科技企业与网络空间国际秩序构建

——基于倡导网络安全规范的视角 *

杨 乐 郎 平

数字时代，具有技术和数据资源优势的科技企业成为影响国际秩序的潜在行动者，但科技企业以何种方式影响国际秩序以及影响程度如何，则需进一步研究。目前网络空间仍然缺乏具有强约束力的国际规则，网络空间国际规范成为构建网络空间国际秩序的有效方式。本文聚焦科技企业微软、西门子和华为倡导网络安全国际规范的实践，形成所属不同国家、不同规范倡导路径和效果的案例光谱。比较研究发现，科技企业中领先的网络规范倡导者已经形成较为成熟的倡导路径，但较难在行业内普及；科技企业倡导行业落实的网络规范比倡导国家落实的网络规范效果更好；科技企业倡导的网络规范能够进入国家主导的国际规范进程，但易受国家间数字竞争和地缘政治的影响。当前，科技企业愈发具备倡导网络空间国际规范的能力和动力，未来主权国家和科技企业依托自身优势实现网络规范对接，协同倡导规范成为构建网络空间国际秩序的可行路径。

关键词：国际秩序 国际规范 科技企业 网络空间治理

问题引出

近年来，科技企业在与主权国家的互动中凭借自身数字技术资源优势，逐渐

杨乐系清华大学新闻与传播学院博士研究生，Email: yanglejoy@163.com；郎平系中国社会科学院世界经济与政治研究所研究员。

* 本文系国家社会科学基金重大项目“网络空间国际规则博弈的中国主张与话语权研究”（项目编号：20&ZD204）和国家社会科学基金一般项目“全球数字治理下的国际互联网规则形成机制研究”（项目编号：21BXW008）的阶段性研究成果。感谢匿审专家对文本所提的宝贵修改意见，以及清华大学新闻与传播学院硕士研究生周玥对文章文本分析部分的助研支持。文责自负。

表现出影响国际秩序的能力。2010年一名突尼斯青年在政府大楼前自焚的视频在用户量过10亿的社交媒体上疯传，开启了至今尚未平息的“阿拉伯之春颜色革命”，直接冲击了现代国家的政权稳定和地区秩序。2021年澳大利亚政府曾策划出台《新闻媒体和数字平台强制性议价法案》，要求互联网平台企业对其平台上的新闻内容向新闻媒体机构付费，脸书（Meta）为阻止该法案的通过，直接屏蔽了澳大利亚新闻媒体在该平台的全部信息。[1]2022年俄乌冲突中，科技企业更是化身“硅谷军团”直接介入。冲突爆发后，乌克兰副总理米哈伊洛·费多罗夫（Mykhailo Fedorov）通过推特平台直接给各大科技巨头写公开信请求科技援助，“面对战争，现代技术是对坦克、火箭和导弹的最佳回应”。[2]作为回应，美国社交媒体脸书封禁俄罗斯官方媒体账号以阻断俄罗斯的“战争宣传”，ICT（信息与通信）科技巨头切断在俄罗斯市场的部分数字化服务和停止芯片供应，马斯克（Elon Musk）的太空探索技术公司（SpaceX）启动卫星通信服务星链（Starlink）保障乌克兰的互联网使用。[3]美国科技企业通过信息操纵、生态封禁和技术断供等方式对俄罗斯进行打压，直接影响了俄罗斯的国内经济和社会稳定。[4]

一系列科技企业卷入国内和国际事务的现象，不禁让人预设现今的科技企业已是能够影响国际秩序的行为者，2021年学者们曾以科技企业能否重塑全球秩序展开过辩论。2021年10月，欧亚集团主席伊安·布雷默（Ian Bremmer）在《外交事务》上发表“技术极化时刻：科技巨头如何重塑全球秩序”一文指出，以亚马逊、谷歌、苹果、阿里巴巴、字节跳动等为代表的科技巨头通过控制其代码、服务器和制定规范等方式行使了传统国家专属的权力，正在成为强大的、自主的地缘政治塑造者。[5]布雷默认为，一方面，这些科技企业不仅是在物理世界行使权力，在数字空间也愈发拥有更大的权力，并且政府对数字空间无法完全控制；

[1] BBC,“Facebook Reverses Ban on News Pages in Australia”, February 23, 2021. https://www.bbc.co.uk/news/world-australia-56165015[2023-04-28].

