美国网络信息技术治理实践与启示

郭滕达，张明喜
（中国科学技术发展战略研究院，北京 100038）

摘 要：当前，网络信息技术加速扩散、融合，为政府治理带来难题。美国对网络信息技术的治理主要从国家安全、跨域管辖等方面进行考量。美国秉持政府、私营部门等共治的“功能治理”架构，重点治理“跨应用领域技术”和“特定技术”两类技术，通过纵向集成和横向集成促进治理的一致性，综合采用事前、事后治理等治理程序。尽管中国国情与美国有所不同，但是美国在相关领域的实践可以为中国提供借鉴。建议采用系统性而非孤立的视角和思维对网络信息技术治理进行思考，积极审慎出台相关法律和规章制度；完善优化纵向和横向集成治理体系；尽快引入循证决策、预见治理、建构性评估等事前事中治理程序。

关键词：美国；网络信息技术；技术治理；国际经验研究
中图分类号：C931 **文献标识码**：A DOI：10.3772/j.issn.1009-8623.2023.01.008

习近平总书记指出，网络信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最大的技术创新领域。网络信息技术的发展一方面带来了巨大的经济红利，另一方面也对国家主权、安全、发展利益、道德伦理造成冲击，给治理带来挑战。不同于刘永谋[1]对技术治理的阐述视角，本文的研究对象是“对技术的治理”，即认为技术治理是指通过灵活协调的规范、原则、决策和体制安排对技术研发、应用过程进行规制，目的在于促进技术自身健康发展，并让技术成为保障国家安全、推动经济社会发展、增进人类福祉的有效手段。本文主要基于美国政府政策、美国智库核心观点、美国相关组织机构治理实践等，采用世界经济论坛的技术治理架构，分析美国对网络信息技术治理的主要考虑和做法，期望为中国政府决策提供借鉴。

1 数字经济背景下美国网络信息技术治理的六大着力点

在数字经济背景之下，网络信息技术扩散、融合的速度十分之快，美国对于网络信息技术的治理主要从如下角度进行考量。

1.1 网络信息技术治理与国家安全

2018 年，美国政府颁布的《国家网络战略》概述了美国网络安全的 4 个支柱，即保护美国人民、国土和美国的生活方式，促进美国繁荣，通过实力维护美国和平，提高美国的影响力，具体手段包括授权国土安全部（DHS）保障美国联邦部门和机构的网络安全，将信息和通信技术提供商作为网络安全的推动者等具体措施[2]。拜登上台之后，于 2021 年 5 月签署了《改善国家网络安全的行政命令》，提出渐进式的改进不会给美国带来所需要的安全，相

第一作者简介：郭滕达（1982—），女，副研究员，主要研究方向为区块链技术发展与政策、科技创新治理。
项目来源：科技部科技创新战略研究专项“区块链技术发展模式、影响及对策建议”（ZLY201818）；山东省重点研发计划（软科学项目）重大项目“促进科技创新要素向中小企业集聚的机制和政策研究”（2021RZA01003）。
收稿日期：2022−11−24

反，政府需要做出大胆的改变和重大的投资，具体提出向零信任架构迈进、加快安全云服务步伐、投资技术和人员等措施[3]。

1.2 网络信息技术治理与跨域管辖

数据的跨境流动正在考验国家和国际治理框架。美国关于跨域管辖权的难题从微软诉美国（关于域外获取数据）的案件中可以看出①。2018 年，特朗普签署了《澄清境外数据的合法使用法》，迫使美国企业遵守美国国内搜查令上交数据，不管这些数据是存储在美国还是外国；同时明确美国行政部门有权与外国政府签订数据共享行政协议[4]。这一法规是美国政府对跨境数据可获取性的重要回应。

1.3 网络信息技术治理与隐私保护

多年来，美国各界对隐私与监管平衡的讨论一直持续②，一方认为制度化监督是良好的政府所必需的治理工具，另一方认为政府不得滥用权力。美国政府在司法方面做出了一些努力，如出台《存储通信法》《执法通信援助法》等，但在隐私权方面仍缺乏联邦层级的立法。随着越来越多新兴技术的出现，政府、公众对隐私和监管之间平衡的博弈也将会更加激烈。

1.4 网络信息技术治理与反垄断

网络信息技术逐渐发展所形成的行业往往规模效应或网络效应非常之大。2021 年 6 月，美国众议院司法委员会审议《合并申报费现代化法案》《州反垄断执法场所法案》《通过启用服务交换法案》《平台竞争和机会法案》《美国选择与创新在线法案》《终止平台垄断法案》等 6 项以技术规制为重点的反垄断法案，旨在控制大型科技企业不断膨胀的权力[5]。

