数字经济

大国的新兴规范倡导与网络性权力运用
——以美国的数字技术规范倡导为例

黄 贝 华佳凡

[摘 要]在国际社会构建新兴国际规范的进程中,国家间规范合作关系所构成的社会网络赋予了中心位置国家进行规范倡导的网络性权力,而既有研究尚未充分关注国家运用网络性权力的具体模式及其作用。具体而言,网络性权力是一国利用其在规范合作网络结构中的位置对其他国家所具有的影响力,而大国可从两个方面利用该权力进行规范倡导:一方面,大国可利用网络性权力强化说服、奖惩与实践等规范推广既有机制的效力;另一方面,大国还可发动伙伴国家以众包形式参与规范扩散,进一步增强其规范影响力。近年来,美国在网络安全与跨境数据流动两个数字技术规范议题上的实践进一步表明,网络性权力有助于提升大国进行新兴规范倡导的成效。这一探讨有助于理解规范合作网络结构对于大国新兴规范倡导的重要作用,也为我国参与新兴技术领域全球治理提供了启示。

[关键词]国际规范;数字技术;网络安全;跨境数据流动;网络性权力
[中图分类号]D815 [文献标识码]A DOI:10.13654/j.cnki.naf.2025.05.005
[文章编号]1003-7411(2025)05-0075-(16)
[收稿日期]2025-03-12
[基金项目]国家社会科学基金重大项目(21&ZD167)
[作者简介]黄贝,武汉大学政治与公共管理学院讲师,武汉大学经济外交研究中心研究员(武汉 430072);华佳凡,国防科技大学外国语学院讲师(南京 210039)。

一、引言

新兴规范构建是国际政治的重要议题。随着数字技术的迅速发展,如何构建数字技术国际规范关乎国际体系的稳定性基础,因而受到国际社会的高度关注。[1]在该领域内,中国、美国、俄罗斯、欧盟等大国及主要区域组织在核心概念理解、主权原则等既有规范适用以及新规

范生成等问题上存在不同程度的分歧，并提出各自的规范倡议，试图塑造更符合自身主张的国际规范。[2]在此背景下，理解与分析大国在新兴规范领域推广规范倡议的行为模式及其影响力来源具有重要的理论与现实意义。

在规范研究领域，国家行为体的规范推广与规范论争等议题已成为知识快速增长的方向。[3]首先，关注国家参与规范进程行为与策略的研究迅速增多，相关研究归纳了规范倡导者会使用一系列吸引支持者的策略。[4]其次，在大国战略竞争加剧的现实背景下，一些学者对规范竞争行为体进行类型学分析，[5]也有学者探讨了规范竞争者的话语与行为策略。[6][7]最后，有研究聚焦于数字技术领域这一新兴规范议题，对国家在网络安全、跨境数据流动等领域内采取的规范倡议策略与规范共识达成的影响因素等问题展开了讨论。[8][9]然而，既有研究大多从规范倡导者、竞争者或追随者的单一视角出发，忽略了国家间规范互动关系这一结构性因素，也未能充分关注新兴规范领域行为体间复杂的多向规范互动对规范推广具有的重要作用。

本文关注新兴规范领域内国家间规范合作互动构成的社会网络，提出国家利用在该网络结构中的位置提升其规范主张影响力的网络性权力，进而对大国运用该类权力的具体模式及其作用进行归纳与分析。本文认为，大国可以运用网络性权力强化说服、奖惩和实践等规范推广既有机制的效力，网络结构也会催生出伙伴国家参与规范推广的众包方式，进一步帮助大国提升其规范主张的影响力。近年来，美国在网络安全和跨境数据流动规范议题内的规范倡导实践可以在不同程度上展现网络性权力的上述运用模式，对这两个案例的比较也体现出网络性权力差异对规范倡导效果的影响。理论层面上，本文通过探讨网络性权力这一概念，发掘了新兴规范进程中国家推广规范倡议的新特征与新态势。现实层面上，本文能为观察当前数字技术国际规范构建进程的最新动态提供启示，并为中国参与新兴技术领域全球治理提供一定政策参考。

二、大国基于规范合作网络的网络性权力及其运用

（一）国家间规范合作网络与网络性权力

行为体间互动关系所构成的网络结构（network）是近年来国际关系研究的重要议题。国际社会中的社会网络既可能是外交关系网络、同盟关系网络等制度化程度较高的关系网络，也可能是经贸网络、价值链网络和外交访问网络等描述行为体间日常行动的互动网络。与对国家物质性实力和国家间双边关系的既有探讨不同，将国家置于国际关系网络结构中的思考有助于捕捉物质与非物质性资源（如信息、信任和承诺）在结构层面的流动，为国家权力这一经典概念提供全球化背景下更为丰富多元的内涵。[10]一国利用在网络结构中位置所发挥的影响力，即网络性权力对多个领域的重要影响也获得诸多实证研究验证。

规范是行为体对共同持有的适当行为的共同预期，主体间性（intersubjective）是规范的重要特征。这种主体间性决定了规范天然地成为行为体间讨论的对象，行为体会向他者明确地阐述规范以获得合法性，或通过推广规范来说服他者采取行动。[11]换言之，规范产生于国家等行为体的互动之中，也在互动之中获得认可，行为体间互动深刻塑造着规范。因此，同样强调互

动关系所具有社会化效应的社会网络视角成为理解规范相关互动及其作用的恰当工具。基于既有文献，本文将一国在规范构建进程中的网络性权力界定为该国利用在规范合作网络结构中的位置对其他国家所具有的影响力。[12]当一国在规范合作网络结构中的位置越靠近中心，以其为中心的网络结构所涵盖的其他行为体越多，该国的网络性权力则越大；反之亦然。这种网络性权力可以通过大国在合作网络结构中的多种中心性指标来衡量。①

一国网络性权力的提升既是其主动采取的规范倡导政策所产生的结果，也受到客观因素的影响。从国家塑造网络性权力的能动性来看，一国可以通过主动投入资金、外交等资源，采取积极的外交措施来推广规范主张，结成规范伙伴关系，拓展所在合作网络结构的范围。大国基于新兴规范合作网络获得的网络性权力及其动态变化部分地反映了前一轮规范扩散的成效。大国首轮规范扩散所获得的规范追随者与其共同构成了规范合作网络的初期结构，而此后大国与其伙伴国发起的每一轮规范扩散将继续塑造规范合作网络，并在一定程度上影响大国下一阶段的网络性权力强弱。当然，新规范的扩散尤其是首轮扩散在理论上并非必然成功，但鉴于大国拥有的物质性资源、外交关系等天然优势，大国构建起一个初期规范合作网络并非难事。事实上，当前大国在新兴技术领域尤其是数字技术领域的新规范倡导通常以构建合作网络，即以提前做好共同提议或伙伴国动员等外交工作为前提，使其规范主张具有更强的合法性与影响力。②