[2] Mykhailo Fedorov, Twitter, Feburary 26, 2022, https: //twitter.com/FedorovMykhailo/status/1497327555690610689/[2022-03-15].

[3] Fox C. H. and Probasco E. S.,“Big Tech Goes to War to Help Ukraine, Washington and Silicon Valley Must Work Together”, *Foreign Affairs*, October 19, 2022, https://www.foreignaffairs.com/ukraine/big-tech-goes-war/[2023-10-19].

[4] 刘典：“科技巨头重塑地缘格局：审视俄乌冲突中的数字权力竞争”，《东方学刊》，2022年第2期。

[5] Bremmer I.,“The Technopolar Moment How Digital Powers Will Reshape the Global Order”, *Foreign Affairs*, October 19, 2021, https://www. foreignaffairs. com/articles/world/ian-bremmer-big-tech-global-order/[2023-10-19].

另一方面，它们越来越多地提供现代社会运转所需的虚拟产品和现实产品的全方位服务，对政府权力进行收编，影响人们的观念和行为。2021年11月，哈佛大学教授斯蒂芬·沃尔特（Stephen M. Walt）则在《外交政策》上发表“科技巨头不会重造全球秩序”对布雷默的观点进行反驳。[1]沃尔特认为物理世界是必备的，数字空间是可选的。物理世界提供着人们的生存必需品，而数字空间提供的产品可以被代替或者放弃，数字空间的各种产品与服务最终还是依赖于物理世界的运转。

两位学者认识到当前科技企业对国际秩序产生影响的潜在能力，并且强调了科技企业对数字空间即网络空间的重大影响。数字化技术不断嵌入政治、经济和社会事务，加速了现实世界和虚拟世界的融合，由此形成的网络空间成为人类活动的主要场所，网络空间成为国际秩序的重要场域，科技企业对网络空间秩序的影响亦将映射到国际秩序中。数字时代科技企业成为国际社会新兴力量，科技企业的技术逻辑、产品与服务以及企业文化深刻影响着网络空间秩序与国际秩序的未来。作为与主权国家身份和实力资源不对等的科技企业如何影响网络空间国际秩序？当前科技企业影响网络空间国际秩序的效果如何？这些问题将是理解数字时代国际秩序变化的新视角。

文献综述

本文的核心研究对象为科技企业，但并非一般意义上从事科技产品和服务研发和售卖的科技企业，而是在生产、经营、服务等重要环节具有优势地位的大型跨国科技企业，常被视为超国家行为体；该类科技企业的产品与服务能够对国际秩序产生影响，常与国际安全和经济议题强相关；该类科技企业有志于塑造网络空间国际规则，常活跃于国际社会的网络空间治理活动。因此，本文的文献回顾将围绕该类科技企业，从跨国企业如何影响国际秩序、科技企业与网络空间国际秩序以及科技企业倡导网络规范等方面展开。

企业对国际秩序的影响发端于国际政治经济研究，企业作为典型的经济主体如何影响主权国家是其核心关切。跨国企业主权侵蚀论是典型研究之一，20世纪60年代制度经济学学者约翰·罗杰斯·康芒斯（John R. Commons）最早将“主

[1] Walt S. M.,“Big Tech Won’t Remake the Global Order”, *Foreign Policy*, Nonmember 8,2021,https://foreignpolicy.com/2021/11/08/big-tech-wont-remake-the-global-order/[2023-08-20].

权”概念用于经济学，[1]70年代雷蒙德·弗农（Raymond Vernon）正式提出跨国公司在国际市场上的纵横捭阖已使“主权国家陷入困境”。[2]90年代苏珊·斯特兰奇（Susan Strange）则直接将公司作为与主权国家平等的行为体纳入传统国家间博弈中。[3]关于企业如何影响国家，弗农认为跨国公司的扩张会对国民经济、民族精英、意识形态和文化产生冲击。[4]特奥托尼奥·多斯桑托斯（Theotônio dos Santos Junior）认为跨国公司能汇聚各行精英领袖，组成准国家型政府，对当地技术和金融进行控制。[5]黄河发现跨国公司还能通过股权并购等方式获得东道国企业的控制权，进而取得东道国经济的控制权。[6]孙溯源则通过对具体的跨国石油企业研究发现，跨国企业的政治献金和院外游说活动也会影响当地政府的对内对外政策。[7]

