统筹发展和安全视野下的数字经济治理绩效研究*

郎 平 郎 昆

【内容提要】 数字经济治理的关键在于平衡好发展和安全的关系。作者基于《新时代国家安全学论纲》一文的理论框架和数字经济的基本特征,从统筹发展和安全的视角出发,将数字经济治理分为基准情景、依附型合作、大国竞争和共享共治四种情景,分析和比较了不同情景下国家统筹发展和安全的绩效。结果发现,基准情景下国家对数字安全的投入应当止于均衡安全水平;依附型合作情景会形成“中心—外围”的数字霸权体系进而固化并加剧全球数字经济发展的不平等;大国竞争情景治理模式容易导致相关国家陷入“数字安全竞赛”困境;共享共治情景有助于实现总福利最大化的目标。数字经济治理中的欧盟数字经济治理模式、美日数字经济合作模式和中美数字竞争模式均会带来一定福利损失。中国提出的网络空间命运共同体倡议则可以充分发挥技术、数据和安全的公共产品属性,通过协调各国利益和促进各方合作,有助于在全球层面实现数字经济高质量发展与高水平安全的动态平衡。

【关键词】 数字经济治理;总体国家安全观;统筹发展和安全;全球数字合作;网络空间命运共同体

【作者简介】 郎平,中国社会科学院大学国际政治经济学院教授,中国社会科学院世界经济与政治研究所研究员(北京 邮编:100732);郎昆,清华大学马克思主义学院博士后(北京 邮编:100084)。

【中图分类号】 D815.5 【文献标识码】 A 【文章编号】 1006-9550(2023)08-0087-22

* 本文系研究阐释党的二十大精神国家社会科学基金重大项目(项目批准号:23ZDA113)的阶段性成果。感谢《世界经济与政治》匿名审稿专家提出的意见与建议,文中疏漏由笔者负责。

一 引言

数字经济是指“以数据资源作为关键生产要素、以现代信息网络作为重要载体、以信息通信技术的有效使用作为效率提升和经济结构优化重要推动力的一系列经济活动”。① 近年来,数字经济迅速发展,已成为新一轮科技革命和产业变革的重要引擎,深刻影响了人类的生产生活方式,也重塑和改变着全球竞争格局。数字经济发展速度之快、辐射范围之广、影响程度之深前所未有,正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。② 与此同时,数字技术的创新应用也带来了诸多安全问题。网络和数据安全领域已成为新时代国家安全的主阵地和主战场。在此背景下,发展和安全之间的张力凸显,处理好发展和安全的关系是数字经济治理的关键。习近平深刻阐述了网络安全和信息化的辩证关系,指出“网络安全和信息化是一体之两翼、驱动之双轮,必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作,要处理好安全和发展的关系,做到协调一致、齐头并进,以安全保发展、以发展促安全,努力建久安之势、成长治之业”。③ 进入数字时代,统筹发展和安全的重要性更加凸显。中国共产党第二十次全国代表大会报告更是将统筹发展和安全提升到新时代党和国家事业发展的战略部署层面,明确提出以新安全格局保障新发展格局。④ 因此,实现数字经济治理高质量发展和高水平安全的动态平衡既是贯彻新发展理念、构建新发展格局的关键,也是实现下一个百年奋斗目标的重要保障。本文研究的核心问题是:在全球层面,何种治理模式有利于实现数字经济高质量发展和高水平安全的动态平衡。

数字经济治理首先要解决好发展问题。以大数据、云计算和人工智能等为代表的数字技术迅速发展,数字经济已经成为推动全球经济增长的重要引擎,正在深刻改变人类的生产生活方式并重塑着全球竞争格局。当前,美国和中国在数字经济领域处于相对领先的位置。从数据来看,2021 年美国的数字经济规模达 15.3 万亿美元,居世界

① 国家统计局:《数字经济及其核心产业统计分类(2021)》,http://www.stats.gov.cn/tjgz/tzgb/202106/t20210603_1818129.html,访问时间:2022 年 12 月 3 日。

② 《习近平著作选读》(第二卷),人民出版社 2023 年版,第 534—539 页。

③ 《习近平谈治国理政》(第一卷),外文出版社 2018 年版,第 197—198 页。

④ 习近平:《高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告》,人民出版社 2022 年版,第 52—53 页。

第一位;中国的数字经济规模达 7.1 万亿美元,居世界第二位。① 可以预见,数字经济在未来国民经济中的比重仍将持续上升。中国政府发布的《"十四五"数字经济发展规划》明确提出,到 2025 年数字经济核心产业增加值占国内生产总值(GDP)的比重达到 10%。② 然而,当前数字经济发展的不平衡问题凸显,不同国家和不同地区之间的"数字鸿沟"日益扩大。主要国家在数据跨境流动、市场准入和技术标准制定等治理领域存在较大分歧,这严重阻碍了全球数字经济发展潜力的充分释放。

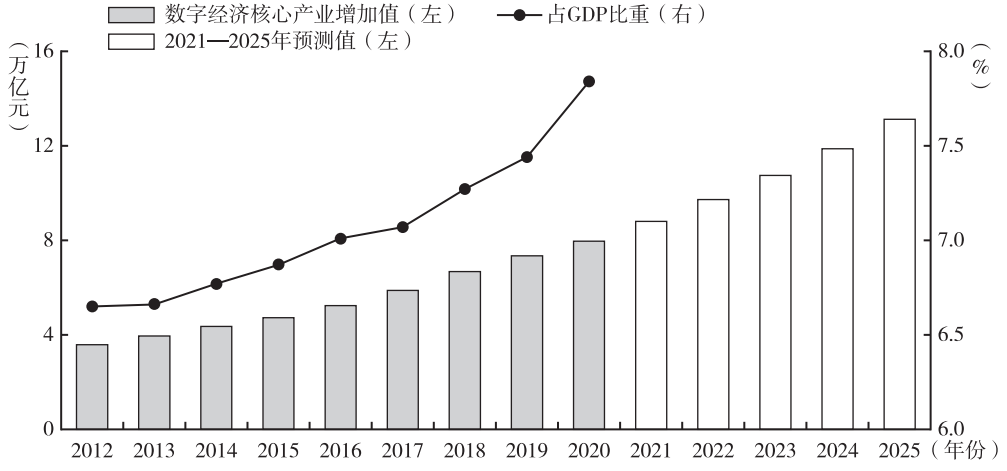

图 1 2012—2025 年中国数字经济核心产业增加值及其占 GDP 比重

资料来源:鲜祖德、王天琪:《中国数字经济核心产业规模测算与预测》,载《统计研究》,2022 年第 1 期,第 4—14 页。

注:数据截至 2020 年,由于 2021 年和 2022 年数据迟滞,故 2021—2025 年数据为预测值。

数字经济治理同样也需要处理好安全问题。数字经济的发展过程中始终伴随着安全风险并给国家安全带来了诸多新挑战,主要表现在三方面:一是垃圾邮件、路由劫持、分布式拒绝服务(DDOS)攻击和勒索软件攻击等恶意网络活动与日俱增,对国家安全(特别是关键基础设施安全)构成了极大威胁;二是数字空间成为国家间战略博弈的重要领域,甚至成为国家间冲突时的主要攻击目标,数字空间的无序状态加剧了国家安全的脆弱性;三是颠覆性技术理论不完善或技术本身存在安全缺陷,新技术的

① 中国信息通信研究院:《全球数字经济白皮书(2022 年)》,http://www.caict.ac.cn/kxyj/qwfb/bps/202212/t20221207_412453.htm,访问时间:2022 年 12 月 8 日。

② 《国务院关于印发"十四五"数字经济发展规划的通知》,http://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm,访问时间:2022 年 12 月 12 日。

快速创新和应用会引发潜在的安全风险。在此背景下,如何走出一条“数字经济活力迸发、数字治理精准高效、数字文化繁荣发展、数字安全保障有力、数字合作互利共赢的全球数字发展道路”[①]日益成为世界各国亟待解决的共同问题。