同时，国家进行规范推广、强化网络性权力的能动性不足以完全决定其网络性权力的大小，还需考虑国家间既有规范观念、现实利益趋近性以及伙伴国导致的网络结构变化等客观因素的影响。在新兴规范议题内，与大国既有规范立场相近、拥有共同现实利益的国家尤其容易在新议题内与其构建规范合作网络，进而赋予大国更显著的网络性权力优势。这一逻辑也与既有规范理论观点一致。新规范的生成与扩散并不是相对于既有规范的“另起炉灶”，而是对其存在较明显的路径依赖。[13]因此，既有规范观念相近的国家更容易在新兴规范领域内开启新合作，大国的新兴规范合作网络往往也以既有规范合作网络为重要基础。例如，在人道主义规范方面立场相近的发达国家，对于网络空间内人道主义原则适用性等议题也拥有相近观点，进而更易在这一新规范领域内开启合作。这一大国新兴规范合作网络的形成路径也在一定程度上解释了为何美国能够在网络安全国际规范构建初期与其他发达国家快速构建起规范合作网络，而主张网络主权的规范合作网络则主要由传统主权观念相近的中俄等发展中国家构成。

鉴于此，国家基于规范合作网络获得的网络性权力与其硬实力、软实力和关系性权力等既有权力概念互有区别，但并不对立。一国既有的资源性权力和关系性权力可以成为其在新兴规范领域网络性权力的基础之一，而网络性权力也受其他客观因素影响。

---

① 具体包括度数中心性（degree centrality）、亲近中心性（closeness centrality）、居间中心性（between centrality）和特征中心性（eigenvector centrality）等指标。

② 例如，中国与俄罗斯在网络安全、跨境数据流动等领域的规范倡导常以上海合作组织成员国共同倡议的方式来发起。美国在数字技术领域往往也通过与盟伴国家的议题联盟共同进行规范倡导。

（二）大国在新兴国际规范倡导中的网络性权力运用

既有规范研究对规范推广的社会化机制已有较多论述，其中包括规范倡导者传授规范的机制，如奖惩、说服等；也包括其他行为体接受规范的机制，如效仿、本地化等。[14]由于新兴国际规范领域中相关规范倡议往往处于兴起与扩散初期，因此本文侧重讨论在新兴国际规范领域内，规范倡导国一方如何运用网络性权力推广与传播本国规范主张。

在当前新兴国际规范构建过程中，一国运用网络性权力进行规范推广的模式主要可分为两类：其一，大国可以借助网络性权力强化规范推广既有机制的效力；其二，大国的网络性权力也可以在结构层面催生由伙伴国家参与众包（crowdsourcing）这一新的规范传播路径。

第一，大国运用网络性权力对既有规范传播机制的强化效果涉及说服、奖惩与实践三种机制（见图 1）。首先，基于网络结构的信息交换可以强化规范推广的说服机制。信息是网络结构中传递的重要元素，也是影响和塑造行为体思想、观念与认知的主要介质。为了获取规范相关的知识信息，各国愿意推动信息网络的形成，而具有网络性权力优势即中心位置国家的信息交换更为高效。一方面，拥有较强网络性权力的国家能够使其信息最大可能地触及其他行为体，并更有效地收集其他行为体的反馈信息，不断完善其规范主张。另一方面，当国家与持有相似规范立场的其他国家利用规范合作网络共同传递信息时，这种信息生产方式还能一定程度上提升信息的可信度与信息“厚度”，提升规范主张的吸引力。[15]网络性权力赋予国家的上述信息优势能够帮助说服机制更为顺畅地发挥效力，从适当性逻辑上强化该国规范影响力。

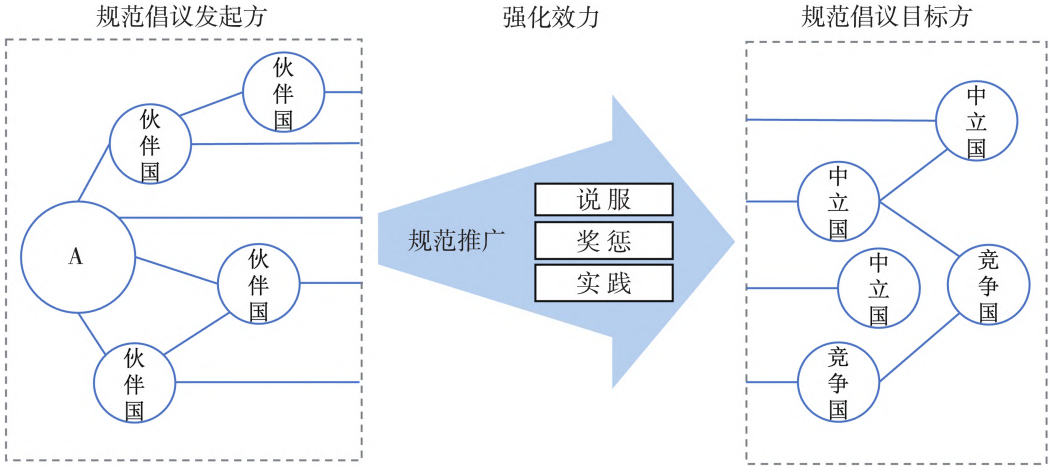

图 1　网络性权力对既有规范推广机制的强化

资料来源：作者自制。

注：圆形代表国家，蓝色实线代表国家间规范合作关系。国家 A 代指在该网络结构中拥有网络性权力优势的大国。

其次，基于网络结构的资源流动可以强化规范推广的奖惩机制。从理性主义视角出发，国家的行为选择与其成本—收益考量密切相关。规范倡导国可以通过奖励与惩罚影响他国现实利益，促使他国遵守其规范主张。而具有较强网络性权力的规范倡导国能够在更大程度

上影响资源的流动效率与方向，从而采取更为有力的奖惩措施。这些资源既可能是社会性的（如地位与羞辱），也可能是物质性的（如援助与经贸合作机会）。[16]例如，美国等西方国家往往动员国际组织、非政府组织与媒体等多类行为体对违背其规范主张的国家进行“点名与羞辱”，或是利用其在国际金融网络中的优势位置，采取初级制裁与次级制裁并行的惩罚措施。国家利用网络性权力对他国进行奖励或惩罚，能够以更大效力改变目标国在该领域的成本—收益结构，促使他国选择接受其规范主张。

最后，基于网络结构的共同行动可以强化规范推广的实践机制。随着规范研究的“实践转向”，行动被视为与言语因素一同影响规范形成的重要维度。国家等行为体对规范的认同不仅体现在观念和语言表达中，还可能通过行动实践而实现。当行为体反复采取某种行动并形成稳定的模式即惯习（habitus）时，这种惯习行为反过来也会使行为体在未来行动中仍遵循这一行为模式。[17]因此，当国家运用网络性权力调动其他行为体参与符合其规范主张的共同行动时，他国能够从行动实践层面加深对该规范主张的接受程度。基于对规范的反复应用，行为者的实践行动也会反过来塑造规范内容。例如，关于网络犯罪的能力建构行动可以帮助相关国家进行情报分享和行动协调，进而催生新的共有观念与规范。[18]

第二，大国对网络性权力的运用还可以在结构层面催生新的规范推广方式，即伙伴国家发挥能动作用，通过众包参与规范推广（见图2）。在新兴规范构建过程中，合作网络结构中的伙伴国家可能在规范倡导国未直接参与的情况下发起相似的规范倡议，从而提升规范影响力。这种由多个行为体或分布式网络大众共同完成某一行为体发起的工作任务（即推广某一规范）的生产方式可称为众包。众包既有可能是参与方自发性、志愿性的行为，也可能与金钱等现实利益相关。[19]