政治经济学研究认识到传统跨国企业的资本扩张造成对主权国家的挑战，国际政治学者在此基础上进一步关注到跨国企业对国际秩序的影响。最为典型的为罗伯特·基欧汉（Robert Keohane）和约瑟夫·奈（Joseph Nye）1971年的《跨国关系与世界政治》以及1977年的《权力与相互依赖》较早打破现实主义下的国家中心论，强调了非国家行为体和跨国联系对国际秩序的影响，跨国企业作为跨国组织的一种形式发挥作用。[8]可以说20世纪70年代开启的对非国家行为体的学术讨论，奠定了非国家行为体参与国际事务的必要性，也让人们认识到非国家行为体对国际政治与经济带来的潜在影响，自此企业作为非国家行为体的一种形式一直在国际政治研究的视野当中。

传统跨国企业以制造业和大宗商品出口企业为主，随着第四次工业革命以及信息时代的到来，以信息和数据为原材料的科技巨头成为能够影响国际秩序的新主体。有研究者将这种科技企业称为非传统型跨国公司，与传统跨国公司相比，

[1] [美] 约翰·罗杰斯·康芒斯：《制度经济学》，北京：商务印书馆，1962年。

[2] Vernon R.,“Sovereignty at Bay”, Pelican, 1971.

[3] Strange S., *The Erosion of the State*, Current History, 1997. [英]约翰·斯托普福德，查立友等译：《竞争的国家 竞争的公司》，北京：社会科学文献出版社，2003年。

[4] Vernon R., *Sovereignty at Bay: The Multinational Spread of U.S. Enterprises*, New York & London: Basic Books, 1971.

[5] [巴西]特奥托尼奥·多斯桑托斯，杨衍永等译：《帝国主义与依附》，北京：社会科学文献出版社，1999年。

[6] 黄河：《跨国公司与当代国际关系》，上海：上海人民出版社，2008年。

[7] 孙溯源：《国际石油公司研究》，上海：上海人民出版社，2010年。

[8] Keohane R. O. and Nye, Jr, J. S. (Eds.), *Transnational Relations and World Politics*, Cambridge Mass: Harvard University Press, 1972.

其呈现出公司资产形态逐渐向无形资产转变，在企业间进行关联交易时，相关的交易标的由传统的原材料、商品等有形资产向数据、信息等无形资产发生转移的特征。[1]黄河将高科技和互联网行业为代表的企业视为这种非传统型跨国公司，认为其具备谋求全球化技术统治、重构国家与市场和打造新型数字剥削形式的潜力。[2]布雷默提出的科技巨头重新塑造全球秩序论，也认为政府无法控制数字空间正在产生的更大新型权力，科技巨头通过控制其代码、服务器和用户守则等正在实施传统国家专属的权力。[3]在新晋的科技平台企业研究中，更有学者发现，平台正在消减国家政府权力、限缩个人和社会的权力，扩大以私营企业为主体的市场部门的权力。[4]

既有研究表明，企业影响国际秩序多表现为企业通过壮大资本和对关键资源的掌握削弱主权国家权力，企业研发的产品能够造成重大的社会政治经济影响，以及企业作为国家竞争力的组成部分卷入到政治博弈中。这些企业影响国际秩序的机制是将企业作为技术和资本的负载体，更多是被动地卷入到国际纷争中影响国际秩序。但企业对国际秩序的影响不仅仅表现为企业对国家主权的影响，也不局限于企业权力与国家权力的竞争以及企业产品对国际社会的影响。国际秩序这一概念有着共识性的内涵界定，研究科技企业如何影响国际秩序应该从其概念本身入手。亨利·基辛格（Henry Kissinger）在《世界秩序》一书中认为，各国接受的规则和规则破坏后各方自我克制形成的均势构成国际秩序。[5]赫德里·布尔（Hedley Norman Bull）把共同利益、国际规则和制度视为国际秩序三要素。[6]阎学通在厘清国际秩序、国际格局和国际体系概念的基础上认为，国际秩序的基本要素为国际主流价值观、国际规范和国际制度安排，国际规范是国际秩序形成的核心条件。[7]邹治波将国际秩序的要素定位为国际行为体（基本要素）、国际规

[1] 梁潇："传统经济与数字经济下跨国公司转让定价问题研究"，《宏观经济研究》，2019年第4期。

[2] 黄河、周骁："超越主权：跨国公司对国际政治经济秩序的影响与重塑"，《深圳大学学报》（人文社会科学版），2022年第1期。

[3] Bremmer I., "The Technopolar Moment How Digital Powers Will Reshape the Global Order", *Foreign Affairs*, October 19, 2021,https://www.foreignaffairs.com/articles/world/ian-bremmer-big-tech-global-order/[2023-10-19].