数字经济治理中的安全风险与创新发展相伴相生。为规制技术发展带来的安全外部性,很多数字经济治理问题(如数据治理和平台治理)既是经济问题,也是安全问题,对数字经济进行治理需要兼顾发展和安全两方面目标。因此,数字经济治理的核心问题是寻求发展和安全的平衡。在实践中,由于不同国家具体国情的差异,各国在选择发展和安全的最优平衡时也存在明显分歧,这是导致当今数字经济领域存在全球治理赤字的主要原因。本文聚焦数字经济治理议题,基于发展—安全的分析框架比较了数字经济背景下国家统筹发展和安全的绩效,对不同情景下的全球总体福利水平进行排序,进而提出了实现全球福利最大化的数字经济治理路径。

二 文献综述

近年来,中外经济学、管理学和政治学等领域的学者就如何在数字经济治理中实现发展和安全的平衡展开了一系列研究和探索,其研究内容主要分为三类。

第一类研究主要基于经济增长理论,重视研究数字经济的发展规律及其对宏观经济增长的影响,将数字经济视为一种新的产业形态,把数据视为新的生产要素。例如,丛林(Lin William Cong)等学者构建了包含数据要素的内生经济增长模型,认为数据要素的运用可以有效提高创新效率,进而促进长期经济增长,因此提出要积极推动数据要素的流动、交易和共享等政策主张。[②] 徐翔和赵墨非分析了数据资本对经济增长的直接影响和溢出效应,使用理论模型和数据模拟证明数据资本积累拉动宏观经济增长的巨大潜力,提出要对内加快布局与数据资本相关的基础设施、对外积极开展跨国数据资本合作。[③] 黄群慧等发现互联网发展可以通过降低交易成本、减少资源错配以及促进创新等渠道显著提升制造业企业的生产效率,认为中国应大力发展互联网技术并实现“互联网+”和制造业的深度融合。[④] 张勋等聚焦数字金融领域,认为数字金融

① 《习近平向2022年世界互联网大会乌镇峰会致贺信》,载《人民日报》,2022年11月10日。

② Lin William Cong, Danxia Xie and Longtian Zhang, “Knowledge Accumulation, Privacy, and Growth in a Data Economy,” *Management Science*, Vol.67, No.10, 2021, pp.6480-6492.

③ 徐翔、赵墨非:《数据资本与经济增长路径》,载《经济研究》,2020年第10期,第38—54页。

④ 黄群慧、余泳泽、张松林:《互联网发展与制造业生产率提升:内在机制与中国经验》,载《中国工业经济》,2019年第8期,第5—23页。

的发展显著提升了农村低收入群体的家庭收入,特别是改善了农村居民的创业行为,因此提出要推进数字金融的发展,强化其在创业、增收和改善收入分配上的作用。① 总的来说,这类研究大多是对传统经济学理论与模型的拓展,对数字经济治理的讨论往往聚焦于政府如何通过增加数字基础设施投入、推动数据共享和鼓励竞争创新等方式来促进数字经济发展的层面,对如何规制和解决数字经济发展过程中的潜在安全风险并未予以足够重视。

第二类研究从产业组织理论和市场监管理论出发,围绕平台企业的反垄断和反不正当竞争问题,讨论和分析了数字经济的监管规则设计。例如,有学者认为以平台为代表的新商业模式在数字经济时代正成为世界经济的主导,并产生了新的垄断。② 让-夏尔·罗歇(Jean-Charles Rochet)等提出平台经济具有交叉网络正效应,平台规模越大效率越高,平台的垄断不一定会损害社会福利。③ 王勇等提出了平台分层理论,认为最优的监管策略是要求平台企业增加分层数目和优化平台市场的分层设计。④ 在数字经济时代,政府和平台企业都是重要的监管主体,公共监管和私人监管并不是简单的替代或互补关系。从监管激励角度来看,适中的强度能够最优地协调政府和平台的监管力度。⑤ 江小涓和黄颖轩认为,大型数字平台依托其数字技术优势带来了“大而管不了”的问题,监管机制也应与时俱进,需要重点推进合规监管、分类监管、技术监管、均衡监管、价值导向监管和敏捷监管。⑥ 陈伟光和钟列炀认为,传统治理机制难以适应全球数字经济的快速发展,未来全球数字经济治理的主体与对象都将趋于多元化,构建统一、包容、共享、互惠的新秩序应当成为全球数字经济治理的理想目标。⑦ 孙晋认为,数字经济具有动态竞争、跨界经营、网络效应和寡头竞争等特征,数字经济治理的关键是进行监管创新,推进落实包容审慎监管、公平公正监管、协同整体监管、激励性监管、信用监管和智慧监管。⑧ 杨东提出,应本着鼓励创新和保护隐私

① 张勋、万广华、张佳佳、何宗樾:《数字经济、普惠金融与包容性增长》,载《经济研究》,2019 年第 8 期,第 71—86 页。

② Alex Moazed and Nicholas L. Johnson, *Modern Monopolies: What It Takes to Dominate the 21st Century Economy*, New York: St. Martin's Press, 2016.

③ Jean-Charles Rochet and Jean Tirole, “Platform Competition in Two-Sided Markets,” *Journal of the European Economic Association*, Vol.1, No.4, 2003, pp.990-1029.

④ 王勇、吕毅韬、唐天泽、谢丹夏:《平台市场的最优分层设计》,载《经济研究》,2021 年第 7 期,第 144—159 页。

⑤ 王勇、刘航、冯骅:《平台市场的公共监管、私人监管与协同监管:一个对比研究》,载《经济研究》,2020 年第 3 期,第 148—162 页。

⑥ 江小涓、黄颖轩:《数字时代的市场秩序、市场监管与平台治理》,载《经济研究》,2021 年第 12 期,第 20—41 页。

⑦ 陈伟光、钟列炀:《全球数字经济治理:要素构成、机制分析与难点突破》,载《国际经济评论》,2022 年第 2 期,第 60—87 页。

⑧ 孙晋:《数字平台的反垄断监管》,载《中国社会科学》,2021 年第 5 期,第 101—127 页。

原则,重构反垄断法及监管体系,实现数据价值的共建、共谋、共享和共治,助力增强中国数字经济的国际竞争力。① 总体而言,这类研究聚焦数字经济监管,其根本逻辑是通过对平台企业的合理监管,从而克服大数据"杀熟"和"二选一"不正当竞争等市场失灵问题,实现社会总体福利最大化。尽管这类研究也涉及数字经济安全议题,但讨论的问题仍局限于用户隐私与企业经营层面的安全,并未上升到国家安全层面。

第三类研究重点讨论了数字技术发展对国家和国际安全带来的新挑战。约瑟夫·奈(Joseph S. Nye)在传统的国际关系分析框架中加入了网络空间这个变量,探讨了网络威慑的概念、手段及实现策略,提出了网络空间威慑的四种途径,进而构建了网络空间治理的国际关系理论。② 米尔顿·米勒(Milton L. Mueller)聚焦互联网治理中的政治因素,认为互联网超越了传统民族国家的边界,并导致国家与全球化监管之间的冲突。③ 托马斯·里德(Thomas Rid)反驳了网络战争即将到来的传统观点,认为技术的发展使得发动网络攻击的门槛越来越高,降低了发生大规模冲突和战争的概率。④ 纳兹利·乔克里(Nazli Choucri)构建了一个网络空间国际关系的分析框架,从国家、国际和全球三个不同的体系层次预测和分析了存在的网络威胁及其对国家安全和国际稳定带来的挑战。⑤ 阎学通和徐舟认为,主要国家在网络空间竞争的重要性已经超越了传统的地缘竞争,网络安全正在成为国家安全的核心。⑥ 刘杨钺梳理了国际政治框架下研究网络安全的三种视角,认为网络安全的内涵应包括四个维度,即网域安全、系统安全、发展安全和信息安全。⑦ 蔡翠红认为,由美国引导的大国网络博弈的地缘政治趋势对全球网络安全形势构成了威胁,因此中国应与各国携手建设网络空间命运共同体。⑧ 上述研究重点讨论了网络空间安全的内涵及实现路径,但现实中的网络空间的安全风险无法彻底根除,绝对安全无法实现,特别是数字技术发展的不确定性带来了未知的安全风险,不安全感又会促使各国持续增加安全投入而忽视成本与收

① 杨东:《论反垄断法的重构:应对数字经济的挑战》,载《中国法学》,2020 年第 3 期,第 206—222 页。

② Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol.41, No.3, 2016, pp.44-71.

③ Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge: MIT Press, 2010.

④ Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol.35, No.1, 2012, pp.5-32.

⑤ Nazli Choucri, *Cyberpolitics in International Relations*, Cambridge: MIT Press, 2012.

⑥ 阎学通、徐舟:《数字时代初期的中美竞争》,载《国际政治科学》,2021 年第 1 期,第 24—55 页。

⑦ 刘杨钺:《国际政治中的网络安全:理论视角与观点争鸣》,载《外交评论》,2015 年第 5 期,第 117—138 页。

⑧ 蔡翠红:《网络地缘政治:中美关系分析的新视角》,载《国际政治研究》,2018 年第 1 期,第 9—37 页。

益之间的效率问题,由此进一步增加了数字空间的军备竞赛风险。

尽管经济学、管理学和政治学领域的研究都对数字经济治理进行了探讨,但既有研究或是侧重促进数字经济的发展,或是聚焦维护相关领域的安全,较少有研究将发展和安全两个目标结合起来建立令人信服的理论分析框架。本文认为,数字经济治理的关键是要平衡好发展和安全的关系,因此对相关问题的研究也应在"统筹国内国际两个大局、发展安全两件大事"的基础上,[①]从平衡发展和安全的视角出发,采取理论模型和案例分析相结合的研究方法,探索实现数字经济治理的最优路径。

三 理论模型

张宇燕和冯维江构建了一个一般性的理论框架,[②]用于研究一国在资源约束的前提下发展和安全的投入产出关系,分析了权衡发展和安全目标后的最优安全水平。本文在建构理论模型时,借鉴了张宇燕和冯维江在《新时代国家安全学论纲》一文中的基本分析框架,同时考虑到数字经济发展产出的规模效应、数据本身具有开放性和共享性等数字经济的特殊性,调整了部分模型假设。基于该理论模型,本文依次分析了数字经济的基准情景、依附型合作、大国竞争和共享共治四种不同的情景,求解出在不同情景下国家统筹数字经济发展和安全的绩效,进而比较了不同情景下的全球总体福利水平。需要强调的是,本文讨论的四种典型情景在现实的数字治理实践中往往会混合出现,但这并不妨碍本模型作为分析工具的理论意义。

(一)模型基本设定

本文认为,数字经济治理面临着"安全—发展"的权衡问题。首先,假设发展成果 y 与安全能力 s 是一对完全互补品(perfect complement),即行为体的总效用函数等于发展成果和安全能力的最小值,表达式为 $u=min\{y,s\}$。当 $y>s$ 时,安全能力能够保护的利益规模小于发展成果,超出保护能力范围的发展成果会损失掉,此时总效用函数等于安全能力 $u=s$;当 $y<s$ 时,安全能力能够保护的利益规模大于发展成果,此时总效用函数等于发展成果 $u=y$;当 $y=s$ 时,行为体安全能力所能保护的利益与其所产出的发展成果相当,此时达到均衡状态,即 $u=y=s$。

其次,假设行为体在数字经济领域的发展成果 y 由两个因素共同决定:数字技术

① 《习近平著作选读》(第二卷),第 537 页。

② 本文构建的一般性理论框架用以锚定、理解和分析国家安全领域的重要议题及其发展背后的约束条件与演变逻辑,而不是直接用作安全治理的政策工具。参见张宇燕、冯维江:《新时代国家安全学论纲》,载《中国社会科学》,2021 年第 7 期,第 141 页。

水平 a 和数字发展投入 x。考虑到数字经济具有规模报酬递增的特征,因此假设数字发展成果的生产函数 y 是关于发展投入 x 的平方项,即 $y=ax^2$。假设行为体在数字经济领域的安全能力 s 也由两个因素决定:数字安全产出效率 b 和数字安全投入 z,并假设其生产函数的表达式为 $s=bz$。①

最后,假设行为体可用于数字经济投入的资源总量 l 是有限的,投入数字经济安全建设的资源量 z 和投入数字经济发展的资源量 x,满足关系 $x+z=l$。以数据治理为例,数据是数字经济发展的核心要素,然而大规模数据的共享和开放也会带来安全风险,事关个人信息保护和国家经济政治安全;与此同时,加大数据安全的治理力度一定程度上也会成为产业创新的约束条件。

(二)基准情景

基准情景是指一国在封闭的条件下完全独立决策,仅将本国的资源投入到发展和安全建设中,以实现效用最大化的目标,而不考虑国际合作和竞争等因素的影响。下面讨论在基准情景下,国家数字经济发展和安全的投入产出选择。

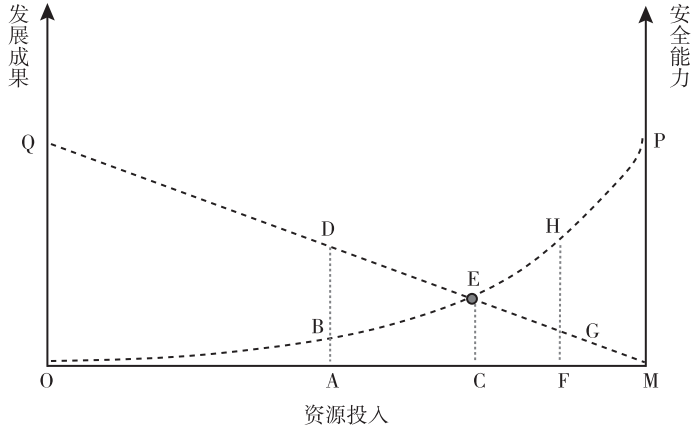

图 2　基准情景下发展和安全的投入产出关系

资料来源:笔者自制。

图 2 展现了基准情景下代表性国家的数字经济发展和安全的投入产出关系示意图。其中,曲线 OP 是一国数字经济发展成果的投入产出函数($y=ax^2$)的曲线,横坐标(左起)代表发展资源投入,纵坐标代表发展成果产出。直线 MQ 是该国数字经济安

① 为简化计算,本文假设数字安全能力产出是安全投入的线性函数。在稳健性检验部分,本文也修改了该假设,将数字安全产品的生产函数修改为边际报酬递增函数,即 $s=bz^2$,发现本文的主要结论依然成立。

全能力的投入产出函数($s=bz$)的曲线,横坐标(右起)代表安全资源投入,纵坐标代表安全能力产出。OM 代表该国全部可投入的资源,线段上不同的点代表不同的资源配置方式。本文讨论了三种资源配置方式:第一,当安全—发展的资源分配点位于 F 时,代表投入 OF 的资源用于发展,产出了 FH 的发展成果,同时投入 FM 的资源用于安全,产出 FG 的安全能力,此时 GH 段的发展成果得不到安全保障,该国数字经济处于安全能力不足的状态,效用水平为 FG。第二,当资源分配点位于 A 时,代表投入 OA 的资源用于生产发展成果,投入 AM 的资源用于建设安全能力,此时产出的安全能力可以保障 AD 水平的发展成果,而实际的发展产出仅为 AB,该国处于安全供给过度状态,效用水平为 AB。第三,当资源分配点位于 C 时,代表投入 OC 的资源用于生产发展成果,投入 CM 的资源用于建设安全能力,此时生产的安全能力 CE 恰好等于其发展成果 CE,该国处于均衡安全状态,效用水平为 CE。通过比较这三种资源配置方式下的效用水平,我们可以发现一国在基准情景下,其数字经济的安全—发展的资源最优分配点应位于 C 点,此时效用水平最高,任何偏离该点的配置方式都会造成安全能力过剩或不足,带来绩效损失。这表明,在基准情景下国家对数字安全的投入应当止于均衡安全水平 CE。