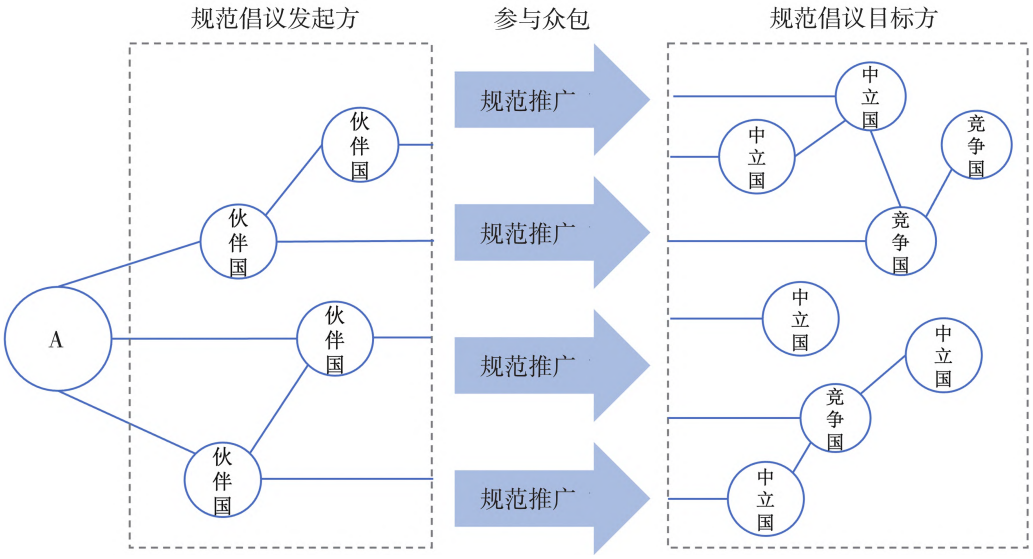

图2 网络性权力所催生的规范众包

资料来源：作者自制。

注：圆形代表国家，蓝色实线代表国家间规范合作关系。国家A代指在规范合作网络结构中拥有网络性权力优势的大国。

在新兴规范领域内，他国积极参与规范众包的动机同样是多样的。这些国家可能由于与倡导国拥有相似的价值观念，或在规范议题上具有相近的现实利益，出于自利性目的参与规范众包；它们也有可能由于受到倡导国的有效动员，或是受既有军事同盟等制度化合作关系的塑造，出于追随性目的参与规范众包。同时，这些参与众包的伙伴国家通常还需要具备发起规范倡导的基本能力，如物质性资源、既有外交关系以及对于特定规范议题的影响力等。

由规范伙伴参与的众包能够从以下方面对倡导国的规范推广发挥正面作用。首先，更广范围内“志同道合者”自愿发起与倡导国立场一致的规范倡议，可以进一步强化规范扩散效果。例如，众包方式可以借助知识集聚与能力互补，为创新合作提供新路径，强化分工与协同作用。在规范倡导国未参与的情况下，网络结构中的伙伴国家能够通过自发的规范合作完善规范相关信息，对规范主张进行“再理解”与“再创造”，为该规范推广提供更为丰富的内容，并通过增加信息来源的多样性提升其可信度。同时，由规范伙伴主动发起的规范相关奖惩行为或实践活动也能形成规范推广的规模效应，加速规范扩散的进程。

其次，规范伙伴参与众包有助于进一步拓展规范扩散范围。单个国家在某一规范议题上可供调配的资源始终有限，这也导致其规范主张的传播范围存在限度。在此情况下，伙伴国家根据自身国家实力、地理位置和既有外交关系等禀赋建立起规范合作子网络，可以从整体上进一步拓展网络结构。同时，社会网络结构本身存在“受欢迎者将更受欢迎”“朋友的朋友也能成为朋友”等网络效应。伙伴国的规范合作行动越活跃，网络结构内的合作关系越有可能更为密集。因此，这些由伙伴国家促成的网络结构发展可以使倡导国的规范主张传递至原本难以触及的受众，提升规范的影响范围。

最后，众包可以帮助规范倡导国降低规范推广的成本和压力。对于规范倡导国而言，当支持其规范主张的伙伴国家增多，且自愿推广相似规范主张时，其规范推广成本能够一定程度上由伙伴国家分摊，减少自身规范投入。这一点在同盟等领域国际合作中也有突出体现，相较于双边关系或轴辐式关系所需投入的成本而言，网络状关系能够更有效地降低中心位置国家成本。[20]同时，规范推广并不总是一帆风顺，当倡导国推广其规范主张的行动受挫时，还将进一步增大倡导国政府的国际与国内声誉压力。因此，独立发起相似规范倡议的伙伴能够成为倡导国在该规范议题上的“代理人”，一方面在其支持与帮助下发起规范倡议与规范合作，另一方面也能帮助倡导国缓冲甚至规避规范推广失败时面临的直接压力。

综上，大国利用来自规范合作网络的网络性权力进行规范推广的模式既包括单一主体发起的规范推广效果的增强，也包括在网络结构层面由伙伴国参与众包这一分散化、多元化的新机制。为了展示上述大国运用网络性权力的理论化模式及其作用，本文将结合新兴技术规范领域大国进行规范倡导的经验事实进行具体阐述。

三、美国利用网络性权力推广数字技术规范倡议的案例分析

本文选择以近年来美国在网络安全规范与跨境数据流动规范两个议题内的规范推广作为案例，案例选择的原因包括：首先，美国是多个新兴国际规范议题内积极的规范倡导者，其资源性实力与同盟体系也为网络性权力提供了天然基础，有必要关注美国在新兴规范倡导中运

用网络性权力的具体过程。其次，选择网络安全规范和跨境数据流动规范议题的原因在于，这两个议题是当前受到高度关注的重要新兴技术规范，也是数字时代国际规范构建的两大前沿阵地。最后，这两个案例能够构成控制其他倡导国属性的正负面案例，以更好地观察网络性权力对于国家规范倡议推广效果的大致影响。

（一）美国在网络安全议题上的规范倡导

网络安全规范是备受瞩目的新兴安全规范领域之一。20世纪90年代，随着新兴信息通信技术开始应用于军事行动之中，国际社会关于网络战、网络军控等概念的讨论逐渐兴起。面对网络空间军事化发展态势，国际社会对网络安全国际规范的关注度不断提升，大国纷纷提出本国在相关领域内的规范倡议。在该议题内，美国为代表的发达国家与中国、俄罗斯为代表的发展中国家之间存在立场分歧，相关规范竞争日益加剧。

为了避免本国在互联网领域的优势地位受到限制，美国坚决反对俄罗斯所提出的签署网络军控新协议的倡议，也无视中国反对网络空间军事化的规范主张，坚持将既有国际法向网络空间的“移植”，并尤为积极地推动武装冲突法在网络空间的适用。2007年爱沙尼亚遭到大规模网络攻击等重大网络安全事件发生后，美国政界及学界对诉诸武力权适用于网络空间这一规范主张的讨论不断升温，即认为国家可以援引《联合国宪章》第51条针对特定网络攻击行使自卫权。2010年，美国国防部常务副部长威廉·林恩（William J. Lynn III）发文表示，“五角大楼已经正式将网络空间作为一个新的战争领域”。同年，美国网络司令部正式成立。2011年，美国政府出台《网络空间国际战略》，明确宣称美国将使用军事手段（自卫权）来回应“通过网络空间从事的某些敌对行动”。[21]