1.5 网络信息技术治理与对华战略竞争

随着中国在网络信息技术领域的话语权地位日益提升，对华战略竞争已经成为美国网络信息技术治理的重要目的。《芯片和科学法案》是对华法案的“集合体”。美国多家智库、期刊也都将网络信息技术治理与中美大国竞争联系起来。例如，《亚洲政策》期刊发表文章提出[6]，为了减少中国企业的市场准入，美国和日本应将不可信的中国 5G 技术驱逐出其信息通信技术（ICT）市场，收紧外国投资审查程序，并确保中国 5G 企业无法利用联合资本市场为其扩张提供资金。美国战略与国际问题研究中心（CSIS）发表报告提出，美国必须确保中国的数据治理模型不会在亚太地区盛行，使得数据治理成为美国在亚太地区经济战略的核心[7]。

1.6 网络信息技术治理与多边合作

美国与主要经济体在网络信息技术治理方面存在共同发展利益，也面临分歧。美国战略与国际问题研究中心报告认为，世界主要经济体对隐私保护、跨境数据流动及政府干预等议程缺少共识，应分析各国数据体制及其冲突，形成 G7 数据治理原则[8]。美国信息技术与创新基金会（ITIF）也指出[9]，欧盟法院裁决“数据隐私盾协定”无效，为美欧发展带来了严重风险，应制定新的“隐私盾协议”，并确定用于执法机构开展跨境数据调用的法律框架，还应制定协调战略，对抗中国、俄罗斯等国家，压制其 5G、人工智能等技术发展。

2 美国网络信息技术治理基本模式

基于世界经济论坛对技术治理的分析框架[10]，本文对美国网络信息技术治理进行结构分析（见图 1）。

2.1 秉持政府、私营部门等共治的“功能治理”架构

分析美国网络信息技术治理的关键之一在于理清规则、规范、政策的来源，美国网络信息技术治理的主导部门通常来源于政府和私营部门等。

2.1.1 美国政府

美国政府并没有设置专门负责网络信息技术

① 微软与美国司法机构展开争论的焦点是美国执法部门是否应该迫使微软交出存储在美国境外服务器上的数据。2016 年，美国联邦第二巡回上诉法院支持微软主张，裁决微软无须依照美国执法部门的要求提交存储在境外的数据。

② 例如，20 世纪 70 年代中期，公钥密码技术的出现使得复杂加密成为可能。出于对其可能影响政府监控通信能力的担忧，从 20 世纪 90 年代早期开始，美国政府推行了 Clipper 芯片计划，试图让加密技术为政府留出一扇后门；克林顿政府提出对 Clipper 芯片的开发和推广进行补贴。政府意图十分明显，如果政府能够让 Clipper 芯片成为最廉价的技术而使工业界普遍采用，就能够间接地规制加密技术。美国政府认为市场会替政府进行规制。然而，补贴计划失败了，对代码本身的质量和开发过程中的保密性的质疑，以及对政府导向的加密体系的反对，使得大多数人拒绝使用该技术。近年来，加密技术对保护公众隐私的强大影响以及对执法监视的挑战越发显而易见，美国各界关于“第二次加密战争”的争论也越来越多。

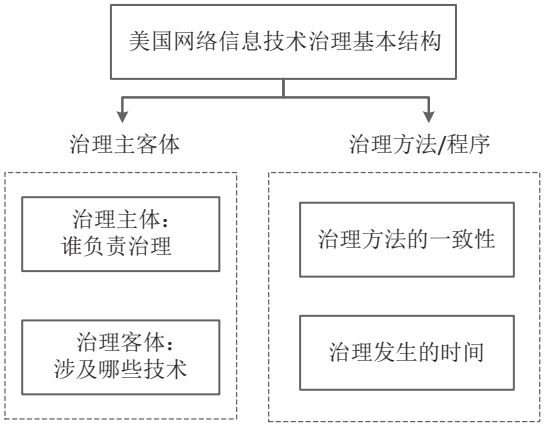

图 1　美国网络信息技术治理基本分析框架

治理的组织机构，主要由独立 / 非独立的委员会和各级行政机构承担网络信息技术治理的具体工作（见图 2）。

独立 / 非独立的委员会一般在政府指导下建立，抽调内阁各部门成员组成，主要承担咨询和协调功能，联邦通信委员会（FCC）是其中的典型代表。行政机构是美国网络信息技术治理决策的执行机构，包括国土安全部、商务部（DOC）、国防部（DOD）、财政部（DOT）等部门，其中，国土安全部下的科学和技术局、网络安全和基础设施安全局，以及商务部下的国家标准与技术研究所是重要的网络信息技术治理执行部门。美国政府在网络信息技术治理

