

“意外挑战”：乌克兰危机升级推动全球数字治理加速转向

岳云嵩¹ 薛新龙²

(1. 中国信息通信研究院, 北京 100191; 2. 对外经济贸易大学, 北京 100029)

摘要: 伴随着全球经济数字化转型, 国家间数字经贸往来大幅增多, 不同国家在跨境数据流动、人工智能治理、跨国平台监管等方面的政策法规差异成为制约发展的巨大障碍。这促使各国加强多边和区域层面对数字议题的讨论, 深化国家间政策法规协调, 使得以发展为导向的全球数字治理体系加速形成和发展。然而, 乌克兰危机升级以来出现了大量用于对抗的数字化元素, 如针对关键基础设施的网络攻击、社交媒体舆情引导与管控、两用数字技术使用、私营跨国数字企业卷入国家冲突等。各国不得不重新审视数字全球化发展与合作, 更多地将注意力从发展转向安全, 对全球数字治理发展走向产生了巨大影响。主要国家不仅加强了国内数字监管治理和国际网络安全合作, 而且积极与盟友合作争夺全球数字经贸治理主导权, 使得全球数字治理底色更保守、取向更强调安全、主导权竞争更激烈、多边解决方案更难达成。面对形势变化, 中国应通过扩大数字领域开放、完善中国数字治理方案、建立多层次数字朋友圈和充分融入多边机制数字治理谈判等方式深化对全球数字治理的影响。

关键词: 乌克兰危机; 数字治理; 数字政策; 数字技术

中图分类号: D815/F742

文献标识码: A

文章编号: 1006-1894 (2024) 03-0098-13

近年来, 全球数字经济蓬勃发展, 跨境数字贸易大幅增多, 出现了跨境数据流动、跨国数字平台监管、数字技术国际标准制定等涉及多个国家协调的数字议题。如何构建和完善全球数字治理体系, 通过一定对话协商机制, 妥善处理数字领域新出现的问题, 推动国际共识乃至国际规则的形成, 成为全球数字经贸高效、有序、公平和安全发展的关键。美欧是过往全球化发展与治理的先驱者, 数字全球化时代也是如此。它们立足数字技术产业优势, 积极与其他国家签订含有数字贸易规则的国际经贸协定, 持续对外输出以开放发展为导向、符合西方价值观和利益的数字治理理念, 在国际社会产生一定影响。然而, 2022 年乌克兰危机升级以来的一系列事件让人们深刻认识到数字技术在现代战争和经济制裁中可能扮演的角色, 严重冲击了数字领域国际合作的默契和信任, 使得全球数字治理重心很大程度从发展转向安全, 出现了一系列巨大转变。对于希望进一步参与全球数字治理体系构建的中国而言, 考察

作者简介: 岳云嵩, 中国信息通信研究院政策与经济研究所副研究员/高级工程师, 研究方向: 数字贸易与数字经济; 薛新龙(通信作者), 对外经济贸易大学国家对外开放研究院教育与开放经济研究中心副研究员, 研究方向: 教育经济学与数字人才。

基金项目: 国家社会科学基金青年项目“数字经济时代兼顾个人信息保护和数据要素市场培育的治理机制设计”(项目编号: 21CJL010); 对外经济贸易大学区域国别研究联合专项课题(项目编号: LHZX202210)。

乌克兰危机升级以来数字化元素的作用,分析全球数字治理可能发生的变化,具有重要的理论和现实意义。

一、全球数字治理内涵、特征与发展

全球数字治理源于全球数字经济快速发展以及由此出现的大量跨国数字经贸交往活动。近年来,互联网、大数据、云计算、人工智能、区块链等技术加速创新,日益融入经济社会发展各领域的全过程,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。^①据测算,2022年全球51个主要国家的数字经济规模达41.4万亿美元,同比名义增长7.4%,在GDP中的占比稳步上升,成为全球经济发展的重要支撑。^②数字经济发展具有非常突出的跨地域特点,消费者足不出户就可以获取网络上的各类型数字服务,实现福利和效用的改善;生产企业通过网络可以跨地域进行协同生产制造,分工范围由一个地区轻易拓展至整个国家乃至全世界。数字经济全球化极大促进了全球经济增长,但也带来了一系列超越传统地缘边界的新问题、新风险,促使各国出台了许多具有明显外部性的数字经济监管治理政策,使得全球经济治理主体更加复杂多元、对象更加复杂多样、机制碎片化更加明显(陈伟光和钟列炆,2022)。在此背景下,数字领域规则、规制、管理、标准等的国际协调和合作变得越来越重要。

全球数字治理主要是指各国共同认识和处理全球性数字问题,围绕数字议题沟通协商,最终构建国际数字规则、标准和行为准则的过程。在高度经济全球化的今天,全球数字治理不仅与国家间数字领域国际合作、协定签署、规则谈判紧密相关,同时也受到各国国内数字政策法规的影响,特别是来自主要经济体的影响。从治理目标看,重点是促进各国在数字领域的互信合作,推动跨国数字经贸活动降低成本、提高效率,提升国际分工深度和广度,防范全球性安全风险。从治理机制看,联合国(UN)、世界贸易组织(WTO)、经济合作与发展组织(OECD)、二十国集团(G20)等传统处理综合性国际事务的多边国际组织仍发挥着积极作用,区域贸易协定成为理念相近国家构建区域性数字治理规则的重要渠道;在国际互联网域名与地址管理组织(ICAAN)、互联网治理论坛(IGF)、国际标准化组织(ISO)等国际性机制基础上形成了允许各国政府、私营部门、公民社会、技术社群等“多利益攸关方”参与的治理模式。从治理议题看,主要聚焦数据、数字技术、数字产品、数字服务等跨境流动或贸易所引发的监管治理问题,如跨境数据自由流动、人工智能伦理、跨国平台监管、数字服务税等。