同时，在网络安全规范领域，美国拥有着广泛的规范合作关系，并具有明显的网络性权力优势。以“度数中心性”（一国拥有的合作关系数量）这一网络性权力的测量指标为例，与美国拥有网络安全规范合作关系的合作国数量达到176个，美国也是当前全球范围内网络安全规范合作关系最多的国家。[22]由于美国与其军事盟友在网络空间的现实安全利益较为趋近，加之既有同盟安排也为美国及其盟友开展网络安全合作提供了制度化渠道，其规范合作网络与北约及亚太等地区军事同盟关系高度重合。美国为了推广网络空间适用诉诸武力权的规范主张，罔顾该规范可能带来的网络战“威胁膨胀”与网络空间军事化等风险，积极利用其网络性权力优势采取了一系列措施。

首先，美国利用政府间和非政府间国际多边平台联合伙伴国家传递该规范信息，试图说服并获得其他国家的支持，塑造规范合法性与合理性。在网络安全国际法领域，美国一贯善于利用政府与学界的“旋转门”，最大限度地发挥学者的支撑和补充作用。[23]2009年，北约合作网络防御卓越中心组织由美国海军学院国际法学者迈克尔·施密特（Michael N. Schmitt）领衔、由西方国际法学者组成的专家组开始编撰《塔林网络战国际法手册》（又称《塔林手册1.0》），这一成果于2013年正式出台，提出了网络空间内诉诸武力权和战时法的详细规则。这份法律文件与美国的网络安全规范主张高度吻合，为其此后推广规范主张提供了有力法律支持。2016年七国集团（G7）会议上，参会国家发布声明一致表示，某些情况下网络行动等同于武力和进行武力攻击。[24]2016年至2017年第七届联合国信息安全政府专家组会议中，美国联合其

西方盟友试图将网络空间内自卫权的行使等内容纳入最终报告，这引发中俄等国反对，并导致该届专家组最终未能出台任何报告成果。

在联合国平台受挫之后，美国继续利用其规范合作网络结构扩散该规范相关信息，以获取中立国家的支持。2017年，《塔林手册2.0》正式出版，这一版本考虑到非西方国家对于专家组代表性的反馈信息，加入了来自中国、泰国和白俄罗斯的三位学者，并在评注中标明国际专家组的不同观点。但是，该手册中关于国家遭受网络攻击时反制措施的规定仍有较大的“自由裁量”色彩，一定程度上继续为美国推广网络空间自卫权的规范主张提供了合法化工具。美国国务院法律顾问布莱恩·依根（Brian J. Egan）等西方国家政府官员对其持肯定态度，北约也在多国密集举办多场宣传推介活动，以进一步传递相关规范信息。[25]

其次，美国利用网络性权力与传统权力的综合优势，与伙伴国家对所谓“网络攻击发起国”采取联合归因或共同反制等惩罚措施。由于诉诸武力权适用于网络空间的规范落实建立在对攻击发起方实现归因（attribution）的基础上，因此美国联合一些盟伴国家积极发起联合归因，共同对其认定的网络攻击发起方进行公开判定。这类行动的意图之一，正是为符合其规范主张的反制措施增强合法性，并为所谓“攻击国”制造国际舆论压力。2017年，特朗普政府将“想哭”（WannaCry）病毒攻击正式归因于朝鲜，首次提及此次归因获得英国、加拿大、日本、澳大利亚和新西兰等国一致认可，也提及与微软、脸书等私营企业展开了归因合作。[26]此后直至2021年年中，美国主导发起了11次联合归因行动，参与伙伴涵盖了北约国家、日本、加拿大等多个地区盟友伙伴。[22]

作为后续措施，美国在实践层面对其网络攻击归因方采取了制裁与网络反击等不同程度的反制措施，这些反制行动也逐渐呈现多节点共同行动的特征。2012年，奥巴马政府因伊朗情报部与真主党（Hezbollah）合作的非法黑客活动对其进行制裁，首次在网络安全政策中引入制裁措施。2015年，奥巴马签署首个制裁跨境黑客的总统令，开始建立针对网络攻击的制裁制度。此后美国对朝鲜、俄罗斯和伊朗等国的个人和实体实施了一系列网络制裁。在特朗普时期，美国政府年均实施网络活动相关制裁的数量从10项增加至57项。拜登上台后，美国政府加强了针对国家实体，尤其是俄罗斯的网络制裁。[27]在美国网络制裁实践的启发下，2019年欧盟也正式建立网络制裁机制，并在2020年首次发起针对第三国具体的个人、实体和机构的网络制裁。欧盟相关法规表示，需要在网络制裁方面与美国等第三国加强协作，以确保制裁发挥最大效应。[28]

“9·11”事件以来，美国、以色列等国开始主张自卫权的行使对象可以包括恐怖主义分子，这种实践也随之出现于网络空间。同时，鉴于针对国家行为体行使自卫权的可能性，美国在安全同盟关系中将网络空间集体自卫作为联合演练与能力构建的重要发展方向。美国与日本等双边层面盟国签署网络合作协议，明确表示缔约国在网络遭到破坏的情况下可以使用盟国的网络发起网络攻击，[29]并进行了一系列网络军事演习，以提升同盟在网络空间的协同攻防能力。[30]北约等多边同盟也在实质上构建起进攻性网络能力，并已明确表示可能会将特定的网络攻击视为武装攻击，并启动《北约宪章》第5条集体安全条款进行应对。[31]这些围绕网络空间自卫权的日常合作也从实践方面推进了美国与其盟伴国家之间的共同规范生成。

最后，在美国未直接参与的场合中，其他伙伴国家在外交表态与实践中积极跟进推广该规范主张，通过众包模式进一步从结构层面拓展规范的影响范围。一些试图在网络安全规范形成过程中发挥更大作用的西方国家提出了各自的规范倡议，并对相关规范有所提及。例如，2017年英国与澳大利亚的双边网络安全对话明确表示，双方一致认为国家根据《联合国宪章》第51条享有在网络空间受到武装攻击时采取自卫行动的“固有权利”。[32]2018年，英国与其他55个英联邦成员国共同签署“英联邦网络声明”（Commonwealth Cyber Declaration）并启动相关网络合作计划，承诺推进《联合国宪章》、国际人道法等既有国际法在网络空间各方面的适用。[33]

在实践层面上，2018年，英国、澳大利亚与荷兰三国政府在美国政府未参与的情况下共同归因并谴责俄罗斯对禁止化学武器组织及马航MH-17调查组发起网络攻击。[34]欧盟基于对所谓网络攻击的归因启动多项网络制裁，对象涉及中国、俄罗斯和朝鲜的多个实体或个人。欧盟还于2018年正式从军事层面将网络空间界定为行动领域，逐步将其纳入欧盟共同安全与防务政策范畴。[35]

除英国和法国等大国之外，值得一提的还有美国北约盟友爱沙尼亚通过参与众包所发挥的作用。虽然爱沙尼亚就传统实力而言属于中小国家，但该国在2007年遭受大规模网络攻击后大力发展网络安全能力，一跃成为网络安全技术强国。同时，该国作为“网络战”受害国的特殊身份使其在网络安全规范领域享有一定国际话语权与影响力。鉴于这一优势，爱沙尼亚成为美国推动诉诸武力权在网络空间适用相关规范的积极伙伴。爱沙尼亚政府明确表示对网络空间诉诸武力权的支持，认为在应对网络空间武装攻击时，可以允许根据《联合国宪章》出于自卫目的使用武力。[36]