[4] 刘金河："权力流散：平台崛起与社会权力结构变迁"，《探索与争鸣》，2022年第2期。

[5] [美]亨利·基辛格著，胡利平译：《世界秩序》，北京：中信出版社，2015年。

[6] [英]赫德利·布尔著，张小明译：《无政府社会：世界政治秩序研究》，北京：北京大学出版社，2007年。

[7] 阎学通："无序体系中的国际秩序"，《国际政治科学》，2016年第1期。

范（核心要素）和惩戒机制（必要要素）。[1]可以看出，国际规范是国际秩序的核心要素之一。对于规范，一个被普遍接受的定义是对某个特定身份所应当采取的适当行为的集体期望。[2]它既能反映某个人群真实的行为模式，又能体现该人群所普遍接受的价值观。[3]因此，国际规范在塑造国际秩序中发挥着两方面的作用：一方面，通过国际规范寄希望于在特定领域各行为体能够对行为达成大致一致的价值判断、形成趋同的行为，增强行为的确定性和预见性，从而形成有序的国际社会环境；另一方面，国际规范是国家可以依据的行为标准，通过遵守国际规范的制度安排和考虑违反国际规范的成本，从而约束其行为。

本文聚焦网络空间国际秩序。既有关于网络空间国际秩序形成机制的研究曾明确定义网络空间国际秩序，指“网络空间不同行为体通过确立相应的制度安排制定国际规范、解决不同层次的问题和冲突的过程，从而避免冲突升级为不可控的状态”。[4]本文将沿用国际规范是网络空间国际秩序关键要素的定义，并在此基础上分析科技企业如何倡导网络安全国际规范影响国际秩序。之所以选择网络安全国际规范，一方面，国际安全是国际秩序的核心，网络安全问题将直接影响国际安全的状态；另一方面，安全议题是传统主权国家主导的核心议题，科技企业若能影响网络安全议题，则更能体现出其作为非国家行为体影响网络空间秩序的能力。因此，本文将科技企业视为具有独立能动性的行为体，以科技企业影响网络安全国际规范的形成作为切入点，分析其倡导网络安全国际规范以建构网络空间国际秩序的能力。

目前，网络空间是人类活动的重要场所，掌握数据和技术资源优势的科技企业有望成为网络空间秩序的构建者，特别是在网络空间仍然缺乏国际规范和国际规则的情况下。正如玛莎·芬尼摩尔（Martha Finnemore）所言，“政府或许不是制定该领域规则的最佳或唯一参与者，因为许多技术掌握在私营部门手中”。[5]王蕾发现互联网企业及非政府组织正在以一种“自下而上”的方式有效参与到网络安全国际规范的制定中。[6]在具体的网络安全国际规范形成过程中，科技企业

[1] 邹治波：“国际秩序的评判研究”，《世界经济与政治》，2022年第5期。

[2] [美]彼得·卡赞斯坦主编，宋伟、刘铁娃译：《国家安全的文化：世界政治中的规范与认同》，北京：北京大学出版社，2009年。

[3] 曹玮：《国际关系理论教程》，北京：中国社会科学出版社，2020年。

[4] 郎平：“网络空间国际秩序的形成机制”，《国际政治科学》，2018年第1期。

[5] Finnemore M. and Hollis D. B., “Constructing Norms for Global Cybersecurity”, *American Journal of International Law*, 110(3): 425–479, 2016.

[6] 王蕾：“自下而上的规范制定与网络安全国际规范的生成”，《国际安全研究》，2022年第5期。

能够促进各方对网络安全概念的理解并有利于形成规范共识。[1]对现实的观察也发现，近年来科技企业不仅积极参与联合国框架下的网络空间国际规范制定，自身也发起了多项网络规范议程。[2]在科技企业作为网络空间国际规范倡导者的实践中，既有研究注意到微软提出的部分议题和倡议已经进入政治层面。[3]2020年丹尼斯·布鲁德斯（Dennis Broeders）等学者编撰的《网络空间治理：行为、权力和外交》论文集中，专门有一章探讨了网络空间治理中非国家行为体的参与，对科技企业和非政府组织等非国家行为体倡导网络空间国际规范进行了较为全面的分析。[4]基于以上研究，本文将以科技企业倡导网络安全国际规范的实践为例，探寻其倡导路径，评估倡导效果，从而分析当前科技企业以独立行为体的身份影响网络空间国际秩序构建的可行性。