接下来,通过求解均衡安全水平的函数表达式,分析其影响因素。在基准情景下,国家面临的最优化问题如式 1 所示:

$$\max_{x,z}\min\{ax^2, bz\} \quad s.t. \quad x+z=l \qquad \text{式 1}$$

对式 1 求最优解,可以得到均衡状态下的数字经济发展成果y^*和安全能力s^*,满足:

$$y^*=s^*=bl+\frac{b^2}{2a}-\frac{b\sqrt{b^2+4abl}}{2a} \qquad \text{式 2}$$

根据式 2,一国在基准情景下的均衡安全水平s^*由三个因素共同决定:数字技术水平 a、数字安全产出效率 b 和可投入资源总量 l。图 3 进一步展示当这三个因素发生变化时对均衡状态下的安全能力和资源配置方式的影响。给定其他因素保持不变,当一国数字技术水平 a 提高时,其数字经济发展成果的投入产出曲线将由 OP1 变为 OP2,从而使该国均衡状态下的发展能力(发展成果)由 C1E1 提高至 C2E2,投入安全能力建设的资源也由 MC1 增加至 MC2;当一国数字安全产出效率 b 提高时,其数字经济安全能力的投入产出曲线将由 MQ1 变为 MQ2,从而使该国均衡状态下的安全能力(发展成果)由 C1E1 提高至 C3E3,投入安全能力建设的资源也由 MC1 减少至 MC3。

当一国数字经济可投入资源总量 l 扩大时,其发展成果的投入产出曲线将由 OP1 延长至 OP3,安全能力的投入产出曲线将由 MQ1 平移至 NQ3。在新的均衡下,该国的数字经济安全能力和发展成果也会由 C1E1 提高至 C4E4。

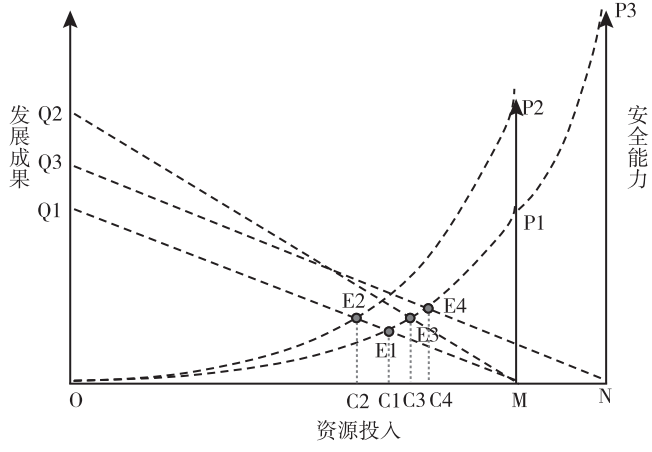

图 3　基准情景下均衡安全水平的影响因素

资料来源:笔者自制。

综上,在基准情景下,国家对数字安全的投入应止于均衡安全水平,此时该国生产的安全能力恰好等于发展成果,任何高于或低于均衡点的安全投入都会带来资源错配和社会福利的损失。提升数字技术水平、安全产出效率或扩大可投入资源总量,均可提高均衡状态下的安全能力和发展水平,同时也会带来资源最优分配比例的变化。其中,安全产出效率的提高会带来总资源中发展投入占比上升,而仅提高数字技术水平会导致总资源中安全投入占比上升。这意味着数字技术水平在提高的同时,也要同步提升数字安全的产出效率,否则会导致均衡状态下需要投入更多的资源用于数字安全能力建设,留给发展投入的资源也会相应减少,从而容易使数字经济治理陷入越发展越不安全、保障安全却阻碍发展的逻辑怪圈。因此,提升数字安全的产出效率是改善数字经济治理绩效的关键。

(三)依附型合作情景

依附型合作情景是指主导国与依附国之间进行的数字经济治理合作,其中的主导国可以在很大程度上利用依附国的资源发展数字经济,同时为依附国提供安全保护。考虑到数字经济的特殊性,数据是其重要的生产要素并具有非竞争性,因此主导国使用资源并不影响依附国的自身使用。为便于分析,假设主导国(A 国)无论是在数字

技术水平还是在数字安全产出效率上,资源总量都高于依附国(B 国),即$a_A>a_B$,$b_A>b_B$,$l_A>l_B$。

图 4 是 A、B 两国的数字经济发展和安全在依附型合作情景下的投入产出关系示意图。B 国将全部的资源 MN 投入数字经济发展,并产出发展成果 NP2,同时要求 A 国为其建设与发展成果相匹配的安全能力 KH。在该情形下,由于 B 国向 A 国开放了全部资源,因此 A 国可用资源总量扩大为 ON。相应地,其发展成果的投入产出曲线将由 OP1 延长至 OP3。考虑到 A 国需要投入 KN 段资源帮助 B 国建设其安全能力,因此 A 国国内安全能力的投入产出曲线将由 MQ1 平移至 KQ3。在新的均衡下,A 国的数字经济安全能力和发展水平为 GE2,B 国为 NP2。代入函数表达式,可以解得两国的均衡发展成果y_A^{**}、y_B^{**}和均衡安全能力s_A^{**}、s_B^{**},如式 3 和式 4 所示:

$$y_A^{**}=s_A^{**}=b_A l_A+\frac{b_A^2}{2a_A}+l_B(b_A-a_B l_B)-\frac{b_A\sqrt{b_A^2+4a_A b_A l_A+4a_A l_B(b_A-a_B l_B)}}{2a_A} \quad \text{式 3}$$

$$y_B^{**}=s_B^{**}=a_B l_B^2 \quad \text{式 4}$$

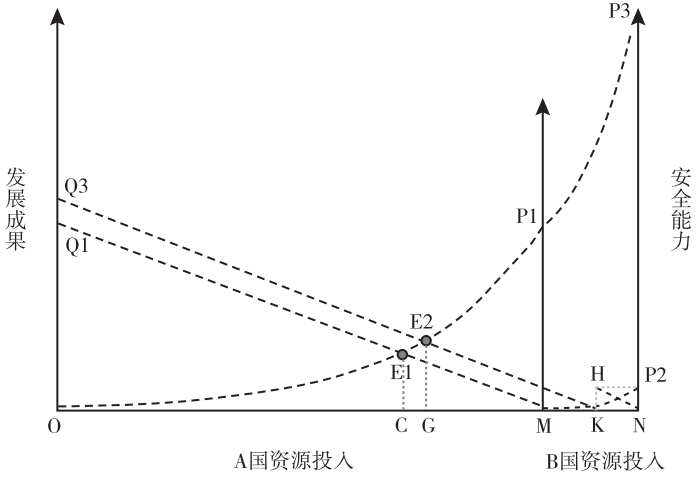

图 4　依附型合作情景下发展和安全的投入产出关系

资料来源:笔者自制。

为了对比依附型合作情景和基准情景下的数字经济治理绩效,参考式 2 中基准情景下的均衡结果,得到 A、B 两国各自独立决策时的均衡发展成果y_A^*、y_B^*和均衡安全能力s_A^*、s_B^*,如式 5 和式 6 所示:

$$y_A^* = s_A^* = b_A l_A + \frac{b_A^2}{2a_A} - \frac{b_A\sqrt{b_A^2 + 4a_A b_A l_A}}{2a_A} \quad \text{式 5}$$

$$y_B^* = s_B^* = b_B l_B + \frac{b_B^2}{2a_B} - \frac{b_B\sqrt{b_B^2 + 4a_B b_B l_B}}{2a_B} \quad \text{式 6}$$

基于式 3 至式 6,本文使用数值模拟的方法计算了 A、B 两国从基准情景转向依附型合作情景后均衡安全水平的变化,并在图 5 中使用三维坐标系呈现这一结果。对 B 国而言,依附型合作使得其均衡状态下的安全能力和发展成果相比基准情景都有了提升,即$y_B^{**}=s_B^{**}>y_B^*=s_B^*$;对于 A 国而言,当且仅当$b_A>a_B l_B$时,依附型合作的结果才优于其基准条件下的均衡,即$y_A^{**}=s_A^{**}>y_A^*=s_A^*$。这意味着只有当 A 国的安全产出效率$b_A$足够高时,其帮助 B 国建设安全能力所付出的资源才能大于其使用 B 国资源的收益,此时依附型合作才能成为对两国福利的帕累托改进。