因此，爱沙尼亚也通过一系列外交举措积极推广该规范。一方面，爱沙尼亚作为北约成员积极承接主办美国支持的“塔林手册”网络安全规范进程，以及北约卓越合作网络防御中心（NATO Cooperative Cyber Defence Centre of Excellence）平台的网络攻防能力建设项目。另一方面，爱沙尼亚政府在联合国专家组等国际合作平台上频繁表达对该规范的支持，并利用本国技术优势推动规范相关合作实践。爱沙尼亚尤其关注与东欧、非洲等地区中小国家围绕网络安全规范进行“小众外交”（niche-diplomacy），并与这些国家开展网络能力构建合作。[37]该国也设立了“电子政务学院”（e-Governance Academy）等向他国政府部门提供数字化培训项目的非政府组织，项目内容包括向他国军事力量提供所谓网络安全解决方案。爱沙尼亚利用其在网络安全规范领域的特殊影响力与更易获得中小国家信任的非大国身份，在支持美国推动网络空间内诉诸武力权等既有国际法适用的进程中扮演了重要角色。

就美国倡导网络空间自卫权等网络安全规范的阶段性效果而言，虽然该规范受到中国等发展中国家反对，未能在联合国等全球平台上获得普遍性认可，但荷兰、法国、芬兰、新西兰、澳大利亚、德国、瑞士、英国和日本等国陆续发布有关网络空间国际法适用的立场文件，爱沙尼亚和以色列政府官员以演讲的形式阐明本国有关网络空间适用国际法的最新立场。这些文件均涉及使用武力和自卫权问题，并有催生出相关国际习惯法规则的可能性。[38]

（二）美国在跨境数据流动议题上的规范倡导

与网络安全领域相似的是，跨境数据流动领域同样尚未形成全球性规范共识，不少国家都提出了各自的规范倡议。具体而言，欧盟关注数据流动所带来的隐私问题，强调要对数据流动采取足够的监管措施；中国、俄罗斯等国强调数据流动对数据主权、国家安全的侵害，认为数据流动应置于严格、广泛的监管之下。与前两类规范倡导国不同的是，美国更关注数据流动所能带来的经济效益，并积极倡导数据自由流动。

在2018年《国家网络战略》中，美国政府将“促进跨境数据自由流动”作为一个重要议题列入目录，指出信息自由流动与美国国家安全存在密切联系，是加强美国国家安全的重要组成部分，并称“互联网自由也是美国外交政策的一个关键指导原则”。同时，该文件还指出数据流动与美国的经济利益密切相关，数据自由流动对经济与科技创新都有着重要意义，各国限制性的数据法规是在实行数字保护主义，会对美国的竞争力产生负面影响，美国将回击此类不合理障碍。[39]类似的表述同样延续到美国2023年的新版《国家网络安全战略》中，文件提出要在更广泛的挑战中促进数据流动，避免严格的数据本地化要求。[40]因此，美国积极构建以其为中心的跨境数据流动规范合作网络，试图运用网络性权力推广其规范倡议。

然而，美国在该领域的网络性权力与网络安全规范领域相比存在明显差距。在跨境数据流动领域内，美国的规范合作国数量远少于其在网络安全规范领域的合作规模。①限制美国该领域网络性权力的一个核心因素在于，美国并未与其盟伴国家建立起充分的跨境数据流动规范合作关系，也未能使盟伴国家成为其规范合作网络进一步拓展的关键节点。由于欧盟在隐私保护、扶持本地数字产业、确保数据主权等方面的利益诉求与美国存在分歧，而军事同盟框架下的利益协调也在这一社会经济议题内难以充分发挥作用。因此，相比于网络安全领域中与军事同盟关系高度重合的合作网络，美国在跨境数据流动领域未能够将盟伴体系中的主导地位迁移到该领域中来，并转化为广泛的合作网络。这导致该规范议题内美国的网络性权力相对较弱，其基于网络性权力进行规范推广的说服、奖惩和实践等机制均受到限制。同时，即便是美国规范合作网络内的伙伴国中，也有部分国家抗拒参与协助美国推广倡议的众包。

首先，多边的国际合作机制一直是美国通过说服和实践机制推广其规范倡议的主要平台。在美国主导下，2004年亚太经济合作组织（APEC）通过了关于数据跨境流动的“隐私框架”，要求成员经济体采取一切合理及适当步骤避免和消除任何不必要的信息流动障碍。在此基础上发展起来的2012年跨境隐私规则体系（CBPR）同样强调数据的自由流动。类似的实践还有在《跨太平洋伙伴关系协定》（TPP）中添加有关禁止数据本地化的相关条款，以及向世界贸易组织（WTO）提交倡导数据流动的《关于电子商务的联合声明》新议案等等。除了借助既有多边平台，美国还为跨境数据流动创设专门的国际机制，如在2022年与其他6个国家与

① 按照最宽松的估计，其合作国数量最多为64个，大致为跨大西洋数据隐私框架、G20（DFFT）、Global CBPR论坛、APEC隐私框架、OECD、FTA体系、英美数据桥等跨境数据流动合作关系的并集。在此范围内，还存在部分国家属于相关组织成员国，但未参与同美国的实质性跨境数据流动规范合作。

地区共同成立了全球跨境隐私规则论坛(Global CBPR Forum),鼓励成员之间加强合作互信,采用共同的数据监管方案,促进全球数据的自由流动。

虽然美国利用其合作网络做了相当多的努力,但其规范合作网络的边界并未得以显著拓展,其倡议影响力依旧大多停留在其原有合作网络内部。比如2012年创设的跨境隐私规则体系,包括美国自身在内至今仍旧只有日本、韩国、新加坡、菲律宾、加拿大、澳大利亚等9个国家参与,而它们大都自议题初期就是美国规范倡议的支持者。新近设立的跨境隐私规则论坛的成员目前也仅有8个,这一国际机制甚至还遭到了一些传统盟友的指责与质疑。例如,德国就对其真实效果持怀疑态度,认为跨境隐私规则论坛并没有改善美国的个人数据安全现状,更不用说达到欧洲所希望的水平。[41]加拿大虽然加入了该论坛,但也同样心存疑虑。一名加拿大官员质疑美国的真实动机,并称如果美国只是想促进互联互通,弥合不同监管模式,完全可以在现有机制的基础上寻求扩展吸纳更多成员,无需创建只适用于少数国家的全球跨境隐私规则论坛。[42]

其次,对于在跨境数据流动方面采取限制措施的国家,美国也并不能够像在网络安全领域一样对其进行有效的奖惩,尤其是直接实施制裁。例如,欧盟作为美国在该领域有力的规范竞争者,大力推动以GDPR为代表的数据流动规范,不仅阻碍了美国规范倡议的扩散,其具体政策实践也切实伤害了美国的现实利益。2018年,意大利以脸书未尽到充分告知义务、滥用数据为由对脸书公司处以1000万欧元的罚款,并勒令其公开道歉。2019年意大利数据保护局(GPDP)又以脸书非法收集21万意大利人数据为由对其罚款100万欧元,[43]德国政府也审查了脸书收集用户数据的行为,认为其未获得用户同意就收集了相关信息严重违法了欧洲数据保护规则,下令脸书公司停止相关行为并调整服务条款。[44]2022年法国数据保护局(CNIL)认定谷歌分析向美国谷歌公司传输个人数据不满足GDPR要求,勒令其在一个月内采取适当措施,否则将强制关闭其在欧洲的业务。[45]