全球数字治理已由起始阶段进入上升阶段。一方面,过去10年全球数字治理取得了巨大进展。一是形成推动数字经贸发展与合作的广泛共识。作为发达国家、新兴市场国家和发展中国家沟通的重要平台,G20早在2016年杭州峰会就提出,将促进成员之间以及成员之外的沟通与合作,探讨共同利用数字机遇应对挑战、促进数

① 习近平.不断做强做优做大我国数字经济[EB/OL].2022,http://jhsjk.people.cn/article/32346871.[2022-02-07](2023-12-02).

② 中国信息通信研究院.全球数字经济白皮书(2023年)[EB/OL].2024,http://www.caict.ac.cn/kxyj/qwfb/bps/202401/P020240109492552259509.pdf.[2024-01-09](2024-01-12).

数字经济推动经济实现包容性增长和发展的路径。二是初步形成美欧等多种数字治理理念和模式。^①例如，在跨境数据流动治理上，美国为保持其全球数字市场领导地位，采用了一种市场驱动的方法，支持开放、互操作、安全和可靠的互联网，促进在线信息的自由流动；欧盟强调对个人权利、基本价值观的保护以及维护“数字主权”的目标，制定了较为严格的监管规定；此外，中国、印度、俄罗斯等新兴经济体也基于本国利益形成了各具特点的监管方式。三是在部分地区和领域形成了一定的数字治理规则。在区域层面，截至2021年底，全球已有约100个区域或双边自贸协定包含数字贸易相关条款，涉及2/3的WTO成员。部分自贸协定更是纳入数字贸易（或电子商务）专章，形成更具系统性的规则安排。在多边层面，OECD牵头推动的数字服务税“双支柱”方案、联合国教科文组织牵头推动的《人工智能伦理建议书》均取得重大进展，WTO电子商务谈判、联合国《全球数字契约》等工作也在持续推进。

另一方面，与其他成熟的全球治理领域相比，全球数字治理仍存在诸多问题和挑战。一是治理主体参与不充分，发展中国家不仅数字化发展基础较为薄弱，而且数字治理能力和参与相关规则制定的意愿也相对不足。例如，在WTO电子商务谈判中，发展中国家的参与率远低于发达国家，且很少提交有实质性内容的提案（岳云嵩和霍鹏，2021）。二是治理诉求冲突，南北国家立场分歧难以弥合。发达国家更关注降低壁垒、开放市场、自由贸易，发展中国家更关注数字能力建设、资金技术援助、中小企业发展等。两类国家利益诉求存在巨大差异，又没有一个能很好平衡各方利益的综合解决方案，使得多边层面各项治理议题的推进阻力巨大。三是治理规则赤字，急剧增长的全球数字治理需求得不到及时满足。由于数字领域议题具有新颖性和复杂性，触及国家间复杂的利益冲突，使得规制制定的速度远远慢于议题的产生速度。四是治理碎片化，主要国家治理理念和模式差异导致数字空间的分裂。全球数字治理已成大国博弈的“新赛道”，与地缘政治相互影响越来越大（张莱楠，2022）。在没有国际共识的前提下，主要国家为实现数字产业的全球扩张，开始通过区域贸易协定输出各自的数字治理理念，甚至直接打压其他国家的企业，导致出现了许多缺乏兼容性和互操作性的区域性数字空间。

二、乌克兰危机升级以来备受关注的跨国数字问题

乌克兰危机升级以来，除直接当事国外，美国、英国、法国、德国、日本等发达国家均不同程度卷入，前沿数字技术应用的深度、广度前所未有，使得一些跨国数字问题受到前所未有的重视。

（一）针对关键基础设施的网络攻击

关键基础设施是指对社会至关重要的系统和资产，一旦能力丧失或遭到破坏，就会对国家安全、经济安全、公共安全等重要领域产生影响，涉及通信、金融、供水、

^① UNCTAD.Digital Economy Report 2021[EB/OL].2021,https://unctad.org/page/digital-economy-report-2021.[2021-09-29] (2023-05-17).

运输、电力、天然气与石油、应急服务、政府运转等。^①进入 21 世纪以来, 关键基础设施的控制和运行愈发依赖信息技术, 关键基础设施的信息系统建设也日益复杂和庞大, 使得关键基础设施的网络攻防成为现代战争的重要组成部分。据媒体消息, 在乌克兰危机升级背景下, 多个冲突关联方声称其关键基础设施遭受网络攻击。2022 年 12 月, 俄罗斯外交部副部长奥列格·瑟罗莫洛托夫 (Oleg Syromolotov) 在接受媒体采访时表示, 俄罗斯今年遭受的网络攻击数量比前一年增加了 80%, 如果说攻击者去年的主要目标是金融机构, 那么今年的主要目标则是公共部门, 包括关键信息基础设施和具有社会意义的机构。^②2022 年 6 月, 乌克兰国家特别通信和信息保护局 (SSSCIP) 称, 自危机升级以来, 该国政府、地方当局及国防组织共遭受 281 次攻击, 成为受到攻击最多的部门; 除此以外, 金融、电信、能源、基础设施等领域也深受网络攻击影响。^③微软公司的一份报告梳理了危机初期俄罗斯军事行动与网络攻击的时间先后, 认为两者间存在高度的关联性。此外, 作为乌克兰一方的支持者, 意大利、黑山共和国、立陶宛、挪威等国也将其关键基础设施的网络攻击归咎于俄罗斯黑客。