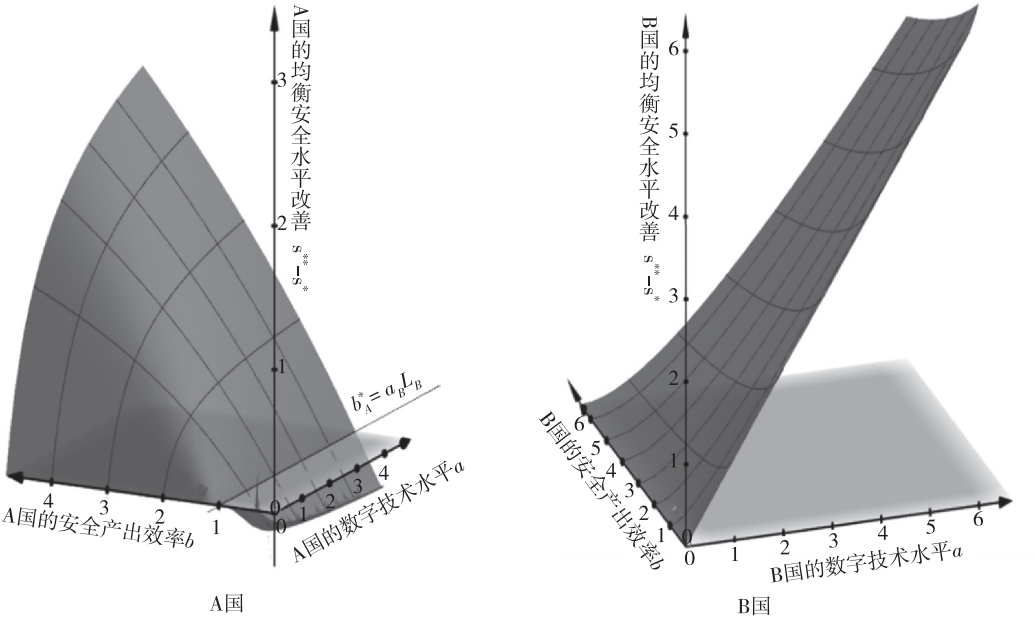

图 5　从基准情景到依附型合作的均衡安全水平改善

资料来源:笔者自制。

综上,在依附型合作情景下,在数字技术水平、安全产出效率和资源总量上占据优势的主导国可以同实力较弱的依附国开展合作,从而同步提升双方均衡状态下的安全能力和发展成果,实现从基准均衡向依附型合作均衡的帕累托改进。但是,上述结论

的成立需要满足一定条件,即主导国的安全产出效率越高,依附国的资源总量越小、数字技术水平越低,这种依附型合作越容易达成。这表明在数字经济治理领域的依附型合作往往发生在互补性较强的两国之间。而对于实力接近的国家来说,依附型合作给双方同时带来的福利改善效果并不显著。

(四)大国竞争情景

大国竞争情景是指国家在数字经济领域开展竞争博弈,其中一国生产的超额安全能力可以转化为对竞争对手的威胁。鉴于大国竞争情景往往出现在实力相近的国家之间,因此为了简化分析,本文假设两国资源总量都相同,即$l_A=l_B$,其中领先国(A 国)在数字技术和数字安全产出效率方面都高于新兴发展国(B 国),即$a_A>a_B$,$b_A>b_B$。

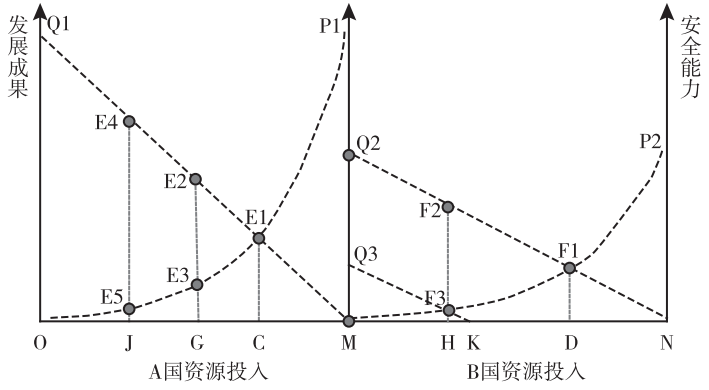

图 6 大国竞争情景下发展和安全的投入产出关系

资料来源:笔者自制。

图 6 是 A、B 两国的数字经济发展和安全在大国竞争情景下的投入产出关系示意图。在该情景下,领先国(A 国)为了获取更大的竞争优势,会倾向于偏离其封闭情景下的资源最优配置点 C,而且选择减少发展投入、将更多资源投入安全能力建设的配置点 G。此时,A 国生产出 GE2 水平的安全能力、GE3 水平的发展产出,从而具备了 E2E3 水平的超额安全能力。在大国竞争情景下,A 国的这种超额安全能力会转化为对 B 国的威胁能力,B 国的安全能力投入产出曲线会从 NQ2 下降为 KQ3,下降幅度等于 A 国的超额安全能力,即 Q2Q3=E2E3。同时,B 国在均衡安全状态下的发展水平也将由基准情景下的 DF1 下降为 HF3。在大国竞争情景下,B 国出于应对 A 国威胁的需要,也会主动提前储备与 A 国等量的超额安全能力。换言之,只要观察到 A 国储备了 E2E3 水平的超额安全能力,B 国也会将资源配置点从封闭均衡下的 D 点调整为 H 点,获得 F2F3 的超额安全能力,且 F2F3=E2E3。此时,A、B 两国会进入大国竞争情

景下的新均衡状态。假设两国都储备 λ 水平的超额安全能力,带入函数表达式,可以解得两国的均衡状态下的发展成果y_A^{***}、y_B^{***}和安全能力s_A^{***}、s_B^{***},如式 7 至式 10 所示:

$$y_A^{***} = b_A l_A + \frac{b_A^2}{2a_A} - \lambda - \frac{b_A\sqrt{b_A^2 + 4a_A b_A l_A - 4a_A\lambda}}{2a_A} \quad \text{式 7}$$

$$y_B^{***} = b_B l_B + \frac{b_B^2}{2a_B} - \lambda - \frac{b_B\sqrt{b_B^2 + 4a_B b_B l_B - 4a_B\lambda}}{2a_B} \quad \text{式 8}$$

$$s_A^{***} = b_A l_A + \frac{b_A^2}{2a_A} - \frac{b_A\sqrt{b_A^2 + 4a_A b_A l_A - 4a_A\lambda}}{2\,a_A} \quad \text{式 9}$$

$$s_B^{***} = b_B l_B + \frac{b_B^2}{2a_B} - \frac{b_B\sqrt{b_B^2 + 4a_B b_B l_B - 4a_B\lambda}}{2a_B} \quad \text{式 10}$$

基于式 5 至式 10,通过对比大国竞争情景和基准情景下的数字经济治理绩效,可以发现在大国竞争情景下,A、B 两国均衡状态下的发展成果均低于基准的情景,其表现为$y_A^{***}<y_A^{*}$、$y_B^{***}<y_B^{*}$,安全能力均高于基准的情景$s_A^{***}>s_A^{*}$、$s_B^{***}>s_B^{*}$,效用水平均低于基准情景。这说明同基准情景相比,大国竞争带来了资源错配,降低了两国在均衡状态下的效用水平。