然而,面对这些违背其跨境数据流动规范主张的情况,美国大多只是在言辞层面进行一定程度的谴责和批评,而非采取更为坚决的制裁等实际措施。例如,美国贸易代表办公室对于欧盟在数据流动、数字税等领域采取了一系列措施进行指责和"污名化",称其名为保护公众隐私,实则是一种数字保护主义,旨在保护欧洲本地数字产业,并声称"如果欧洲坚持其做法,美国将别无选择地将其视为战略威胁"。[46]然而在具体的政策实践中,美国却对欧盟进行了相当程度的妥协,以协调双方监管机制之间的差异。而其尝试与欧盟进行协调监管的框架,如曾达成的安全港(The Safe Harbor)、隐私盾(Privacy Shield)协议最终都遭到欧盟方面废止。现存的跨大西洋数据隐私框架也遭到了相当多的质疑。2023年9月,CNIL专员向欧盟法院提起诉讼,要求废止跨大西洋数据隐私框架。该专员指出,美国根本没有达到所要求的与欧盟同等的数据保护水平,尤其是美国情报机构还在大规模收集欧洲的个人数据。[47]意大利GPDP官员也曾公开表示无论美国如何努力,都无法制定出达到欧盟保护水平的法律,难以保证传输到美国的数据受到同等保护。[48]

最后,在通过众包拓展规范倡议影响力的模式上,美国在其合作网络中所能利用的资源

也大幅减少。仅有日本、新西兰等部分盟伴国家愿意参与众包，积极自发地推广数据自由流动倡议，这也体现出与网络安全规范领域的较大差异。

在跨境数据流动规范领域，日本是积极参与众包、配合美国规范推广的典型代表。一方面，日本对美国主导的相关国际机制积极响应，如前文提到的CBPR体系、TPP、全球跨境隐私规则论坛等机制。同时，日本与美国的双边数字贸易协定中也包含了大量禁止数据本地化的措施，如禁止限制数据存储位置、禁止对跨境数据流征税、禁止披露源代码等等。[49]另一方面，日本也尝试在规范构建中主动发挥影响。在2019年达沃斯论坛与G20峰会上，日本提出了基于信任的数据自由流动（DFFT）治理理念，呼吁通过国际数据分发的自由化来解决与隐私、安全、知识产权和其他问题，旨在确保有价值信息的无缝流动，不会受到国家规则的不合理约束。日本政府宣称，有必要在医疗、气候变化、物联网应用等关键领域实施DFFT，实现政府和利益攸关方之间的合作，以促进个人和非个人数据的跨境流动。[50]该理念受到了美国的欢迎，很快进入了G7集团的议程。在2023年日本召开的G7数字与技术部长会议上，成员国首次同意为促进DFFT建立一个具有常设秘书处的国际框架。除日本外，新西兰也有类似举措，该国于2020年联合智利和新加坡共同创建了《数字经济合作伙伴协定》（DEPA），同样旨在通过禁止数据本地化，促进数据自由流动来拉动经济和产业发展。

然而，在美国网络性权力较弱的情况下，一些美国的传统伙伴国家虽然迫于美国的压力，对其规范倡议给予一定的响应，但是并不会主动帮助其拓展新的规范合作关系，在事实上拒绝参与规范众包。例如，澳大利亚虽然同日本一样参与了CBPR、全球跨境隐私规则论坛等诸多美国主导的跨境数据流动国际机制，但对于帮助美国推广其规范倡议缺乏兴致，甚至“阳奉阴违”地在国内实行数据流动限制性政策。2022年，澳大利亚内政和网络安全部长克莱尔·奥尼尔（Clare O´Neil）就表示，无论数据储存在哪里都同样安全的想法是“绝对不正确”的，澳大利亚需要重新考虑数据储存要求，将数据本地化作为国家数据安全行动计划的一部分。[51]同年，澳大利亚通过《隐私法》新修正案，提高了对相关违法行为的惩罚措施，赋予了政府更多的监管权力。这类国家对众包的抗拒及对倡导国规范主张的“阳奉阴违”都使得美国的规范推广效果大打折扣。[52]

简而言之，美国在跨境数据流动领域推广其规范倡议的案例与网络安全领域案例形成了对比。在该议题内，美国网络性权力较弱，所能够动员的其他国家和使用的手段都相对有限，对规范倡导的促进效果不足，美国的跨境数据流动规范倡议也未能成为公认的主流性规范。

通过上述案例比较可以看出，虽然目前在网络安全规范和跨境数据流动规范这两个数字技术国际规范领域内均未形成全球性规范共识，但美国推广其规范主张的实际效果由于其网络性权力的差别而存在不同。在网络安全规范这一具有较强网络性权力的议题领域内，美国可以强化规范推广的说服、奖惩与实践机制效力，且通过伙伴国家共同参与的众包进一步提升其规范主张的影响范围与效果。相反，由于美国在跨境数据流动规范领域的网络性权力较弱，其基于说服、奖惩和实践机制所能采取的规范推广措施都相对更为有限，甚至对规范竞争者不得不进行一定妥协，因此其规范推广效果较差（见表1）。

表1 美国在数字技术领域的规范倡导案例情况

主要案例	案例类型	网络性权力的具体运用	规范倡导效果
美国在网络安全议题的规范倡导	正面案例（网络性权力较强）	• 利用多边平台联合其他国家塑造规范合法性与合理性 • 与伙伴国家对所谓“网络攻击发起国”进行联合归因及共同反制 • 英国、澳大利亚和爱沙尼亚等国政府在各自规范倡议中积极跟进，推广其主张	效果较好：公开支持美国规范主张的国家增多，并可能催生相关国际习惯法规则
美国在跨境数据流动议题的规范倡导	负面案例（网络性权力较弱）	• 利用多边平台联合其他国家推广规范倡议 • 使用谴责、污名化等相对温和的反制手段，但需要对规范竞争国作出妥协 • 规范推广众包国较少，存在伙伴国抗拒参与众包的情况	效果较差：规范支持国数量基本没有变化，规范倡议不具有影响力优势

资料来源：作者自制。

四、结论

当前，围绕构建网络安全规范和跨境数据流动规范等新兴国际规范的国家间互动日趋频繁与密切，诸多大国试图通过规范合作推广其规范倡议。本文从国家间规范合作关系这一结构性现象出发，剖析大国在新兴规范倡导过程中运用网络性权力的具体模式。一方面，网络性权力能够被用于强化说服、奖惩和实践等规范推广的既有机制，推动更多国家接受与认可大国规范倡议；另一方面，网络性权力还能催生伙伴国家参与众包这一结构层面的规范推广模式。本文通过分析美国近年来在网络安全和跨境数据流动两个数字技术规范议题内的规范倡导，进一步展示了网络性权力对于大国新兴规范倡导具有的重要作用。

需要说明的是，本文是对国际规范领域大国网络性权力的初步探讨。本文以美国的数字技术规范倡导为例，提出和归纳大国运用网络性权力的主要模式及其作用，挖掘大国在当前新兴规范进程阵营化背景下推广规范倡议的新特征与新态势。由于本文并非严格意义上的因果型研究，研究对于普遍性因果分析框架的构建与验证尚有不足，而未来研究也可通过拓展案例分析范围和挖掘因果机制等方式进一步讨论国际规范领域内大国网络性权力的适用范围与影响因素，以期进一步深化对新兴规范构建进程中国家多元能力属性及规范倡导策略的学理认识。