(二) 社交媒体管控和网络舆情引导

过去 20 年, 全球社交媒体用户数量呈指数级增长, 达到 46.2 亿人, 约占世界总人口的 58.4%。^④除了基础的社交娱乐功能外, 社交媒体还深度融入日常生活的方方面面, 在很大程度上取代了传统的报纸、杂志和电视等媒体, 成为人们获取资讯的重要途径以及政治家和公众人物展示形象和传达政策的舞台。这导致社交媒体在现代舆论战中的价值不断增加, 成为叙述事实和塑造形象的重要工具。乌克兰危机升级被认为是第一次全面的“社交媒体战争”, 冲突关联方将社交媒体武器化, 频繁发动网络舆论攻势, 试图对冲突走势施加影响。一方面, 乌克兰总统泽连斯基活跃在社交媒体平台, 频频发布最新消息, 努力将乌克兰描绘成一个道德高尚却遭受苦难的国家, 以影响国际社会舆论, 获得资金、武器和政治支持; 另一方面, 俄罗斯积极利用国营媒体宣传, 同时限制对 Facebook、Twitter、Instagram 等境外社交媒体的访问, 从而强化冲突合理性的叙述, 争取国内支持, 打击对手士气。与传统舆论战相比, 网络空间舆论战仍然聚焦宣传道德正义、提升凝聚力、强化战斗意志等目的, 但是出现了一些新变化。第一, 手段的变化, 主要表现为通过行政命令的方式限制敌对方使用本方社交媒体平台, 或封禁敌对方主导的社交媒体平台, 以便争夺战场后方网络舆论主导权。第二, 工具的变化。数字技术在舆论战中更深度应用, 社交媒体出现大量干预舆论的社交机器人, 以及通过人工智能深度伪造形成的虚假图文

① 左晓栋. 关键信息基础设施, 保! [EB/OL]. 2015. http://www.cac.gov.cn/2015-11/04/c_1117015673.htm. [2015-11-04] (2023-05-17).

② Sumaira FH. Number of Cyberattacks against Russia Increased by 80% In 2022 [EB/OL]. 2022. <https://www.urdupoint.com/en/world/number-of-cyberattacks-against-russia-increased-1616609.html>. [2022-10-28] (2023-05-17).

③ Gatlan Sergiu. Ukraine Targeted by Almost 800 Cyberattacks since the War Started [EB/OL]. 2022. <https://www.bleepingcomputer.com/news/security/ukraine-targeted-by-almost-800-cyberattacks-since-the-war-started/>. [2022-06-30] (2023-05-17).

④ DataReportal. Digital 2022: Global Overview Report [EB/OL]. 2022. <https://datareportal.com/reports/digital-2022-global-overview-report>. [2023-01-26] (2023-05-17).

和音频内容。第三，效果的变化。舆论宣传的效率更高、传播范围更广，舆情信息在非常短时间内就可以传递给所有社交媒体用户，并在平台推送、社交媒体发酵和政府舆情干预的作用下，产生巨大的舆论影响。

（三）军民两用数字技术的发展应用

作为一种通用目的性技术，数字技术在经济社会发展和国防军队建设中均有着巨大的应用潜力，可以极大促进相关领域的成本降低、效率提升和协同优化。乌克兰危机升级以来，一些原本应用在消费生活领域的数字技术、产品和服务迅速被转变为战争工具，并展现出独特优势，在战场中初露锋芒。第一，无人机在前方战场的应用。例如，乌克兰在冲突中使用了TB-2、A1-SM Furia、PD-1s、UJ-22s等军用无人机和DJI Mavic四轴飞行器，执行包括目标识别、活动检测、空中打击、媒体素材收集等任务。^①与传统军用飞机相比，无人机具有成本低、功能多、突防能力强、战法灵活等优势，不仅可以与其他兵种开展协同作战，还可以很好地执行精准打击和高危任务，减少己方人员损失。^②第二，卫星互联网的网络协同支持。乌克兰危机爆发后不久，美国太空探索技术公司SpaceX即开始向乌克兰提供免费的“星链”（Starlink）服务，通过低地球轨道卫星提供空中无线互联网。凭借“星链”的支持，乌克兰在很大程度上克服了俄罗斯对其通信网络的干扰，确保一线部队能及时获取外部情报信息、军队指挥系统指令能顺畅传达、无人机能正常开展远程侦察和打击。有研究认为，“星链”在打击“莫斯科”号巡洋舰事件中发挥了重要作用，形成了“北约各型侦察监视平台—北约/乌军指挥控制中心—“星链”网络—前线作战部队”的信息传递网络（彭中新等，2022）。