综上,在大国竞争情景下,两国为应对潜在的安全风险,都会选择储备超额安全能力、减少均衡状态下的发展成果产出,同基准情景相比造成了福利损失。需要强调的是,大国竞争情景下的均衡非常不稳定,参与博弈的双方都有激励进一步增加其安全投入以获得超过竞争对手的安全优势,从而可能演变为一场“安全竞赛”。在极端情况下,领先国(A 国)会选择维持高于新兴发展国(B 国)最大安全能力的超额安全水平,从而迫使 B 国把全部资源投入到安全能力建设中并完全放弃发展。换言之,B 国要想妥善应对 A 国的威胁,解决之道并不是简单增加安全投入;只有当 B 国主动提高自身的数字安全产出效率且使其最大安全能力赶超 A 国,A 国才会放弃极限施压的策略。

(五)共享共治情景

在共享共治情景下,各国为实现社会整体福利最大化的目标,发挥技术、数据和安全的公共产品属性,以共享共治的理念在数字经济领域开展合作。仍然假设有两个国家(A 国和 B 国),A 国无论是数字技术水平还是数字安全产出效率,其资源总量都高于 B 国,即$a_A>a_B$,$b_A>b_B$,$l_A>l_B$。

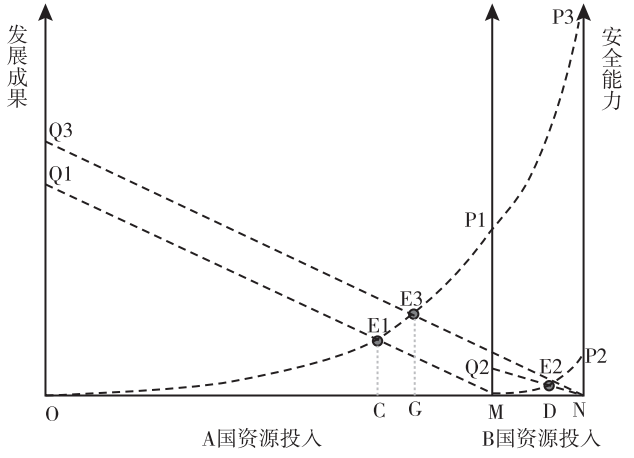

图 7　共享共治情景下发展和安全的投入产出关系

资料来源:笔者自制。

图 7 是在共享共治情景下 A、B 两国的数字经济发展和安全的投入产出关系示意图。在该情景下,A、B 两国会结成“共同体”来决定其最优安全和发展投入:由于两国技术充分共享,因此共同体的数字技术水平等于两国技术水平的最大值,即$a^{*}=a_{A}$;由于两国数据充分共享,因此可投入的总资源水平等于两国资源的总和,即$l^{*}=l_{A}+l_{B}$;由于两国安全共建,两国将数字安全能力作为一种国际公共产品合作提供,且安全产出效率等于两国产出效率的最大值$b^{*}=b_{A}$。如图 7 所示,两国的数字经济发展成果投入产出曲线为 OP3,两国的安全能力投入产出曲线为 NQ3;在均衡状态下,两国将投入 OG 的资源用于数字经济发展,NG 的资源用于数字安全建设,并产出 GE3 水平的发展成果和安全能力。代入函数表达式,两国的均衡发展成果y_{A}^{****}、y_{B}^{****}和均衡安全能力s_{A}^{****}、s_{B}^{****},如式 11 所示:

$$y_{A}^{****}=y_{B}^{****}=s_{A}^{****}=s_{B}^{****}=b_{A}l_{A}+\frac{b_{A}^{2}}{2a_{A}}+b_{A}l_{B}-\frac{b_{A}\sqrt{b_{A}^{2}+4a_{A}b_{A}l_{A}+4a_{A}b_{A}l_{B}}}{2a_{A}}\quad\text{式 11}$$

基于式 5、式 6 和式 11,通过对比共享共治情景和基准情景下的数字经济治理绩效,可以发现在共享共治情景下,两国均衡状态下的发展成果与安全能力均高于基准下的情景,即$y_{A}^{****}=s_{A}^{****}>y_{A}^{*}=s_{A}^{*}$,$y_{B}^{****}=s_{B}^{****}>y_{B}^{*}=s_{B}^{*}$。这说明共享共治不但实现了两国各自福利水平的帕累托改进,而且在均衡状态下两国福利水平相同。

综上,本文通过构建理论模型分析了不同情景下国家统筹数字经济发展和安全的

绩效。进一步,本文将模型中所讨论的四种情景按照总体福利水平从高到低进行排序后发现,共享共治情景>依附型合作情景>基准情景>大国竞争情景的治理绩效。为检验结论的稳健性,本文修改了部分模型假设,如将数字安全的生产函数修改为边际报酬递增、将两国模型拓展到多国模型等,检验发现本文的主要结论依然稳健成立。

四 案例分析

数字经济作为一个新兴领域,世界主要大国都在探索并提出本国的数字经济治理方案。本文理论模型中提出的四种情景为分析各国数字经济治理模式提供了新视角。具体来说,基准情景适用于各国的数字治理实践,欧盟的数字经济治理模式具有代表性,本文以此为例检验基准情景的结论。依附型合作、大国竞争两种情景在现实中已经初见端倪,当前美日在数字经济领域的合作是依附型合作的典型代表,而中美在数字经济领域的竞争则体现了大国竞争的特征。共享共治作为一种理论上的最优情景,尽管在现实中并未出现,但中国提出的网络空间命运共同体理念与共享共治情景契合。

(一)基准情景:欧盟数字经济治理

欧盟在数字经济治理领域起步较早,其在治理过程中对发展和安全目标的平衡为理解基准情景提供了典型案例。欧盟长期以来重视数字安全能力建设,在个人数据保护、数字经济监管方面走在世界前列。联邦德国在 1970 年通过了世界上第一部个人数据保护法,即《黑森州数据保护法》;[①]瑞典于 1973 年出台了《瑞典数据保护法》;法国于 1978 年制定了《信息技术与自由法案》;英国也在 1984 年通过了《数据保护法》;[②]1981 年,欧洲委员会颁布了《关于在自动处理个人数据方面保护个人的公约》(简称“108 公约”),这是世界上首部聚焦个人数据保护的国际公约;[③]1995 年,欧盟颁布了《数据保护指令》(简称“95 指令”),进一步完善了欧盟的数字治理规则;[④]2018 年 5 月,欧盟的《通用数据保护条例》(GDPR)正式生效。[⑤] GDPR 的生效使全球为欧

① 王华伟:《数据刑法保护的比较考察与体系建构》,载《比较法研究》,2021 年第 5 期,第 135—151 页。

② 李春华、万其刚:《国外网络信息立法情况综述》,载《中国人大》,2012 年第 20 期,第 45—48 页。

③ Council of Europe, “Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,” https://rm.coe.int/1680078b37,访问时间:2023 年 2 月 1 日。

④ European Union, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,” https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX%3A31995L0046,访问时间:2023 年 2 月 3 日。

⑤ European Union, “General Data Protection Regulation (GDPR) Compliance Guidelines,” https://gdpr.eu/,访问时间:2022 年 12 月 14 日。

洲企业和公民提供互联网服务的企业都被纳入监管约束范围,此举成功地将欧盟的市场力量转化成了规范性权力,推动其数字空间治理原则和数字产业标准的国际化。① 除此之外,欧盟把大型互联网平台企业作为监管的重点对象,重视对平台企业的反垄断监管,以维护数字经济发展的公平竞争环境。②

欧盟长期以来强调的数字安全治理模式也在一定程度上抑制了其经济的发展。当前欧盟的数字经济发展相对滞后,在第五代移动通信技术(5G)通信、人工智能、大数据和云计算等领域的技术研发明显落后于中美两国。根据联合国发布的《2021 年数字经济报告》,在全球体量前 100 名的数字平台的市值总和中,中美两国占了近 90%,欧盟仅占 3%,远低于目前欧盟经济总量在世界经济总量中的占比(18%)。③ 为扭转这一局势,欧盟近年来在数字经济治理中更加强调发展和安全的平衡,出台了一系列政策法规,旨在提升数字经济的全球竞争力。2020 年欧盟发布了《欧洲数据战略》,该文件以数字经济发展为主要视角,概述了政策措施和未来规划,目标是到 2030 年使欧盟在数字经济中的份额与欧盟的经济比重匹配。④ 2022 年欧盟先后通过了《数据治理法》《数字服务法》和《数字市场法》,旨在加强对互联网巨头的监管,为本土中小企业发展释放空间,从而激活欧盟数字经济市场的创造力,提升欧盟在数字经济领域的竞争力和主导权。