在现实层面，本文亦可为观察与研判大国塑造新兴国际规范的政策成效提供一定启示。特朗普的重新上台将使美国的新兴规范倡导政策迎来重大转变，其对国际规则的轻视将使美国政府对达成新兴规范共识的关注度大大降低，并引发国际社会对其国际权威与声誉的进一步质疑。同时，特朗普第二任期的“美国优先”政策已再次对其与欧洲、亚洲等地区内重要伙伴国的关系造成巨大冲击，美国借助网络性权力联合塑造国际规范的态势也将转向消极，这将导致美国对数字技术等领域新兴国际规范的影响力显著下降。在此情况下，中国参与新兴

技术全球治理的进程将同时面临挑战与机遇。我国应做好充分准备，及时应对特朗普政府在数字技术等领域对我国规范主张的抹黑与打压，呼吁国际社会抵制美国破坏国际秩序稳定性的行为。同时，中国可借助美国政府降低对全球数字治理关注度、放弃规范领域网络性权力的战略机遇，拓展规范合作伙伴关系，加强与“全球南方”国家的规范对话，分化美西方盟伴合作网络，推动中国规范主张在国际社会的影响力进一步提升，以促成新兴规范共识朝向良性方向发展。

参考文献

[1] 孙学峰.数字技术创新与国际战略竞争[J].外交评论，2023(1)：54-77.

[2] 郎平.网络空间：国际治理与博弈[M].北京：中国社会科学出版社，2022：196-199.

[3] 吴文成.从扩散到竞争：规范研究纲领的问题转换与理论进步[J].太平洋学报，2020(9)：27-39.

[4] Carmen Wunderlich. Rogue States as Norm Entrepreneurs：Black Sheep or Sheep in Wolves´ Clothing?[M]. Cham：Springer Nature，2020.

[5] Alan Bloomfield and Shirley V. Scott，eds. Norm Antipreneurs and the Politics of Resistance to Global Normative Change[M].London：Routledge，2017.

[6] 陈拯.框定竞争与“保护的责任”的演进[J].世界经济与政治，2014(2)：111-127.

[7] 黄宇韬.从自主争论到目标争论——新兴国家如何推动国际规范的转变[J].世界经济与政治，2023(4)：62-95

[8] 李益斌，王昊语.国际议程设置与中国倡导信息安全规范的扩散[J].外交评论，2023(2)：22-48

[9] 黄贝.国家间网络安全约束性协议何以达成[J].世界经济与政治，2024(11)：86-114.

[10] 陈冲，刘丰.国际关系的社会网络分析[J].国际政治科学，2009(4)：92-111

[11] Martha Finnemore. National Interests in International Society[M].Ithaca：Cornell University Press，1996，pp.22-24.

[12] 庞珣，何晴倩.全球价值链中的网络性权力与国际格局演变[J].中国社会科学，2021(9)：26-46.

[13] 潘亚玲.国际规范生成：理论反思与模型建构[J].欧洲研究，2019(5)：56.

[14] 陈拯.建构主义国际规范演进研究述评[J].国际政治研究，2015(1)：138-141.

[15] 王蕾.“信息就是力量”：信息生产与规范竞争[J].世界经济与政治，2023(1)：65-68.

[16] Jeffrey T. Checkel. International Institutions and Socialization in Europe：Introduction and Framework[J].International Organization，Vol.59，No.4，2005，pp.808-810.

[17] 朱立群，聂文娟.国际关系理论的“实践”转向[J].世界经济与政治，2010(8)：98-115.

[18] Martha Finnemore and Duncan B. Hollis. Constructing Norms for Global Cybersecurity[J].American Journal of International Law，Vol.110，No.3，2016，p.476.

[19] John Prpić，Araz Taeihagh，and James Melton. The Fundamentals of Policy Crowdsourcing[J].Policy & Internet，Vol.7，No.3，2015，pp.340-361.

[20] Luis Simón，Alexander Lanoszka and Hugo Meijer. Nodal Defence：the Changing Structure of US Alliance Systems in Europe and East Asia[J]. Journal of Strategic Studies，Vol.44，No.3，2021，pp.360-388.

[21] International Strategy for Cyberspace[EB/OL].https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf，2011-05-16.

[22] Cyber Norms Index and Timeline[EB/OL].https://carnegieendowment.org/projects/cybernorms?lang=en, 2025-03-10.
[23] 黄志雄,应瑶慧.美国对网络空间国际法的影响及其对中国的启示[J].复旦国际关系评论,2017(2):67.
[24] G7 Principles and Actions on Cyber[EB/OL].https://2009-2017.state.gov/s/cyberissues/releasesandremarks/258028.htm, 2016-03-13.
[25] 黄志雄.《塔林手册2.0版》:影响与启示[J].中国信息安全,2018(3):85-86.
[26] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea[EB/OL].https://trump-whitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/, 2017-12-19.
[27] Sanctions by the Numbers: Spotlight on Cyber Sanctions[EB/OL].https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber, 2021-05-04.
[28] 张华.欧盟网络制裁机制的国际法透视[J].欧洲研究,2020(6):55-56.
[29] 蔡翠红,李娟.美国亚太同盟体系中的网络安全合作[J].世界经济与政治,2018(6):51-77.
[30] 江天骄,于大皓.美国军事联盟中的网络安全合作及内在矛盾[J].东北亚论坛,2025(3):79-81.
[31] 李享.北约网络安全体系建设及其影响[J].信息安全与通信保密,2022(6):3.
[32] Joint UK-Australia Statement on Cyber Co-operation[EB/OL].https://www.gov.uk/government/news/joint-uk-australia-statement-on-cyber-co-operation, 2017-07-11.
[33] Commonwealth Cyber Declaration[EB/OL].https://thecommonwealth.org/commonwealth-cyber-declaration-2018, 2025-03-02.
[34] Australia Condemns Cyber Operations Attributed to Russia Targeting OPCW and MH17 Investigations[EB/OL].https://www.internationalcybertech.gov.au/node/88, 2018-10-05.
[35] The EU's Cybersecurity Strategy for the Digital Decade[EB/OL].https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX%3A52020JC0018, 2020-12-16.
[36] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266[EB/OL].https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf, 2021-07-13.
[37] Liisi Adamson.Let Them Roar: Small States as Cyber Norm Entrepreneurs[J].European Foreign Affairs Review, Vol.24, No.2, 2019, p.232.
[38] 张华.网络空间适用自卫权的法律不确定性与中国立场表达——基于新近各国立场文件的思考[J].云南社会科学,2021(6):81-92.
[39] National Cyber Strategy of the United States of America[EB/OL].https://www.energy.gov/sites/prod/files/2018/10/f57/National-Cyber-Strategy.pdf, 2018-09-20.
[40] National Cybersecurity Strategy[EB/OL].https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 2023-03-02.
[41] Regulation of Global Data Flows: A Story of the Impossible?[EB/OL].https://www.bfdi.bund.de/SharedDocs/Downloads/EN/DokumenteBfDI/Reden_Gastbeitraege/2022/Regulation-global-data-flows.html, 2022-05-23.