（四）与数字经贸相关的单边制裁措施

截至2024年1月，美欧等国家已经对俄罗斯进行了10余轮制裁，可以说几乎所有可以用来制裁的手段均已使出，使得乌克兰危机升级成为检验西方国家现代制裁工具的一次绝佳机会。通过对2022年以来欧盟的数字制裁政策进行梳理，从中可以看出，数字领域已成为国家间单边制裁的重点，涉及内容包括以下6个方面。第一，数字产品相关出口管制，限制特定稀土、半导体、IT组件、软件、技术、设备等对俄罗斯出口，打击俄罗斯国防安全供应链，削弱俄罗斯技术基础和工业能力。第二，数字服务出口管制，限制俄罗斯获取金融、保险、法律、咨询等其他商业服务，这些均为对生产管理过程高度重要且可以通过数字化手段交付的服务。第三，针对数字实体和相关个人的制裁，如俄罗斯电信运营商Rostelecom等电子通信和高科技企业，限制其从国际市场获得产品和技术支持，实施债务和股权限制，甚至冻结资产。第四，针对数字媒体的制裁，暂停Rossiya RTR、Rossiya 24、TV Centre International

^① CSIS.Ukrainian Innovation in a War of Attrition[EB/OL].2023,https://www.csis.org/analysis/ukrainian-innovation-war-attrition. [2023-02-27](2023-05-17).

^② 孙焰,陈灿健.对战争影响愈发重要——无人机性能不断提升[EB/OL].2021,https://m.gmw.cn/baijia/2021-01/28/34579293.html. [2021-01-28](2023-05-17).

等俄罗斯媒体的广播活动，禁止它们通过有线电视、互联网和智能手机应用等形式在欧盟传播其内容，以及禁止在这些媒体上发布广告。第五，针对数字金融的制裁，将 Sberbank 等俄罗斯主要银行剔除出环球银行金融电信协会（SWIFT）系统，并封堵俄罗斯使用虚拟货币规避制裁的可能。第六，数字领域国际合作限制，阻碍俄罗斯正常参与相关国际标准、规则的制定。

（五）私营数字跨国企业参与国际冲突

私营数字跨国企业的崛起是全球数字经济快速发展的写照，1990 年全球市值最高的 10 家企业中只有 1 家数字企业，2020 年这个数字上升到了 7 家。由于数字经济发展受到“网络效应”“规模经济”“锁定效应”等因素影响，少数头部数字企业往往能获得更大比重的市场份额，取得巨大的商业成功。随着这些企业提供的数字产品、服务和技术在生产经营活动中的重要性不断提升，它们开始变得像公共基础设施一样无处不在。当这些具有平台特性的数字企业成长至产业和金融体量可以与中等经济强国匹敌，一旦它们具有某种政治倾向，将深刻影响国内政治和世界政治（薛晓源和刘兴华，2022）。因此，对于具备一定公共属性的数字企业，各国普遍希望它们能秉持“科技无国界”“技术中立”等原则，而且它们在大多数时候为了开拓国际市场也是这么做的。然而，乌克兰危机升级以来大量美国私营数字跨国企业摒弃过去一直坚持的原则，即便没有受到行政命令影响，仍然选择退出俄罗斯市场，甚至参与政府对俄罗斯的施压。例如，英特尔、AMD、英伟达、高通等企业中断关键元器件的供给，谷歌 Play 商店、苹果 APP 商店、Paypal 等数字生态对俄罗斯用户进行限制，微软、谷歌、SpaceX 等企业为乌克兰提供网络安全、卫星导航等支持。原因可能是多方面的，包括母国政府非官方层面施压、重点市场舆论环境影响、俄罗斯业务在全球营收中占比较低等。例如，2022 年 2 月以来，耶鲁大学管理学院持续发布与俄罗斯开展业务的企业名单，通过舆论施压迫使企业退出俄罗斯；^① 2022 年 11 月，北约秘书长延斯·斯托尔滕贝格（Jens Stoltenberg）指出，北约与 Starlink、微软、亚马逊、YouTube 等私营企业开展密切合作。

三、乌克兰危机升级与全球数字治理发展新趋势

乌克兰危机升级期间，数字领域相关技术、应用、企业和政策发挥了巨大作用，对各国数字政策乃至全球数字治理产生了深远影响。

（一）乌克兰危机升级对全球数字政策制定的影响

各国决策者由此对数字经济发展合作出现了 4 个方面的感知变化。第一，认识的加深。数字技术和产业已经成为决定国家综合实力的关键因素，对经济、政治、军事、外交等方面至关重要。第二，自主的担忧。数字领域“单边制裁”和“长臂管辖”不断增多，相关风险随着数字全球化的发展进一步提升。第三，风险的体会。网络安

^① Yale School of Management. Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain[EB/OL]. 2023, <https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain>. [2023-09-28] [2024-01-28].

全对国家安全至关重要，需要重点防范关键基础设施的网络风险。第四，默契的破坏。私营数字跨国企业受到其母国政治权力的影响，资本与技术 in 政治面前难以保持中立，放任它们进入市场和发展壮大存在巨大风险。

这些感知变化传导作用于政策层面，出现在主要经济体官方机构文件或对外表态中，成为各国制定数字领域政策法规的重要依据。例如，2023 年 9 月，欧盟委员会发布的《2023 年欧盟数字化 10 年状况报告》指出，2022 年地缘政治的重要性进一步凸显，其背景是俄乌冲突的爆发以及由于战略利益和价值观竞争所导致的部分经济领域分裂风险加剧，同时数字技术是地缘政治紧张局势和日益激烈的技术竞赛的中心。2023 年 12 月，第 9 轮欧盟—美国网络对话再次就以俄乌冲突为标志的全球网络威胁环境交换意见，并就针对供应链、关键基础设施和知识产权的恶意网络活动以及针对企业和公民的勒索软件攻击增加表示关切。2022 年 11 月，中国国家发展和改革委员会发布的《关于数字经济发展情况的报告》指出，数字经济发展的外部环境发生深刻变化，个别国家为维护自身科技垄断和霸权地位，遏制打压中国数字技术和数字产业创新发展，必须把数字技术的命脉牢牢掌握在自己手中，在科技自立自强上取得更大进展。