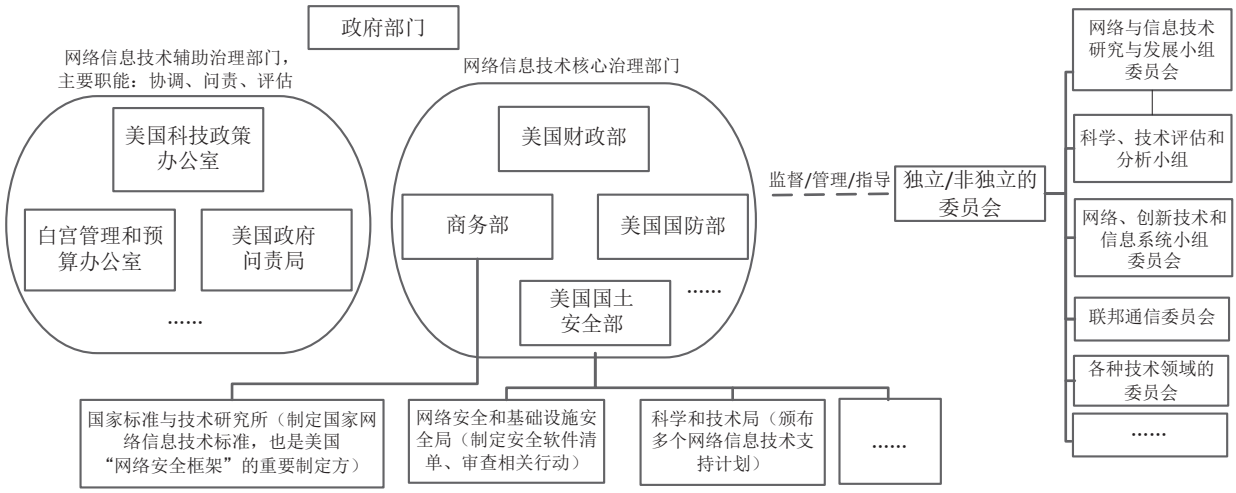

图 2　美国网络信息技术治理中的政府职能结构

中的主要职责大致可以概括为：支持研发、吸引资本投入、组建委员会或联盟、制定标准、建立法规、评估风险、发布指南、搭建平台等。

2.1.2　非政府部门

对于美国非政府部门参与网络信息技术治理，可以从 3 个方面理解。一是科技巨头企业、行业协会、网络信息技术社区等深度参与治理。随着数字技术渗透到社会各个领域，美国一些科技巨头企业通过拥有、运营大量数字基础设施存储公民数据，利用信息技术形成“信息茧房”，在网络信息技术治理中拥有重要话语权，例如，谷歌主导建立的 Andriod、Chromium、TensorFlow 等框架，通过开源形成了全球垄断，美国甚至出现了网络信息技术治理“私营化”的趋势。行业协会、技术社区等参与网络信息技术治理主要体现在制定行业技术标准、建立行业联盟等方面。例如，微软收购的 Github 已经成为全球开源社区基础设施的事实标准。二是美国智库、情报机构、风险投资企业等通过多种手段推动治理。它们对网络信息技术治理的推动作用不容忽视，在政治主张等方面各有侧重，通过广泛搜集信息、敏锐察觉技术发展动态、搭建多方沟通桥梁、参加政府听证会、提供咨政建议等方式，将其思想理念渗透到美国网络信息技术决策之中。三是学术界、产业界等与政府部门形成协同共治。例如，产业界在美国隐私参数工程平台（P3P）工作组的成员构成中占据大量位置（68%）[11]。美国国家人工智能研究资源（NAIRR）工作组汇集了来自学术界、产业界和政府的 10 余位专家，为人工智

能研发、竞争、商业应用等广泛议题提供建议。

2.2 重点治理跨应用领域技术和特定技术两类技术

美国网络信息技术治理客体一般可以分为两类，即跨应用领域技术和特定技术，这两类治理对象通常互有交叉。

2.2.1 跨应用领域的网络信息技术治理

例如，《加州消费者隐私法》关于隐私和数据共享的规则可以应用于人工智能、区块链等多种技术治理领域，因为这些技术的应用均依赖数据，且跨越多个行业领域。跨应用领域的性质使得美国对这类技术主要采用公共辩论、裁决和立法等方式进行治理。

2.2.2 特定网络信息技术治理

当前，美国主要关注的网络信息技术聚焦在5G、人工智能、量子、区块链等领域。对这种具体技术的治理往往一开始属于私营部门治理范畴，例如，美国的行业协会在区块链技术标准等方面发挥了极其重要的作用。随着技术的发展，以及其为经济、社会、国家安全带来影响的凸显，政府部门开始介入特定技术的治理，通常采取前文提到的组建委员会、建立备忘录、发布指南等形式。