[42] Howard Solomon.Canada , U.S. in Group Planning to Bridge Global Privacy Rules [EB/OL].https : //www.itworldcanada.com/article/canada-u-s-in-group-planning-to-bridge-global-privacy-rules/480686 , 2022-04-22.

[43] Italy's Privacy Watchdog Fines Facebook 1 Million Euros [EB/OL]. https : //apnews. com/general-news-21e87c64297c4cbd8572cec83ad993f0 , 2019-06-29.

[44] Natasha Lomas. German Antitrust Office Limits Facebook's Data Gathering [EB/OL]. https : //techcrunch. com/2019/02/07/german-antitrust-office-limits-facebooks-data-gathering/ , 2019-02-07.

[45] Google Analytics and Data Transfers : The French Position [EB/OL]. https : //www.simmons-simmons.com/en/publications/cl4clgd2m17ge0a447gm3m9xn/google-analytics-and-data-transfers-the-french-position , 2022-06-13.

[46] Charlene Barshefsky. EU Digital Protectionism Risks Damaging Ties with the US [EB/OL] https : //www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103 , 2020-08-02.

[47] Patrice Navarro and Julie Schwartz. Member of French Parliament Lodges First Request for Annulment of EU-US Data Privacy Framework [EB/OL].https : //www.engage.hoganlovells.com/knowledgeservices/news/member-of-french-parliament-lodges-first-request-for-annulment-of-eu-us-data-privacy-framework , 2023-09-08.

[48] La privacy non è più la Cenerentola dei mercati globali - Intervento di Guido Scorza [EB/OL].https : //www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9890379 , 2023-05-26.

[49] FACT SHEET on U. S. -Japan Digital Trade Agreement [EB/OL]. https : //ustr. gov/about-us/policy-offices/press-office/fact-sheets/2019/october/fact-sheet-us-japan-digital-trade-agreement , 2019-10-07.

[50] Overview of DFFT [EB/OL].https : //www.digital.go.jp/en/dfft-overview-en , 2025-03-13.

[51] Brandon How. New Cyber Strategy to Consider Data Localisation Rules : O'Neil [EB/OL].https : //www.innovationaus.com/new-cyber-strategy-to-consider-data-localisation-rules-oneil/ , 2025-03-13.

[52] 华佳凡.美国及其主要盟伴跨境数据流动政策模式探因[J].当代亚太,2023(5):130-165.

〔责任编辑 孟祥臣〕

and South Korea using product space theory. The results indicate that export comparative advantages of the three countries have shifted from gradient complementarity to increasingly fierce structural competition. China is promoting a "path-creation" type of catching-up in high-tech fields, while also exhibiting "path-mixing" characteristics. Japan, on the other hand, focuses more on consolidating its comparative advantages in key upstream segments but faces challenges in expanding into new fields. South Korea is striving to enhance the autonomy of its industrial chains to address geopolitical risks while consolidating its comparative advantages in core industries. The study shows that under the influence of economic security competition and regional cooperation games, the evolution of comparative advantages is no longer a process naturally dominated by market mechanisms and technological diffusion. Political logic has become a key factor influencing the evolution of comparative advantages of China, Japan, and South Korea. And the strategic adjustments and structural competition driven by it are leading to a profound reshaping of the regional economic landscape.

Key Words: Evolution of Comparative Advantages; Economic Security; Regional Cooperation Games; Geopolitics; Product Space

Advocacy of Emerging Norms and Use of Network Power by Major Powers: A Case Study of U.S. Digital Technology Norms

HUANG Bei HUA Jia-fan ·75·

Abstract: In the process of constructing emerging international norms, the social networks formed through inter-state normative cooperation endow centrally positioned states with network power to play a leading role in norm advocacy. However, existing research has yet to fully explore the mechanisms through which states exercise such power and the effects. More specifically, network power refers to the influence a state derives from its structural position within normative cooperation networks. Major powers can leverage this power to promote norms in two primary ways. First, they may reinforce existing mechanisms of norm diffusion, such as discursive persuasion, material incentives and disincentives, and the practice of norms, by leveraging their central positions within normative networks. Second, they can mobilize partner states to participate in the diffusion process through a crowdsourcing approach, thereby amplifying their normative influence. Recent U.S. efforts to promote digital technology norms, particularly in the areas of cybersecurity and cross-border data flows, further illustrate the effectiveness of network power in advocating for emerging international norms. The findings shed light on the importance of normative cooperation networks in great power norm entrepreneurship and offer practical insights into China's engagement in global governance of emerging technologies.

Key Words: International Norms; Digital Technology; Cybersecurity; Cross-border Data Flows; Network Power

Upgraded Japan-UK Defense Cooperation: Motivations, Implications and Trends *CUI Pu-ge QU Bing* ·91·

Abstract: In recent years, Japan and the United Kingdom (UK) have strengthened defense cooperation. They have signed and practiced a series of defense cooperation agreements (DCAs) in five areas, including political consensus, information security, defense industry, operations and logistics, and interoperability. These DCAs have helped Japan and the UK enhance strategic coordination and tactical collaboration, progressively achieving the cross-border flow of information, personnel, and materials, as well as the tactical integration of their armed forces. The upgraded defense cooperation has resulted from similar security concerns and practical considerations, such as overcoming U.S. technological limitations and reducing the cost of defense research and development. It is worth noting that while increasing the security linkage between Europe and Asia, the upgraded Japan-UK defense cooperation has a clear tendency to deter China and would intensify the tension in the Indo-Pacific region. As Japan and the UK still emphasize the increasing common security threats and the need to use their defense cooperation as a hedge against the uncertainties of Trump's second term, the two countries will continue to deepen their cooperation, including addressing the relatively weak areas, such as cooperation in information security. However, the historical estrangement between the two sides, the limitation of defense resources, and the control of the alliance relationship by the U.S. restrict the development of Japan-UK cooperation.

Key Words: Japan; United Kingdom (UK); Defense Cooperation; Defense Cooperation Agreements (DCAs); Europe-Asia Interconnection; Interoperability; U.S. Factor

Pan-Securitization and U.S. Critical Equipment Exclusion Policy against China: A Case Study of ZPMC

XING Ya-jie ZHU Si-si ·108·

Abstract: In the digital age, critical equipment can be seen as a core asset tied to national security and strategic competition. During Donald Trump's first term, the United States demonstrated an increasing tendency to pan-securitize both its perception of Chinese critical equipment and the corresponding policy designs. After Joe Biden assumed office, this pan-securitization has extended further into the domain of port equipment, hyping up security threats posed by Chinese port facilities and making targeted efforts to contain and restrict the global reach of these facilities. ZPMC, a Chinese company with significant global influence, has become a focal point of these efforts. Despite of its high industrial reliance on ZPMC, the U.S. has continued to advance regulatory measures, including official inquiries, investigative hearings, and legislative restrictions. These actions aim to amplify the percieved security threat associated with ZPMC, while intensifying suppression both through vertical escalation of government interventions and through the construction of a horizontal pressure network comprising media, public discourse, and private-sector actors. These measures have disrupted industrial and maritime cooperation between China and the United States, weakened China's regional partnerships in Europe and the Global South. As a result, the logic of political competition in global port infrastructure has been reinforced, and global port development and cooperation face increasing challenges.

Key Words: Port Equipment; Pan-securitization; ZPMC; Critical Equipment; Strategic Anxiety