图 1 乌克兰危机升级暴露数字领域风险与全球数字政策取向

从具体举措看,乌克兰危机升级中备受关注的跨国数字问题亦折射出一系列数字领域安全风险,无疑将加快甚至促成各国做出相应决策部署。关键基础设施网络攻击风险,将驱动各国加强关键基础设施信息安全保护,建立更严格的管理体系,限制竞争对手设备使用,并通过国际规则对国家层面的攻击行为进行约束。社交媒体内容舆情引导风险,将使各国加强社交媒体平台和内容的监管,促进地缘政治盟友在打击虚假信息和舆情引导方面合作。军民两用数字技术应用风险,将使各国限制对竞争对手的高水平数字技术和产品出口及可替代的数字产品进口以遏制其产业发展,利用国际规则约束竞争对手的贸易保护行为以抢占国际市场。数字领域单边制裁风险,将使各国降低对竞争对手关键产品进口的依赖,并通过国内防御性贸易政策和国际规则约束潜在的单边制裁活动。数字跨国企业参与国家冲突风险,将使各国完善平台政策,明确平台的责任和义务,着力提升本土平台竞争力。

(二) 乌克兰危机升级以来全球数字治理发展趋势

各国为强化数字领域安全可能采取的政策分为两类:一类是直接政策,通过完善对内数字领域监管治理和对外网络安全合作,加强对关键领域的管控,提升技术产品自主性,直接降低安全风险;一类是间接政策,聚焦数字技术产业竞争,通过塑造有利于自身的国际规则,打击和约束竞争对手,同时积极与盟友合作,抱团增强抵御风险、赢得竞争的實力,间接降低安全风险。这些政策将藉由各国国内市场和外交互动两条路径给全球数字治理带来一系列影响。

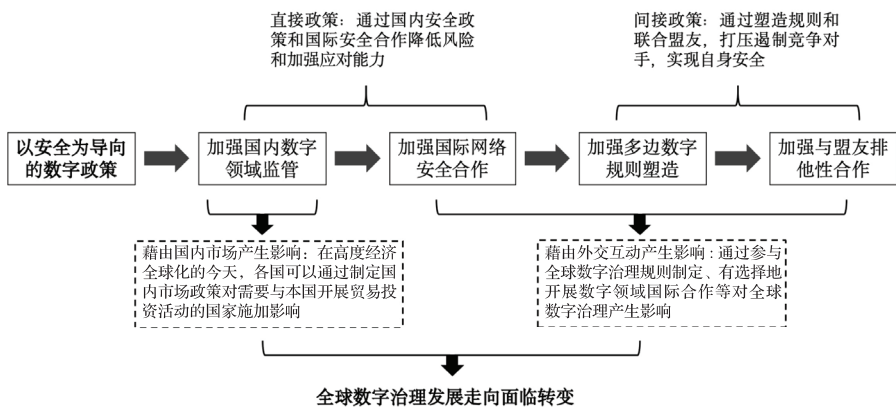


图2 从全球数字政策到全球数字治理

1. 全球数字治理底色更为封闭保守, 各国国内数字监管政策明显增多

国内治理和国际治理不是相互割裂, 而是相辅相成、互为补充、协同发展的, 国内治理是国际治理的基础和前提, 国际治理是国内治理的延伸和保障。全球治理变革表面上是国际舞台的合作较量, 实质上是国家之间的制度博弈, 是各国竞相把自己的国内制度输出为国际规则的尝试, 是各国以国内法为基础进行妥协调和的结果。^①

^① 王轶. 坚持统筹推进国内法治和涉外法治[EB/OL]. 2021, <http://sft.hebei.gov.cn/system/2021/03/30/030085133.shtml>. [2021-03-30] (2023-05-17).