科技企业与网络空间国际秩序的困境

网络空间是互联网高度普及后人类活动的新空间，维护国际秩序的传统权力由主权国家主导，但网络空间打破了传统主权国家对权力的垄断。权力运行方式的改变使既有国际规则体系难以维系，网络空间面临缺乏国际规则的挑战，表现为既有国际规则在网络空间不适用、新的规则难达成。但与此同时，具备技术和人才资源优势的科技企业在网络空间秩序面临失灵之时具有参与网络空间治理的能力和动力，成为推动网络空间有序发展的重要力量。

（一）网络改变维护国际秩序的传统权力

主权国家的权力行使维护着国际秩序，但网络对国家权力的要素、形式及实

[1] Abrahamsen R. and Leander A.,“Routledge Handbook of Private Security Studies”, Routledge, Taylor & Francis Group, 2016.

[2] Eggenschwiler J. and Kulesza J.,“Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace”, in *Governing Cyberspace. Behavior, Power and Diplomacy*, Edited by Broeders D. and Van Den Berg B., Rowman & Littlefield Publishers, 2020. 杨乐、崔保国：“科技企业参与联合国框架下网络空间国际规则进程2022年度回顾”，《中国信息安全》，2022年第2期。

[3] Jeutner V.,“The Digital Geneva Convention: A Critical Appraisal of Microsoft’s Proposal”, *Journal of International Humanitarian Legal Studies*, 10(1): 158-170, 2019.

[4] Gorwa R. and Peez A.,“Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft’s Cybersecurity Tech Accord”, 2018; Hurel L. M. and Lobato L. C.,“Cyber-Norms Entrepreneurship? Understanding Microsoft’s Advocacy on Cybersecurity. Governing Cyberspace: Behaviour, Power and Diplomacy”, in *Governing Cyberspace. Behavior, Power and Diplomacy*, Edited by Broeders D. and Van Den Berg B, Rowman & Littlefield Publishers,2020.

施方式带来全面影响。在传统国家实力构成中，领土面积、军事武器、人口规模、经济生产等国家资源是衡量国家实力的重要指标。但网络空间的核心是数据和技术，谁拥有数据，谁掌握技术，谁就拥有更多的权力。正如叶成城在讨论数字时代大国竞争中提出的观点，数字时代下数据、硬件与算法成为核心生产资料，用户数据的获取能力、智能算法的编写能力与核心硬件的研发能力成为核心数字资源。[1]而这些核心数字资源当前都散落在非国家行为体之中，特别是科技企业和互联网技术社群组织。军事权力方面，ICT技术的军民两用性和网络攻击技术的低门槛打破了传统国家对军事的垄断，使大量的个人和组织团体拥有了网络军事能力。经济和社会方面，互联网科技企业打造的数字经济正在成为拉动国家经济发展的主要引擎，占一国国内生产总值（GDP）份额日益增多。[2]社交媒体企业已经能够塑造人们的社会观念和行为，传统国家掌控的“公权力”逐渐被私有化。[3]网络空间衍生的人类活动新场景和权力新形式正在从政治、经济、军事和社会等多方面对传统国家权力产生冲击。

事实上，网络技术打破了部分传统国家的权力垄断，使权力转移到非国家行为体手中，特别是拥有数据和技术资源的科技企业。约瑟夫·奈曾在评估网络空间对国家权力影响时认为，国家已不再是网络空间唯一的行为体，个人和私营组织也能在世界政治中发挥直接作用，非正式网络可以削弱传统官僚机构的垄断地，权力正在从国家行为体向非国家行为体扩散。[4]在数据赋权驱动下，拥有数据、掌握技术的科技企业成为非国家行为体的代表，有望成为网络空间国际秩序的建构者。科技企业的产品、用户遍布全球，微软、脸书、腾讯、字节跳动等科技巨头的用户量都超过10亿，一家企业的产品技术规则可以全球应用。利用技术和知识资源，科技企业不断提高其研发能力以增强产品竞争力，引领了以人工智能、5G、区块链、量子计算为代表的新一轮科技浪潮。

