 12 页。

〔41〕赵鼎新:《集体行动、搭便车理论与形式社会学方法》,《社会学研究》2006 年第 1 期。

〔42〕Castells M., *Communication Power*, New York, NY: Oxford University Press,2013,pp. 90 - 95.

〔43〕Fenwick, M., McCahery, J. A. & Vermeulen, E. P. M.,"The End of 'Corporate' Governance: Hello 'Platform' Governance", *Eur Bus Org Law Rev*,2019(20),pp. 171 - 199.

〔44〕胡泳、马爱:《人工智能治理:波兰尼双重运动理论视角》,《现代出版》2023 年第 3 期。

〔45〕Jinhe Liu,Le Yang,"'Dual - Track' Platform Governance on Content: A Comparative Study between China and United States", *Police & Internet*,2022,14(2),pp. 304 - 323.

〔46〕Flew,T.,& Lin,F.,"The Third Way of Global Internet Governance: A Dialogue with Terry Flew", *Communication and the Public*,2022,7(3),pp. 121 - 129.

〔责任编辑:李本红〕