通常来说，外部冲击对全球治理的影响，首先是作用在国内数字治理层面，然后才会逐渐传导到国际层面，因为国内治理的自主性和灵活性更高，更容易做出调整。

乌克兰危机升级以来，数字全球化的武器化趋势逐步明显，加剧了数字领域的信任赤字。针对暴露的风险隐患，各国竞相加强数字领域监管治理，涉及网络安全、数据保护、内容治理等多个领域。在网络安全方面，相关国家先是纷纷发布网络安全预警提示，然后通过出台政策法规强化对关键基础设施的网络安全保障。例如，日本经济产业省（METI）发布了《加强关键基础设施公司（和政府机构）网络安全措施的建议》，新加坡网络安全局（CSA）宣布将修订和扩大《新加坡网络安全法》，加拿大制定《关键网络系统保护法》，欧盟委员会制定《欧盟网络防御政策联合通信》和通过《欧盟网络团结法案》，美国发布《国家网络安全战略》，澳大利亚政府结束了《2023~2030 年澳大利亚网络安全战略》讨论文件的磋商。在数据治理方面，各国数据保护立法体系建设明显加快，对公民数据安全、国家经济利益的考量更加全面。例如，泰国、越南、古巴、尼日利亚、巴基斯坦等国相继实施个人数据保护法；美国对跨境数据流动的政策立场发生重大转变，先是放弃在 WTO 电子商务谈判中对数据本地化、跨境数据流动等议题的支持，^①随后又发布行政命令限制敏感数据流向中国等关注国家；印度发布了第 4 版《个人数据保护法案》（草案），删除了数据本地化存储要求、数据泄露的刑事责任、可携权和被遗忘权等内容；欧盟理事会通过《数据法案》，促进“数字单一市场”的数据流动，确保相关方更公平地参与数据价值分配。大量涉及具体领域的数字保护政策法规出台，如工信产业、金融产业、移动应用、未成年人等。在数字内容方面，各国加强了平台中介的审核责任，加强对虚假信息、非法信息的打击力度。例如，印度通过《信息技术（中介准则和数字媒体道德规范）规则》修正案，明确了社交媒体在发布被政府归类为虚假、不真实或误导性信息方面的义务；奥地利政府发布了《打击深度造假的行动计划》，包括风险分析、监管目标和措施建议；新加坡《通讯网络安全（杂项）法案》开始生效，规定在线通信服务提供商必须删除被归类为“恶劣内容”的信息，遵守监管部门发布的屏蔽和删除要求；土耳其通过《新闻法》，规定在社交媒体上传播虚假信息可能被判 1~3 年监禁。这些国内数字监管治理政策法规的出台将导致更多数字贸易和投资相关壁垒的出现，使得全球数字治理面临起点更低、问题更多、协调更难等问题。

2. 全球数字治理取向转向安全优先，网络安全合作受到更多重视

网络安全的国际治理由来已久。据 IGF 统计，2008~2022 年，全球共形成 38 项与网络安全相关的国际协定，内容涵盖信息安全、产品可靠性、网络能力管控、合作与援助等方面。早期网络安全国际合作主要是为了更好地应对共性的网络安全风险、提升互信和政策透明度、促进区域数字经济一体化，如东非共同体发布的《网络法律框架》、东盟发布的《信息通信技术的安全使用工作计划》、非盟发布的《网

^① USTR.USTR Statement on WTO E-commerce Negotiations[EB/OL].2023,https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations.[2023-10-24](2024-01-28).

络安全和个人数据保护公约》。

乌克兰危机升级暴露了数字化发展的安全赤字和治理赤字,使得全球治理的发展议题不得不在一定程度上让位于安全议题,主要国家对国际网络安全问题的重视程度大幅提升。2022年3月,美国总统拜登在声明中指出,美国将加强国家网络防御,强制联邦政府和关键基础设施部门采取广泛的网络安全措施,并创建创新的公私伙伴关系和倡议,以应对可能出现的俄罗斯网络攻击。2022年5月,欧盟理事会批准的《关于网络态势结论》指出,网络空间已成为地缘政治竞争的舞台,欧盟必须能够迅速有力地应对网络攻击,并呼吁欧盟委员会和网络安全局采取进一步的行动。

同时,网络安全合作重点也变得更具对抗色彩。一方面,主要国家与盟友在网络安全领域合作明显加强,进一步强调对地缘政治对手网络攻击的防范和应对。2022年6月,北约《马德里峰会宣言》指出,北约面临来自网络空间的威胁,将通过加强军民合作和利用国家资产,提高应对网络和混合威胁的复原力。2022年11月,七国集团(G7)发布联合声明指出,将深化七国集团之间的战略合作,通过充分利用共同的分析资源来预防、检测和打击各种形式的网络攻击,更好地保护关键基础设施,保护私营部门和研究团体免受外国恶意投资、收购、网络活动和专有技术非法外流等敌对活动的侵害。另一方面,多边层面围绕冲突时期网络安全行为准则的讨论出现巨大分歧。从第二届联合国网络空间治理开放成员工作组(OEWG)实质性会议各方提案和2022年6月工作组主席散发的基础案文(0号案文)看,各成员围绕网络安全不同解决方案的争论更趋激烈,美国、瑞士等认为国际人道法能够在网络空间直接适用,保证自卫权的行使;俄罗斯、伊朗等认为应制定新的国际公约并建立术语清单,防止个别国家凭借技术实力滥用自卫权。^①

3. 全球数字治理主导权竞争更激烈,国际机制、规则和标准博弈升级

数字外交^②是各国主动构建数字领域国际合作网络、对外输出数字治理理念、深化对全球数字治理影响的重要途径。乌克兰危机升级以来数字技术产业及其全球性规则的重要性进一步凸显。主要国家为了塑造更符合自身利益的全球数字化发展环境,通过增设机构、加大投入等方式加强了数字外交部署。例如,2022年4月,美国国务院下设的网络空间和数字政策局(CDP)开始运作,负责网络空间和数字外交方面工作,由国际网络空间安全、国际信息通信政策和数字自由3个政策单元构成,为相关部门政策协调、数字外交政策制定提供支持。2022年7月,欧盟理事会批准了《关于欧盟数字外交的结论》,强调数字技术为欧盟公民和全球人民的生活带来了新的机遇和风险,成为可以改变地缘政治力量平衡的关键竞争参数,将确保数字外交成为欧盟对外行动的重要组成部分,并与其他关于网络和混合威胁的外部政策密切协调。

^① 中国信息通信研究院.全球数字治理白皮书(2022年)[EB/OL].2023,http://www.caict.ac.cn/kxyj/qwfb/bps/202301/P020230110553626083595.pdf.[2023-01-10][2023-05-17].