（二）网络空间面临国际规范赤字挑战

网络空间国际秩序需要新的规则体系维护，但主权国家面临网络空间国际规范赤字的新挑战。网络空间不同于传统现实世界，原有的国际规则体系难以直接移植至网络空间，新的网络空间“硬法”也难以在短期内建立。以网络恶意行

[1] 叶成城：“数字时代的大国竞争：国家与市场的逻辑——以中美数字竞争为例”，《外交评论（外交学院学报）》，2022年第2期。

[2] 阎学通、徐舟：“数字时代初期的中美竞争”，《国际政治科学》，2021年第1期。

[3] 刘金河：“权力流散：平台崛起与社会权力结构变迁”，《探索与争鸣》，2022年第2期。

[4] [美]约瑟夫·奈著，王吉美译：《权力大未来》，北京：中信出版社，2012年。

为、网络犯罪、数字贸易为代表的网络空间新兴治理议题反映出网络空间治理的全新性，但新兴议题国际规则匮乏是当前面临的难题。网络恶意行为颠覆了传统作战的形式，既有战争法和人道主义法如何应用于网络空间尚未明确，2013年开启的《塔林手册》进程致力于制定适用于网络空间的战争法，但其由欧美法学学者主导，较难发展成为国家间普遍承认的国际法。2019年联合国框架下开启的《联合国打击网络犯罪公约》旨在达成在打击网络犯罪中具有法律约束力的国际公约，但主权国家在术语使用、基本原则、定罪范围和国际合作等核心议题上仍然未达成共识，公约进程举步维艰。[1]数字贸易规则方面，以世界贸易组织（WTO）、二十国集团（G20）、经济合作与发展组织（OECD）等既有政府间组织主导推进，以《区域全面经济伙伴关系协定》（RCEP）、《数字经济伙伴关系协定》（DEPA）、《全面与进步跨太平洋伙伴关系协定》（CPTPP）为代表的多边谈判并行推进，但大国博弈充斥其中，就数据跨境流动、数字贸易规则等核心议题迟迟难以达成共识。[2]

联合国框架下，20世纪90年代就开启了遏制网络空间恶意行为的国际规范进程，但实质性成效缓慢。1998年，俄罗斯向联合国大会裁军和国际安全事务委员会提交“约束信息通信技术不当使用，并强化全球信息与电信系统安全性”的提案。联大通过提案并于2004年成立联合国信息安全政府专家组（UNGGE），该机制是目前主权国家推进构建网络空间国家负责任行为规范的核心议程。然而，随着UNGGE的议题进入深水区，各方分歧愈发明显，被寄予厚望的2017年组会未能形成共识性报告。互联网治理学者米尔顿·穆勒（Milton Mueller）曾在2017 UNGGE组会失败后发表“永别了，规范”一文，断定了网络规范难以达成的现实。[3]为继续推进UNGGE进程，2019年开启了与UNGGE并行的开放式工作组（OEWG），OEWG作为非正式咨询会议面向联合国所有成员国和非国家行为体开放，试图解决UNGGE代表性不足的难题，但实质性进程依然缓慢。联合国框架下规范进程的屡屡受阻印证了研究者观察到的，网络空间正处于国际秩序的形成时期，就网络空间的整体安全和稳定而言，国际规范仍然是一片空白。[4]

---

[1] 姜博谦、王渊洁：“2022年度《联合国打击网络犯罪公约》谈判进展”，《中国信息安全》，2023年第1期。

[2] 中国信通院：《全球数字经贸规则年度观察报告（2022年）》，集智白皮书N0.202211。

[3] Mueller M. L.,“ A Farewell to Norm”, September 4, 2018, https://www.internetgovernance.org/2018/09/04/a-farewell-to-norms/[2023-08-20].