2.3 通过纵向集成和横向集成促进治理的一致性

技术治理需要观察相互关联的政策、标准和规章制度是如何在不同的主体之间进行纵向和横向整合[10]。

2.3.1 纵向集成治理

美国对网络信息技术的纵向集成治理可以从竞争、合作两个角度理解。

一是竞争。与中国竞争是美国网络信息技术治理的重要议题。美国在支持技术研发、执行技术出口审查、建立技术联盟、限制人才流动等方面采取了一系列行动。近期，美国智库关于中国在国际电信联盟（ITU）中的作用，以及如何发挥美国在国际电信联盟中作用的建议、报告越来越多。2020年12月，美国战略与国际问题研究中心报告指出，美国缺乏战略性组织；中国利用其在国际电信联盟中的领导地位，推动有利于中国企业的技术标准，并使中国的监控和审查模式合法化；美国政府应与国际电信联盟建立更全面的伙伴关系，共同扩大参与标准和体系采购的私营公司数量[12]。2021年5月，美国战略与国际问题研究中心报告再次强调，中国向国际电信联盟各研究小组派出了规模最大的代表团；在国际电信联盟高层领导的支持下，华为通过这些研究小组开展工作，就5G、网络安全和人工智能等主题提出了2 000多项新标准提案；美国要在国际电信联盟2022年选举中运用在世界知识产权组织和经济合作发展组织选举中的经验和良好做法，建立广泛的联盟，以支持志同道合的候选人，争取在国际电信联盟中谋求更多职位[13]。

二是合作。通过合作弥合国家、地区间的鸿沟是美国推动网络信息技术治理的重要目标之一，美国在此方面亦采取了很多做法。除了与发达经济体之间的合作之外，美国与发展中国家和较为落后国家在网络信息技术领域的合作也已经开展。美国国际开发署（USAID）于2020年4月发布《数字战略2020—2024年》[14]，该战略旨在实现开放、安全、包容的数字生态系统，增强美国国际开发署伙伴国家的自力更生能力。美国国际开发署开发了数字生态系统国家评估（Digital Ecosystem Country Assessment，DECA）决策工具，帮助美国国际开发署特派团、其合作伙伴和其他相关利益攸关方确定机会，最大限度地获得利益[15]。

2.3.2 横向集成治理

美国对网络信息技术的横向集成治理可以从利用层级、共建生态两个角度理解。

一是利用层级。即依靠不同层级的特定权力机构，通过发布指南、组织协调等来促进政府部门治理的一致性。例如，网络和信息技术研究与发展计划（NITRD）是美国网络信息技术研发的主要政府资助来源。美国政府建立了小组委员会、非政府组织、政府间组织等三方组织结构，协调、管理、指导、执行网络信息技术研发活动，通过网络和信息技术研究与发展小组委员会和政府间组织等建立长期合作关系，促进网络和信息技术研究与发展各部门之间的信息共享和工作协调（见图3）。美国政府也善于利用“安全港”等措施为联邦政府、州府之间的差异和冲突留出“缓冲区”。“安全港”措施可以理解为一种豁免安排，例如，美国在推行区块链技术和加密货币时尝试使用了很多“安全港”条款，美国国会成立的区块链核心小组提出为区块链开发者及区块链服务供应商提供一个“安全港”，使他们免受发牌及注册监管，允许使用或交易加密货

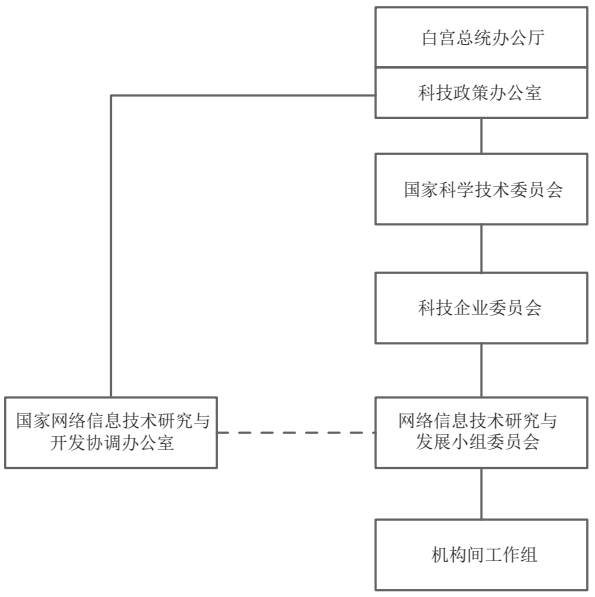

图 3　网络和信息技术研究与发展计划组织结构

资料来源：http://www.nitrd.gov/about/index.aspx。

币但不持有代币的公司免受资金转移法律的约束，以促进更好的横向集成治理。

二是共建生态。政府在幕后搭台设计，企业、高校和科研机构、非营利组织、媒体平台等在“台上唱戏”是构建横向集成治理体系的关键。以美国开源软件生态构成为例（见图 4），美国国防高级研究计划局（Defense Advanced Research Projects Agency，DARPA）与 Linux 基金会展开广泛合作，推出 OPS-5G 计划，致力于安全的 5G 网络软件和应用程序开发。美国国防高级研究计划局与 Linux 基金会结盟的意图是加速安全的开源创新，增强美国在突破性技术上的竞争力，在整个生态系统中促进企业、高校、科研机构等利益相关主体利用、共享资源。