^② 本文中的数字外交是指围绕数字领域问题开展的外交,而不是借助数字技术开展的外交。

在这一轮数字外交的竞合博弈中，地缘政治成为关键驱动因素。美国试图通过数字外交主导和垄断全球数字治理话语权和规则制定权，实现在新兴领域对中国的打压遏制；欧盟短期内不得不在一定程度上倒向美国，但是对于个人隐私保护、数字市场构建仍有自己的坚持和考量；中国面对美国的步步紧逼，也相应加强了数字外交部署。在此背景下，几乎所有国际数字治理机制均出现了更激烈的竞争，包括联合国框架下《全球数字契约》关于开放、自由和安全的数字未来的共同原则的谈判，国际电信联盟（ITU）、国际电工委员会（IEC）、电气工程师协会（IEEE）等机构关于数字标准的制定，WTO 电子商务谈判、区域贸易协定等关于数字贸易规则的谈判等。具体竞争一方面表现为国际组织的机制设计、议程安排和官员选举，例如，在 2022 年 9 月 ITU 全权代表大会的换届选举中，美国经过周密部署，其候选人以 139 票接任赵厚麟成为新一任秘书长，俄罗斯候选人则只获得了 25 票；^① 另一方面表现为数字治理原则、标准和规则制定，例如，2023 年 4 月，在维也纳举行的《联合国网络犯罪公约》特设委员会第 5 次条约谈判会议中，围绕公约的基本原则、涵盖犯罪范围、个人数据保护等问题，欧盟与中国、俄罗斯之间出现了激烈辩论。^②

4. 全球性解决方案达成共识更困难，合作阵营化和治理碎片化问题加剧

数字治理碎片化主要是指由于各国在政策法规、经济利益、价值观等方面存在巨大差异，以及对自身网络安全的担忧和数字主权的追求，导致全球性的数字治理方案难以形成，取而代之的是一个以国家集团为单位的数字治理系统，且这些系统彼此之间缺乏沟通、相互排斥。乌克兰危机升级以来，美国着力将中国和俄罗斯捆绑，试图把中国塑造为“共谋”的角色，从而利用西方同盟关系打压遏制中国，推动关键领域“去中国化”，导致世界政治经济变得更加分裂（易小准等，2022）。受此影响，全球数字领域合作变得更集中在区域层面，且更聚焦强化与有限盟友合作和争取中间势力支持，加剧了全球数字治理的碎片化、阵营化问题。

一方面，地缘政治伙伴间的数字贸易和投资协定快速增多，通过率先制定规则和扩大规则适用区域，强化规则制定的先发优势和示范效应。具体表现形式有：首先是加入包含数字贸易规则的区域贸易协定，如英国宣布实质性结束关于加入《全面与进步跨太平洋伙伴关系协定》（CPTPP）的谈判，希望通过消除数字贸易壁垒、促进数字贸易信任，帮助英国成为数字贸易的领导者；其次是推动现有贸易投资协定升级谈判，加入数字贸易规则条款，如中国和新加坡宣布实质性结束自贸协定升级谈判，增加电信服务的章节，纳入市场准入、透明度和数字经济等新规则；最后是推动达成新的包含数字贸易规则的协定，如英国与加拿大宣布就新贸易协定进行谈判，英国与韩国结束关于自贸协定现代化的磋商，重点均为数字贸易。

另一方面，地缘政治伙伴间的数字治理国际协调和合作快速增多。相比于贸易

^① Emma Farge. U.S. Candidate Beats Russian to Head U.N. Tech Agency[EB/OL]. 2022, <https://www.reuters.com/business/media-telecom/us-candidate-beats-russia-head-un-telecoms-agency-2022-09-29/>. [2022-09-29] (2023-05-17).

^② Digital Watch Observatory. Countries Clash over Cybercrime Negotiations at the UN[EB/OL]. 2023, <https://dig.watch/updates/countries-clash-over-cybercrime-negotiations-at-the-un/>. [2023-04-24] (2024-01-28).

投资协定，数字领域倡议、宣言、备忘录等合作形式更灵活，达成难度更低，成为主要国家抢先输出治理理念、强化对全球数字治理影响的重要手段。2022年以来，全球数字领域国际合作协议出现了爆炸性增长，内容涉及跨境数据流动、新兴技术、半导体、网络安全、内容审核等。最多的是美国、欧盟、日本、韩国、新加坡等经济体之间的相互合作，如欧盟先后与日本、韩国、新加坡、加拿大达成了数字合作伙伴关系协定；其次是“发达国家+发展中国家”的合作，如美国与13个国家宣布启动“印太经济繁荣框架”（IPEF），采取“多轨并行”的灵活谈判模式及“多方联动”的数字技术治理合作策略，与越南、泰国和菲律宾等东盟成员加强数字技术绑定关系（周念利和吴希贤，2023）；最后是发展中国家之间的相互合作，数量相对有限但增长迅速，如中国与东盟、沙特及非洲10多个国家签署数字领域合作备忘录，东盟发布《人工智能治理与道德指南》。

四、结论

全球数字治理转向受到许多因素影响，如数字技术发展应用过程中的客观安全风险、围绕新一轮产业科技革命的激烈竞争、国家间相对力量变化导致的地缘政治冲突等。乌克兰危机升级虽然不一定是主导的驱动因素，但一定是最能直接揭露数字技术对未来竞争格局和国际环境影响的因素。