欧盟数字经济治理起步较早,但欧盟在制定数字经济治理规则时比较强调安全能力建设,重视对个人数据隐私的保护和平台企业的监管,这在一定程度上约束了企业的创新发展,部分导致欧盟的数字经济发展落后于中美两国。在此背景下,欧盟开始调整战略,重视提升本土企业的创新能力,在数字经济治理中兼顾发展和安全两方面目标。

(二)依附型合作情景:美日数字经济治理合作

美日数字经济治理合作可被视为依附型合作情景的案例。美国帮助日本建设其数字安全治理能力,日本也积极支持美国关于数据开放共享的主张。一方面,美国凭借其科技优势,通过数字经济治理合作方式为日本在数字安全方面提供保护。美国长

① 蔡翠红、张若扬:《“技术主权”和“数字主权”话语下的欧盟数字化转型战略》,载《国际政治研究》,2022 年第 1 期,第 9—36 页。

② 钟鸣:《欧盟数字平台监管的先进经验及我国的战略选择》,载《经济体制改革》,2021 年第 5 期,第 165—172 页。

③ UNCTAD, “Digital Economy Report 2021,” https://unctad.org/webflyer/digital-economy-report-2021,访问时间:2022 年 12 月 10 日。

④ European Commission, “European Data Strategy,” https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en,访问时间:2022 年 12 月 10 日。

期以来重视数字安全和网络攻防能力建设,并积极同盟友和伙伴组建“意愿联盟”,构筑网络空间的集体防御机制。① 2019 年 4 月,美日两国的联合声明指出,“国际法适用于网络空间,网络攻击在某些情况下可以视为武装攻击,因而适用于《美日安保条约》第 5 条”,美日两国正式把网络空间安全纳入共同防卫的范畴。② 2014 年,美日成立了网络防御政策工作组,组织多轮网络安全对话,通过领导人峰会和美日安保磋商委员会等机制,在数字安全领域展开常态化合作。③ 在美国的帮助下,日本的网络空间安全水平得到了显著提升。以 2021 年东京奥运会为例,日本在奥运会期间共遭遇了约 4.5 亿次网络攻击,但在应对这些网络攻击的过程中,美国提供了大量的技术支持。④ 2022 年 11 月,日本宣布加入北约网络防御合作卓越中心,在日美同盟的基础上获得了北约数字安全力量的支持。⑤

另一方面,日本积极响应支持美国关于数据开放共享的主张。美国长期以来倡导建立跨境数据自由流动的相关规则,但在“棱镜门”事件之后受到包括欧洲国家在内的批评指责。2018 年美国国会通过了《澄清域外数据合法使用法案》,⑥以国内立法的形式赋予了美国政府对他国数据的长臂管辖权,其本质是要求他国数据对美国的单向开放。尽管美国的数字霸权行径受到了包括欧盟在内的多方抵制,但日本还是对其予以了积极回应。2019 年 6 月,日本在二十国集团(G20)大阪峰会上提出了“基于信任的跨境数据流动”理念,其核心内容同样是倡导数据自由开放流动,这其实是对美国数据话语权的附和。⑦ 2019 年 10 月,日本签署了《美日数字贸易协定》,反对各国对数字产品和服务征税,保证在所有领域进行无障碍的跨境数据交易。⑧ 除此之外,日

① The White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf,访问时间:2022 年 12 月 12 日。

② Ministry of Foreign Affairs of Japan, “Japan-U.S. Security Consultative Committee (Japan-U.S. ‘2+2’),” https://www.mofa.go.jp/na/fa/page3e_001008.html,访问时间:2022 年 12 月 12 日。

③ 江天骄:《美日网络安全合作机制论析》,载《国际展望》,2020 年第 6 期,第 127—145 页。

④ “US-Japan Cybersecurity Cooperation: Beyond the Tokyo 2020 Olympics,” https://pacforum.org/publication/us-japan-cybersecurity-cooperation-beyond-the-tokyo-2020-olympics,访问时间:2022 年 12 月 14 日。

⑤ 《日本加入北约网络防御合作卓越中心居心叵测 警惕日本与北约加速勾连》,http://www.news.cn/mil/2022-11/17/c_1211701740.htm,访问时间:2022 年 11 月 17 日。

⑥ The 115th Congress of the United States, “H.R.4943-CLOUD Act,” https://www.congress.gov/bill/115th-congress/house-bill/4943/text,访问时间:2022 年 12 月 24 日。

⑦ Ministry of Foreign Affairs of Japan, “G20 2019 Japan Leaders’ Special Event on Digital Economy,” https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/special_event/,访问时间:2022 年 12 月 21 日。

⑧ US Trade Representative, “U.S.-Japan Digital Trade Agreement Text,” https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text,访问时间:2022 年 12 月 12 日。

本还通过加入美国主导的“印太经济框架”,在数字技术标准制定、数字贸易规则和跨境数据流动等方面支持美国构建以遏制中国为目标的“包围圈”。

美日数字经济治理合作在本质上是要建立一个以美国为中心的数字霸权体系,体现了依附型合作的特征。这种依附型合作还体现在其他多边机制中,如跨境隐私规则体系、全面与进步跨太平洋伙伴关系协定(CPTPP)和美墨加协定(USMCA)等。在该模式下,主导国凭借其在数字技术水平、安全产出效率和资源总量上的优势,获取了对体系中其他国家的非对称权力,而依附国则处于边缘位置,向主导国开放国内资源并接受其安全保护。这种依附型合作存在三方面缺陷:其一,主导国以本国效用最大化为目标进行资源配置,进而实现本国数字经济发展和安全的平衡,而这种资源配置方式在很大程度上会损害他国的福利水平。其二,主导国为维持自身的优越地位会凭借其权力对其他国家进行技术封锁、安全威胁和资源剥削,从而长期固化“中心—外围”的体系结构。其三,依附型合作体系得以维持的前提是主导国长期对他国数字主权、安全和发展利益的损害,难以实现体系内所有国家福利的普遍提升,因而不具有可持续性。

(三)大国竞争情景:中美数字竞争

中美数字竞争可被视为大国竞争情景的案例。美国长期以来都是全球数字经济第一大国,而中国作为数字经济的第二大国,对美差距缩减的趋势明显。因此,美国 2023 年发布的《国家网络安全战略》将中国视为“最广泛、最活跃和最持久的威胁”,声称“美国将动用一切国家力量来瓦解和摧毁威胁美国利益的行为体”。① 一方面,美国把同中国的相互依赖关系武器化、供应链问题安全化,以国家安全为由限制中国数字经济的发展。自 2018 年中美贸易摩擦以来,以华为和中兴为代表的中国企业被美国政府列入制裁名单。特朗普政府时期,美国启动了“净网行动”,力图将中国的数字企业排除在美国市场之外。拜登政府基本延续了特朗普政府的对华科技遏压政策,通过采取加大对本国科技投入、扩大对华企业制裁以及加紧构建排华小圈子等手段筑起“小院高墙”,以供应链安全和数据安全为由限制打压中国芯片制造和互联网应用等数字经济产业的发展。除此之外,美国政府还发布了《美国国防部云战略》《美国数据隐私和保护法案》等文件,强化了美国在数字领域的安全保障能力。②

① The White House, “National Cybersecurity Strategy,” https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf,访问时间:2023 年 4 月 23 日。

② US Department of Defense, “DoD Cloud Strategy,” https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF,访问时间:2022 年 12 月 20 日;US Congress, “H.R.8152-American Data Privacy and Protection Act,” https://www.congress.gov/bill/117th-congress/house-bill/8152/all-actions?overview=closed#tabs,访问时间:2022 年 12 月 20 日。