2.4　综合采用事前、事后治理等治理程序

事前治理力求在技术应用和任何相关挑战出现之前建立机制，从而避免或预防风险。美国对网

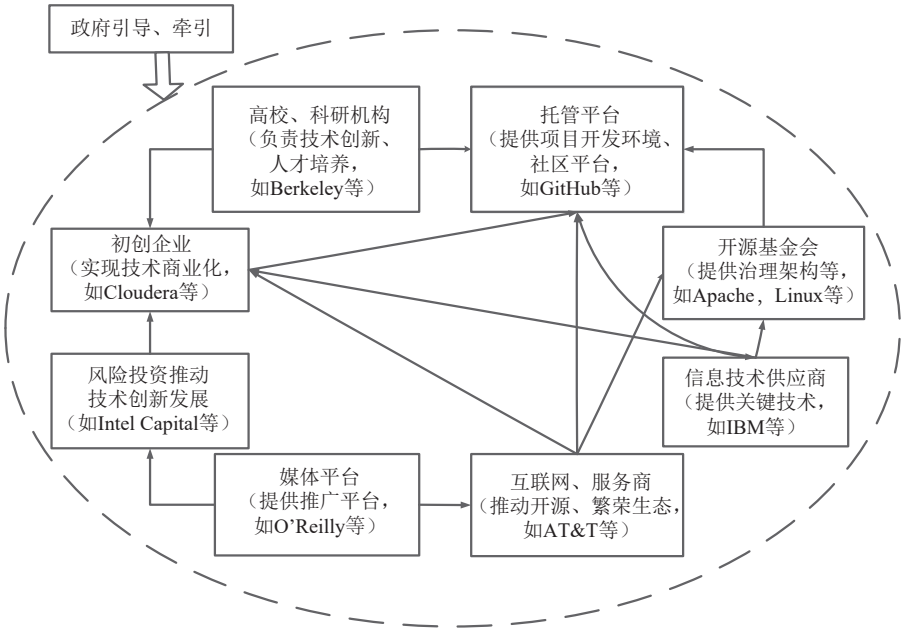

图 4　美国开源软件生态构成的关键要素

资料来源：作者与企业的内部交流研讨；→表示一项要素对另一项要素的促进方向。

络信息技术事前治理的方法主要包括风险分析（依靠专家听证会证词、科学数据、情景分析、小规模试点验证等来评估和管理风险）和学术界比较提倡的预期治理[16]（不仅关注技术成果可能带来的后果，更注重技术发展本身，强调探索未知、意见交换、优化整合过程的动态平衡，并不断反馈[17]）。拜登政府在执政之初就明确强调，基于科学量化的风险分析将再次成为政府对包括网络信息技术在内的新兴技术进行治理的前提和基础。拜登政府的“恢复政府信任计划”明确指出要彻底审查“不正当的

政治干预”，试图通过恢复科学诚信和循证决策提高政府技术治理能力和实际效能[18-19]。这是事前治理值得借鉴的方式。

事后治理则寻求在风险出现后进行管理，例如，设立法律法规，迫使立法者重新考虑治理机制是否仍然适当。利用法律规制技术是美国对网络信息技术进行治理的最常见方法。例如，20 世纪，电话网的技术设计给执法带来了难题，尤其是对于那些依赖于监听情报的执法活动而言。在线路交换网中，认定并监听某一电话线路相对容易，而在数据包交换网中，由于数据包的传播路径捉摸不定，所以监听就变得相对困难。这一设计促使美国国会在 1994 年颁布了《执法通信援助法》。它要求：网络必须被设计成保护执法能力的模式，以便实施电子监听。这一要求曾经在一系列的“安全港”协议下协商，最终规定标准网络必须符合法律的这一要求。《执法通信援助法》是一个信号，随后这种信号不断涌现，2005 年 8 月，联邦通信委员会规定，语音通话技术（VOIP）“必须设计成便于政府监听的模式”[20]。