乌克兰危机升级以来，数字领域相关的技术、应用和制裁层出不穷，使得南方国家很难再简单相信西方国家开拓国际数字市场时叙述的“美好愿景”，就连西方国家自身也开始以“国家安全”为由限制合作，对高度依赖“信任”的数字经济国际合作无疑产生了巨大的负面冲击。在此影响下，我们可以看到全球范围出现了更多的数字领域相关监管政策、经贸摩擦和阵营对抗，全球数字治理的底色变得更加封闭保守、取向变得更加强调安全、主导权竞争变得更加激烈、多边共识达成变得更加困难。从短期看，一些国家的数字政策制定者难免将更关注如何战胜竞争对手，把“相对收益”摆在首位；从长远看，数字政策制定者还是会回归理性，把争取更多的“绝对收益”作为核心目标，只是需要多久还尚不明朗。

中国将不得不面对更复杂严峻的全球数字治理形势。作为国际治理的重要一极，欧盟由于对美国严重的军事依赖，不得不在一定程度上放弃“战略自主”，转向与美国更紧密合作；同时因为中俄一直保持着紧密的合作关系，对中国的不信任度大幅提升。这为美国在新兴数字领域国际治理中强化影响和遏制中国创造了绝佳条件。美国不仅联合盟友对ITU等国际组织的人事任用、议程设计、表决投票等方面施加影响，还依托G7、IPEF、美欧贸易和技术委员会（TTC）等建立多圈层的经济和技术合作机制，试图构建以美国为核心的全球数字经贸网络，削弱中国在全球数字治理领域影响力，维系其在数字时代的全球霸权。

中国需更加积极地参与全球数字治理，加大数字公共产品对外输出，巩固和延伸数字经济发展优势，在未来国际竞争中争取主动。第一，需稳步扩大数字领域对

外开放，进一步缩减外资准入负面清单，积极对接 CPTPP、《数字经济伙伴关系协定》（DEPA）等国际高标准国际经贸规则，扩大规则、规制、管理、标准等制度型开放，提升国内市场监管政策的国际影响力。第二，需加快形成数字治理中国方案，在深入研究和明确中国数字领域核心利益的基础上，参考国际通行惯例推动国内数字领域监管政策法规制定，逐步形成具体的、可落地、可对接的对外政策法规。第三，需建立多层次的数字伙伴关系，要紧密联系发展中国家，分享数字技术应用与政策制定经验，为它们的数字能力建设提供支持，共同推动更加包容的全球数字治理体系建设；同时要尽可能维持与欧盟合作，充分运用好双多边数字交流合作机制，增进互信。第四，需积极参与多边数字治理机制，充分应用好联合国、WTO 等多边机制，深化与各方对话协商，妥善处理分歧，寻求数字治理的最大公约数。

参考文献：

- [1] 陈伟光, 钟列炆. 全球数字经济治理: 要素构成、机制分析与难点突破 [J]. 国际经济评论, 2022, (2).
- [2] 彭中新等. “星链”在俄乌冲突中的运用分析与思考启示 [J]. 战术导弹技术, 2022, (6).
- [3] 薛晓源, 刘兴华. 数字全球化、数字风险与全球数字治理 [J]. 东北亚论坛, 2022, (3).
- [4] 易小准等. 俄乌冲突对国际经贸格局的影响 [J]. 国际经济评论, 2022, (3).
- [5] 岳云嵩, 霍鹏. WTO 电子商务谈判与数字贸易规则博弈 [J]. 国际商务研究, 2021, (1).
- [6] 张荣楠. 全球数字治理博弈与中国的应对 [J]. 当代世界, 2022, (3).
- [7] 周念利, 吴希贤. 拜登政府主导 IPEF 数字技术治理合作内容、挑战及应对研究 [J]. 亚太经济, 2023, (3).

Unexpected Challenge: Ukraine's Crisis Escalation Pushes Global Digital Governance to Accelerate Shift

YUE Yunsong XUE Xinlong

Abstract: With the Digital transformation of the global economy, digital economic and trade exchanges between countries have increased significantly. The differences in policies and regulations of different countries in cross-border data flow, AI governance, transnational platform supervision and other aspects have become a huge obstacle to development. This has prompted countries to strengthen discussions on digital issues at the multilateral and regional levels, deepen coordination of policies and regulations between countries, and promote the accelerated formation and development of a global digital governance system oriented towards development. However, during the Ukraine's Crisis escalation, a large number of digital elements were used for confrontation, such as network attacks against key infrastructure, social media public opinion control, the use of dual-use digital technology, and the involvement of private transnational digital enterprises in national conflicts. Countries have begun to re-examine the development and cooperation of digital globalization, shifting their attention from development to security, which has greatly affected the development direction of global digital governance. Major countries have not only strengthened domestic digital regulatory governance and international cybersecurity cooperation, but also actively cooperated with allies to compete for the dominant position in global digital economic and trade governance, making the global digital governance background more conservative, the orientation more focused on security, the competition for dominant power more intense, and multilateral solutions more difficult to achieve. Faced with changes in the situation, China should deepen its impact on global digital governance by expanding the opening up of the digital field, improving China's digital governance plan, establishing multi-level digital circles of friends, and fully integrating into multilateral mechanisms for digital governance negotiations.

Keywords: Ukraine's Crisis; digital governance; digital policy; digital technology

(责任编辑: 梁丽华)