另一方面,中国通过着力提升自主创新水平以应对美国的遏压。芯片断供“卡脖子”问题让中国认识到供应链中的短板和风险,提升经济安全水平、实现核心技术自主可控成为社会各界的共识并采取了积极有效的应对措施。中美发生贸易摩擦以来,中国各级政府密集出台了一系列政策扶持半导体行业的发展,为相关企业提供土地、税收、人才、技术和资金等方面的支持;以华为、小米和吉利汽车等为代表的中国企业也纷纷加快了国产芯片的研发步伐,国产替代成为大势所趋。2018 年以来,金融领域的大量投资涌入芯片领域。根据《财经》杂志统计,2018—2020 年的三年间,中国半导体投资额超过了过去 10 年的总和。① 在立法层面,中国政府出台了《网络安全法》《数据安全法》《个人信息保护法》和《数据出境安全评估办法》等法律法规,强化数字安全体系和能力建设。

在中美数字竞争的背景下,两国都将大量资源投入安全能力建设,这也体现了大国竞争情景的特征。在大国竞争的情景下,领先国和新兴发展国都有动机选择将更多资源投入数字安全能力建设,这可能偏离资源的最优配置水平,造成资源错配并阻碍数字经济的发展。与此同时,各国通过不断增加安全投入的方式来缓解各自的安全焦虑,可能会让国家陷入“数字安全竞赛”的困境,增加系统性风险,带来更大的安全隐患。

(四)共享共治情景:网络空间命运共同体

网络空间命运共同体是习近平 2015 年在第二届世界互联网大会上提出的治理主张,“网络空间是人类共同的活动空间,网络空间前途命运应由世界各国共同掌握。各国应该加强沟通、扩大共识、深化合作,共同构建网络空间命运共同体”。② 2022 年习近平向乌镇峰会致贺信时又明确指出,“加快构建网络空间命运共同体,为世界和平发展和人类文明进步贡献智慧和力量”。③ 网络空间命运共同体的理念主张与共享共治情景具有一致性。一方面,网络空间命运共同体坚持共商共建共享的全球治理观,有助于释放数字经济的发展潜力,各国共享发展成果。网络空间命运共同体强调“发展共同推进、安全共同维护、治理共同参与、成果共同分享”;④主张构建利益共同体,“确保不同国家、不同民族、不同人群平等享有互联网发展红利”。⑤ 在该理念的指

① 财经网:《中国芯片业这三年》,https://news.caijingmobile.com/article/detail/428351?source_id=43,访问时间:2023 年 1 月 4 日。

② 《习近平谈治国理政》(第二卷),外文出版社 2017 年版,第 534 页。

③ 《习近平向 2022 年世界互联网大会乌镇峰会致贺信》,载《人民日报》,2022 年 11 月 10 日。

④ 世界互联网大会:《携手构建网络空间命运共同体行动倡议》,https://cn.wicinternet.org/2020-12/29/c_173670.htm,访问时间:2022 年 12 月 20 日。

⑤ 中华人民共和国国务院新闻办公室:《携手构建网络空间命运共同体》,http://www.scio.gov.cn/zfbps/32832/Document/1732898/1732898.htm,访问时间:2022 年 12 月 7 日。

引下,数字技术、数据资源和网络安全的国际公共产品属性才能被充分释放,有助于弥合数字鸿沟,促进全球普惠包容发展,让各国共享数字发展红利。

另一方面,网络空间命运共同体倡导开放合作的网络安全理念,有助于促进各国合作实现数字安全目标。网络空间命运共同体主张“加强关键信息基础设施保护国际合作,维护互联网基础资源管理体系安全稳定,合作打击网络犯罪和网络恐怖主义……反对以牺牲别国安全谋求自身所谓绝对安全,反对一切形式的网络空间军备竞赛”。① 在数字时代,各国面对的传统和非传统安全威胁更加复杂多变,跨地区、跨国家的攻击可以通过互联网高频率、低成本完成,增加了监管难度和治理成本。网络空间命运共同体倡议有助于促进各国合作应对全球性威胁和挑战,共同维护网络空间和平、安全和稳定。

网络空间命运共同体是中国提出的数字经济治理理念,体现了共享共治情景的特征。共享共治情景可以充分发挥数字技术、安全能力和数据资源的公共产品属性,通过在共同体层面实现发展和安全的平衡,有助于释放数字发展红利、促进各国合作实现总福利最大化的目标。因此,中国提出的网络空间命运共同体倡议,有助于在全球层面实现数字经济高质量发展与高水平安全的动态平衡。

五 结论

数字经济治理的关键是平衡好发展和安全的关系。本文基于《新时代国家安全学论纲》一文的理论框架,从统筹发展和安全的视角出发,分析了数字经济治理的不同模式和路径选择。本文通过构建理论模型分析了基准情景、依附型合作、大国竞争和共享共治四种数字经济治理情景,研究了数字经济背景下国家统筹发展和安全的绩效,并对不同情景的总福利水平进行了排序。本文将欧盟数字经济治理、美日数字经济治理合作、中美数字竞争和网络空间命运共同体四个典型案例与理论模型中的四种情景对应,探讨了在全球层面实现数字经济治理发展和安全平衡的路径,得出四点结论。

第一,在基准情景下,国家对数字安全的资源投入应当止于均衡安全水平,如果偏离了该资源配置方式,就会造成安全能力过剩或不足,带来绩效损失。在现实中,由于数字技术发展服从摩尔定律,技术的快速迭代进步在提高数字经济发展成果产出的同时,也导致安全能力的不足。此时,若能同步提升数字安全的产出效率,便可在资源配

① 中华人民共和国国务院新闻办公室:《携手构建网络空间命运共同体》,http://www.scio.gov.cn/zfbps/32832/Document/1732898/1732898.htm,访问时间:2022 年 12 月 7 日。

置方式不变的情况下实现更高水平的发展和安全平衡。因此,提升数字安全的投入产出效率是实现数字经济有效治理的关键所在。

第二,在依附型合作情景下,当主导国同依附国在数字经济治理领域展开合作时,主导国会利用依附国的资源发展数字经济,同时也会为依附国提供安全保护。然而,我们应对此合作模式保持清醒认识,依附型合作在本质上是要构建一个“中心—外围”的数字霸权体系。在该合作模式下,主导国凭借其在数字经济领域的先发优势,享有非对称权力,依附国则长期受到主导国的控制和剥削,这将固化并加剧全球数字经济发展的不平等。

第三,在大国竞争情景下,领先国和新兴发展国都有安全动机生产超额的安全能力以应对来自竞争对手的潜在威胁,但容易陷入“数字安全竞赛”困境。在该模式下,双方可能偏离实现发展和安全平衡的资源配置方式,造成绩效损失并积累系统性风险。对于新兴发展国而言,只有提高自身的数字安全产出效率,才能促使竞争对手放弃极限施压的策略。

第四,在共享共治情景下,各国如果在技术、资源和安全领域展开充分合作,那么就会在共同体的层面达到发展和安全的平衡,实现总福利最大化的目标。中国提出的网络空间命运共同体理念体现了共享共治情景的特征,这一治理模式有助于协调各国利益,在全球层面实现数字经济高质量发展与高水平安全的动态平衡。

基于统筹发展和安全的视角,本文认为数字经济治理的最优路径是在共享共治的基础上推动构建网络空间命运共同体。实现国家层面的数字经济治理要注重两方面内容:一是要探索新发展理念,通过对外开放实现高质量发展,因为不发展才是最大的不安全。二是要坚持从总体的视角看待国家安全,通过推动国家安全能力现代化实现安全产出效率的提升,实现更高水平的国家安全。对于全球数字经济合作,无论是组建以维护一国霸权为目的而不顾他国国家利益的“小圈子”,还是以“脱钩断链”的方式遏压竞争对手、制造网络空间的分裂与对抗,都会对相关各方的福利造成损害。各国只有在共享共治的基础上,以开放、互利、共赢为基础开展国际交流与合作,才能最终实现多方共赢,共享数字红利,造福全人类。

(截稿:2022 年 11 月　责任编辑:赵远良)