3 关于网络信息技术治理的启示与思考

基于上述分析认为，美国在网络信息技术治理方面的一些做法值得中国借鉴、反思。

3.1 美国网络信息技术治理的若干启示

3.1.1 政府在网络信息技术治理中有合理边界

数字经济时代，美国网络信息技术治理的多个考量维度之间存在固有的相互联系，国家安全、数据治理、国际关系等并不割裂。美国政府应对网络信息技术挑战的逻辑起点是认识到网络信息技术治理涉及多个利益相关主体，涵盖经济、社会、国家安全、大国竞争等多种层面，其对网络信息技术的治理存在明确边界，一是必须干预，如围绕涉及国家安全的网络信息技术研发或应用，动用多领域力量进行治理；二是较少干预，如针对科技巨头早期的并购行为①、特定网络信息技术的早期发展等，更多的是创造自由、宽松的政策氛围。

3.1.2 规制网络信息技术所产生的平台往往比规制使用者行为更为有效

在对网络信息技术进行治理的过程中，应确保政府的治理能力不被日新月异的技术所削弱。从前文提到的电话网和加密技术案例可以看到，如果要实现这个目标，政府不直接规制使用者行为，而从具体技术行为所产生的平台等入手，往往更为有效。例如，在电话网案例中，由于当时美国的电话公司数量很少，所以规制相对容易。

3.1.3 激励多方、多层级主体共同参与治理

如果没有强有力的纵向和横向集成的治理架构来解决网络信息技术治理问题，一个国家的安全、投资潜力等都将受到威胁。尽管美国在此方面亦面临很多挑战②，但也有很多成功案例。当前，美国政府越来越注重把风险投资家 / 企业、产业界、基金会、智库甚至媒体等都纳入其技术治理主体成员中，引导多方、多层级主体参与治理，共建生态。

3.1.4 前移治理时机

根植于美国传统中的“技术怀疑论”在其技术治理中发挥着重要作用。“技术怀疑论”起源于 1945 年左右，原子弹的研制和应用使得科学家开始质疑那些从研究中衍生出来的各种应用是否得当，会对世界未来产生什么影响；参与当时科学家运动的科学家曾争取在白宫和国务院任命一些科学顾问，尽管这一行动失败了，但是把总统科学咨询提到了美国公共科学议程上[21]。拜登上台伊始决定将总统科学顾问提升至内阁级别，也部分预示了其会延续“技术怀疑论”，更加谨慎地利用科学方法评估技术研发与应用，通过科学循证等事前治理方法指导技术发展。

3.2 从理论和实践角度看中国网络信息技术治理

从理论角度看，技术治理可被认为是与国家治理、意识形态等量齐观的概念[22]。刘永谋[23-24]认

① 早期，美国对收集和使用公民数据、并购和反垄断等方面的干预较少。许多公司通过收购竞争对手或潜在的有价值的公司而成长起来。据统计，从 2009 年到 2019 年，五大公司（谷歌、亚马逊、Facebook、苹果、微软）进行了 400 多次收购，很少被竞争主管部门阻止，也很少受到审查。

② 网络信息技术往往跨越政治和自然界限，哪些方法论、标准和法律适用，很难权衡。例如，美国政府问责局的文件显示，网络安全与数字经济密不可分，但是 2021 年新成立的网络空间安全和新兴技术局的职责设定，可能会使得美国在数字经济和网络政策问题上难以绝对统一。

为，技术治理是将现代科技的成果用于社会公共事务当中，以提高整个社会运行的效率。他提出，技术治理应坚持两个基本原则：科学管理和专家政治。丁大尉等[11]认为，技术治理是通过合作协商、建立伙伴关系、确立共同目标等方式对技术生产实施管理，从而将现代技术的发展从单一的政府发号施令或政府决策转向多元主体参与。虽然学术界对技术治理概念界定的角度不甚一致，但是普遍存在一个共识，即技术治理必须坚持正确的价值取向。对于网络信息技术而言，在技术的发展过程中，各种社会因素不断渗透进来，技术的社会效用被涵盖于技术的本质之中，从而打破了技术与社会之间的边界[25]；作为网络信息技术的治理主体之一，政府的治理行为往往落后于其他社会主体，极易形成“全球公域”思潮。因此，必须认识到，人民性是网络信息技术治理应该反映的正确的意识形态。

从实践角度看，中国的网络信息技术治理体系经过了多年的发展，逐渐形成了由互联网信息内容管理、网络安全多层次保护、关键信息基础设施安全保护、个人信息和重要数据保护、网络产品和服务管理、网络安全事件管理等构成的多维体系。在治理过程中，中国主要坚持对网络信息技术治理的“预先同意”原则[26]，即以保护国家安全和国家主权为底线，通过各种法规、制度化解网络信息技术发展对国家安全和国家主权的冲击。然而，需要认识到，网络信息技术往往具有虚拟性、时空压缩性等特征，技术发展带来了权力的分散化，促使企业、公众等都有可能成为直接的网络信息技术治理者，这将对中国传统治理模式带来挑战。