[4] 郎平：“网络空间国际秩序的形成机制”，《国际政治科学》，2018年第1期。

（三）科技企业倡导网络空间国际规范

科技企业掌握的数字资源使其具备参与网络空间国际规范制定的内在能力。网络空间的核心是数据和技术，如今这些核心数字化生产资料大多掌握在科技企业手中，生产力也为科技企业所有。全球最受欢迎的社交软件脸书目前每月活跃用户近30亿，2020年脸书创造和存储的数字信息超过640亿太字节（TB），足以填满约5000亿部智能手机。5G和物联网的发展将使汽车、工厂和整个城市都与传感器连接，由此生产的数据将进一步激发数据生产力，而科技企业将掌控数据生产力。此外，ICT技术的军民两用性使掌握网络安全技术的科技公司具备了网络军事能力。科技企业对数字资源的掌握使其拥有了参与网络空间国际规范制定的更强话语权。

同时，科技企业遭受严峻的网络安全威胁使其具备参与网络空间国际规范制定的外在动力。ICT技术的军民两用性使科技企业不仅是网络安全的保障者也成为网络攻击的目标，根据2021年深度追踪（Darktrace）发布的最新报告， ICT产业超过金融产业成为2021年全球网络犯罪分子最常针对的领域，ICT攻击目标包括电信提供商、软件开发商和托管安全服务提供商等。2020年12月为用户提供网络基础设施管理的美国太阳风（SolarWinds）软件公司，被黑客植入木马，高达200多家重要机构受到攻击，波及北美、欧洲等全球重要科技发达地区，其中美国占比超过60%。[1]多达250个组织遭受了第二阶段的攻击，最终源起于SolarWinds的ICT供应链攻击事件导致全球18000多个组织受影响。网络安全威胁已对科技企业的切身利益产生直接影响，这促使其倡导网络空间国际规范约束网络空间行为。正是在拥有技术和数据资源优势的科技企业具备参与制定网络空间国际规范的内在能力和外在动力的基础上，科技企业开始大力倡导网络安全国际规范。

科技企业倡导网络安全国际规范的实践

欧美国家是传统的科技强国，以微软和西门子为代表的老牌科技企业在数字时代有着先发优势，中国作为新兴大国大力发展科技产业，培育出华为等具有全球竞争力的科技企业。面对日益严峻的网络空间威胁，不同企业基于自身发展和

[1] CISA, Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, December 17,2020. https://www.cisa.gov/uscert/ncas/alerts/aa20-352a[2022-10-21].

外部环境采取不同的方式倡导网络安全国际规范，力图通过产业力量建构网络空间国际秩序。美国微软、德国西门子和中国华为形成了科技企业倡导网络安全国际规范不同路径和影响效果的实践光谱。

（一）微软依托产业倡导影响政府的网络规范

微软作为全球科技巨头提供200多种在线服务，拥有全球超过10亿的用户群体。2013年的“斯诺登事件”揭秘了包括微软在内的九家美国科技企业加入美国国家安全局的“棱镜”计划，允许国安局直接访问其用户电子邮箱、聊天记录、视频、照片等多项个人信息数据。[1]一时间，微软卷入巨大的用户信任风波，在通过加强产品安全性和以司法途径起诉政府过度获取企业数据后，微软也开始建立网络安全规范试图指导和约束网络空间各方行为。十年前微软曾以倡导规范的方式发布《Windows原则：促进竞争的十二项规范》以解决政府的反垄断诉讼，其高层管理者深知在与政府互动中通过倡导规范影响国家行为的可行性。[2]“斯诺登事件”后国际社会强烈意识到网络安全对国家安全和个人隐私安全的重要性，对于政府过度收集个人信息的行为，企业和用户都提高了警惕，迫切需要国际规则约束政府和企业的行为以保障数据与隐私安全。在此背景下，微软倡导网络安全国际规范不仅是维护企业自身利益，也满足了国际社会对网络安全保障迫切性的需求。截至2023年10月，微软共发布8份网络安全规范报告，提出了“数字日内瓦公约”[3]和“私营企业在网络空间负责任行为规范”等在国际社会引起广泛关注的网络安全规范，并且通过打造产业界网络安全联盟、影响国家主导的网络安全规范内容和与主权国家规范进程互动，不断提升其作为规范倡导者的影响力。

1.打造强代表性的网络安全产业联盟

2017年微软提出的“数字日内瓦公约”在国际社会引起广泛关注，2018年4月微软联合34家企业共同发起了企业间的网络安全联盟——网络安全技术协议（Cybersecurity Tech Accord，简称Tech Accord），作为实体产业联盟平台进一步推

[1] The Guardian,“NSA Prism Program Taps in to User Data of Apple, Google and Others”, June 7, 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data/[2022-11-22].

[2] [美]布拉德·史密斯、卡罗尔·安·布朗著，杨静娴、赵磊译：《工具还是武器》，北京：中信出版社，2020年。

[3] Smith B.,“The Need for a Digital Geneva Convention, Transcript of Keynote Address at the RSA Conference 2017”, https://blogs.microsoft.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf[2023-10-22].