4 主要启示与建议

中国在网络信息技术发展阶段、网络信息技术发展所处环境等方面与美国有所不同，不应一味向美国看齐，要秉持公平正义、多元共享、协同共治等思想，积极探索符合网络信息技术发展特征的治理观念和策略。

（1）采用系统性而非孤立的视角和思维对网络信息技术治理进行思考。

建立鼓励创新的治理框架。一是大力支持网络信息技术发展和数字经济创新，注重二者的结合性。二是发挥政府部门及独立（由政府监督）的委员会或非独立的委员会在网络信息技术治理中的关键指导作用①和参与作用②，审慎出台相关法律。三是探索私营部门充分参与网络信息技术治理的科学路径③。四是与更多国家建立良好伙伴关系，积极应对国外对中国网络信息技术及数字经济发展的遏制与打压。五是投入更多资源，提升全社会网络安全意识和水平④。

（2）加快完善优化中国网络信息技术横向、纵向集成治理体系。

一是增强中央政府、地方政府在网络信息技术治理方面的一致性，协调地方政府之间的资源配置，避免资源过度浪费；同时，引导高校、科研院所、科技型企业、数据信息机构、核心智库、媒体平台等共同参与横向集成治理，补足生态系统重要要素短板。二是进一步提升中国在国际组织中的话语权；积极谋求与国际组织在网络信息技术方面的利益一致性，开展国际合作，通过多方论坛（如数字经济峰会）、政府间合作平台（如金砖国家新工业革命伙伴关系创新基地）等，推进全球网络信息技术纵向集成治理。

（3）尽快引入循证决策、预期治理、建构性评估等事前、事中治理方法。

对网络信息技术的治理应积极采用循证决策、预期治理、建构性评估等方法，政府应通过发布备忘录、指南等形式，建立事前、事中治理程序，可包括：预见创新机会和风险并实施动态监管，围绕目标制定弹性治理方法，积极采用数据分析、量化研究而非单一的调查统计方法增加监管干预的针对性和及时性，探索引入人文学者、社会学者参与治

① 明确政府对网络信息技术的治理边界，在组建多方机构、立法、评估、协调等方面发挥核心作用，推广使用监管沙箱、安全港等有利于创新的机制，一定要避免“一刀切”型的政策出台。

② 政府在网络信息技术治理的过程中，不应该形成与私营部门等的“二元对立”关系，而应充分思考如何真正参与网络信息技术治理过程，变为整个治理链条上的重要一环。

③ 探索引导科技型企业、核心智库、技术社区、行业协会等共同参与网络信息技术治理的科学路径。

④ 在政府和全社会网络信息技术技能，尤其是网络安全技术技能方面投入更多资源，鼓励相关领域科技型企业通过职业教育、在职培训等方式加强政府部门网络安全管理和实践技能，提升全社会网络安全意识和水平。

理对话、交流。■

参考文献：

[1] 刘永谋 . “新技术治理的隐忧”：以智能治理和生化治理为例 [J]. 当代美国评论 , 2019, 3(1): 39-48.

[2] White House. National Cyber Strategy of the United States of America[R]. Washington, D.C.: White House, 2018.

[3] White House. Executive order on improving the nation’s cybersecurity[EB/OL]. (2021-05-12)[2021-05-13]. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[4] United States Department of Justice. Cloud act resources[EB/OL]. [2021-06-07]. https://www.justice.gov/dag/cloudact.

[5] CHANCE C. House judiciary committee passes six antitrust bills targeting tech platforms and large transactions, setting up vote before house of representative[EB/OL]. (2021-06-01)[2021-08-09]. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/06/House-Judiciary-Committee-Passes-Six-Antitrust-Bills-Targeting-Tech-Platforms-and-Large-Transactions.pdf.

[6] HAROLD S W, TSUNODA R K. Winning the 5G race with China: A U.S.-Japan strategy to trip the competition, run faster, and put the fix in[EB/OL]. (2021-07-29)[2021-07-31]. https://www.nbr.org/publication/winning-the-5g-race-with-china-a-u-s-japan-strategy-to-trip-the-competition-run-faster-and-put-the-fix-in/.

[7] GOODMAN M P, RISBERG P. Governing data in the Asia-Pacific[R]. Washington, D.C.: CSIS, 2021.

[8] Goodman M P. Advancing Data Governance in the G7[R]. Washington, D.C.: CSIS, 2021.

[9] CORY N, DICK E. How to build back better the transatlantic data relationship[R]. Washington, D.C..: ITIF, 2021.

[10] WEF. Global technology governance: a multistakeholder approach[R]. Geneva: WEF, 2019.

[11] 丁大尉 , 李正风 , 胡明艳 . 新兴技术发展的潜在风险及技术治理问题研究 [J]. 中国软科学 , 2013(6): 62-70.

[12] CORDELL K. The International Telecommunication Union: the most important UN agency you have never heard of[R]. Washington, D.C.: CSIS, 2020.

[13] CORDELL K. How to win international telecommunication union[R]. Washington, D.C.: CSIS, 2021.

[14] USAID. USAID’S digital strategy overview[EB/OL]. (2021-08-16)[2022-01-02]. https://www.usaid.gov/usaid-digital-strategy.

[15] USAID. Digital Ecosystem Country Assessment: Colombia[R]. Washington, D.C.: USAID, 2020.

[16] BARBEN D, FISHER E, SELIN C, et al. Anticipatory governance of nanotechnology: foresight, engagement, and integration[M]. Cambridge: The MIT Press, 2008: 979-1000.

[17] 杨素雪 , 孙启贵 . 新兴技术的预期治理 : 内涵、意义与过程 [J]. 科技管理研究 , 2019, 39(23): 47-53.

[18] White House. Memorandum on restoring trust in government through scientific integrity and evidence-based policymaking[EB/OL]. (2021-01-27)[2022-01-02]. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/27/memorandum-on-restoring-trust-in-government-through-scientific-integrity-and-evidence-based-policymaking/.

[19] 劳伦斯・莱斯格 . 代码 2.0 网络空间中的法律 (修订版)[M]. 李旭 , 沈伟伟 , 译 . 北京 : 清华大学出版社 , 2020: 70.

[20] 尹楠楠 , 刘国柱 . 美国新兴技术治理的理念与实践 [J]. 国际展望 , 2021, 13(2): 103-119, 156-157.

[21] 王作跃 . 在卫星危机的阴影下 : 美国总统科学顾问委员会与冷战中的美国 [M]. 北京 : 北京大学出版社 , 2011: 28-40.

[22] 刘明奎 . 网络社会技术治理主义批判与概念重构 [J]. 江西社会科学 , 2020(9): 12-23.

[23] 刘永谋 . 大数据与技术治理 [J]. 民主与社会科学 , 2019(3): 53-57.

[24] 刘永谋 . 技术治理的哲学反思 [J]. 江海学刊 , 2018(4): 46-52.

[25] 张成岗 . 技术与现代性研究 : 技术哲学发展的“相互建构论”诠释 [M]. 北京 : 中国社会科学出版社 , 2013: 150-282.

[26] 刘连泰 . 信息技术与主权概念 [J]. 中外法学 , 2015, 27(2): 505-522.

（下转第68页）

toolbox of risk mitigating measures[EB/OL]. [2022-07-14]. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g- networks-eu-toolbox-risk-mitigating-measures.

[22] Council of the EU. Cyber-attacks: council prolongs framework for sanctions for another year[EB/OL]. [2022-07-11]. https://www.consilium.europa.eu/en/press/press-releases/2021/05/17 /cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year.

A Brief Analysis of the EU Technology and Industrial Policies in Cybersecurity

HUO Hong-wei

(Ministry of Science and Technology of the People's Republic of China, Beijing 100862)

Abstract: Cyberspace has become an important place for major countries to compete and cooperate. As one of the regions with the highest penetration of cyber infrastructure in the world, the public in the EU has widespread concerns about cyber threats. The European Commission regards cyberspace as an important carrier of global strategy. While maintaining its own network security, it has launched a series of new strategies and measures in network technology planning and industrial policy. In response to this situation, China should also actively adopt targeted policies and measures, and comprehensively use various means such as laws and regulations, technological innovation, industrial promotion, and cyber diplomacy to create a favorable internal and external environment for the development of the cyber security industry.

Keywords: the European Union; cyberspace policy; cybersecurity; policy research

(上接第56页)

Practice and Enlightenment of the U.S. Network Information Technology Governance

GUO Teng-da, ZHANG Ming-xi

(Chinese Academy of Science and Technology for Development, Beijing 100038)

Abstract: At present, the rapid diffusion and integration of network information technology brings difficulties to government governance. In the U.S., the governance of network information technology mainly considers national security, cross-domain jurisdiction, etc. It adheres to the "functional governance" structure of co-governance by the government and the private sector, focuses on governance of "cross-application technology" and "specific technologies", promotes the consistency of governance through vertical integration and horizontal integration, and comprehensively adopts governance procedures such as pre-event and post-event governance. Although China's national conditions are different from those of the U.S., the practice of the U.S. in related fields can also provide reference for China. It is recommended to use a systematic rather than isolated perspective and thinking to think about network information technology governance, and actively and prudently introduce relevant laws and regulations; improve and optimize the vertical and horizontal integrated governance system; and introduce evidence-based decision-making, predictive governance and constructive evaluation as soon as possible.

Keywords: the U.S.; network information technology; technology governance; international empirical study