广微软倡导的规范倡议。截至2022年11月，Tech Accord已经有161家科技企业联名签署，覆盖多样化的科技行业（见图1）。Tech Accord纳入了网络安全、IT和云数据安全领域的较多核心企业，特别是美国Telelink、英国BT、法国Orange和日本NTT等8个国家级电信巨头的签署使Tech Accord在产业界获得了全球性影响力，有效增强了其作为网络安全规范倡导者的合法性，使其能够获得主权国家的关注并给予其准国家主体的协商谈判地位。Tech Accord签署成员具有国际化特征，涵盖了23个非美国本土企业，覆盖了北美、拉丁美洲、欧洲、亚洲和非洲地区（见图2）。

图1 Tech Accord网络安全产业联盟签署企业的行业分布

资料来源：笔者根据Tech Accord官网新闻数据整理。

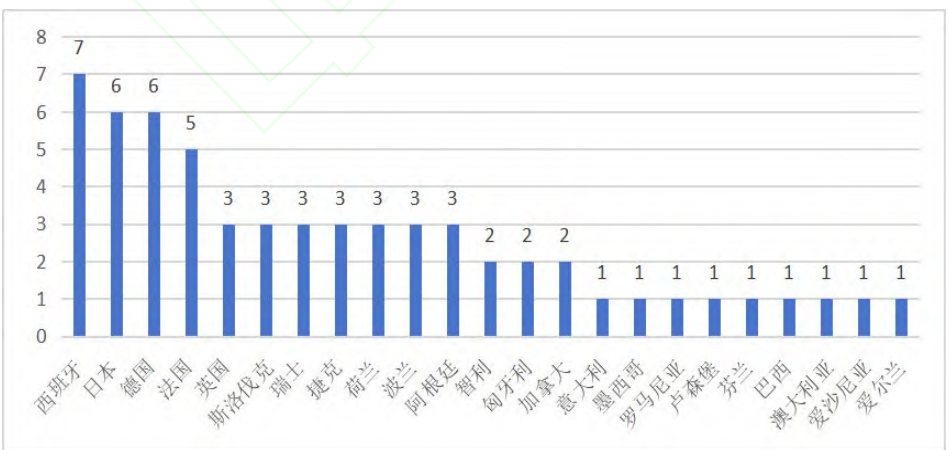

图2 Tech Accord签署企业所属国家分布（除美国本土101家签署企业外）

资料来源：笔者根据Tech Accord官网新闻数据整理。

2.影响网络空间负责任的国家行为规范

网络空间负责任的国家行为规范（Norms of Responsible State Behavior）是目前主权国家在UNGGE和OEWG机制下推动的约束国家网络空间行为的主要国际规范进程，微软作为科技企业积极倡导网络安全规范，试图影响该议程。本文对UNGGE和OEWG的5份报告中负责任的国家行为规范文本部分和微软的8份网络安全规范倡导文件进行文本分析。研究发现，在UNGGE和微软重合的9项议题中，避免国家使用ICT技术威胁国际和平、负责任地披露漏洞、禁止开发或扩散有害隐藏功能、保障网络武器不扩散、共享技术信息类型、国际合作及与私营企业合作控制网络武器扩散这6项议题微软先于UNGGE提出（见表1）。

表1 微软与UNGGE和OEWG的网络安全规范的议程设置

序号	议题内容	微软提出时间	UNGGE提出时间	议题主题
1	鼓励各国避免使用ICT和ICT网络开展可能威胁国际和平的行动。	2013年，2014年，2016年，2017年，2018年	2015年，2021年	避免国家使用ICT技术威胁国际和平
2	各国确保迅速解决ICT漏洞以减少被恶意行为者利用的可能性。及时发现和负责任地披露和报告ICT漏洞可以防止有害或威胁性，增加信任和信心，并减少对国际安全和稳定的相关威胁。	2013年，2014年，2016年，2017年，2018年	2015年，2021年	负责任地披露漏洞
3	禁止在ICT产品中引入有害的隐藏功能和利用漏洞的措施，这些漏洞可能危及系统和网络（包括关键基础设施）的机密性、完整性和可用性。	2014年，2016年，2017年，2018年	2015年，2021年	禁止开发或扩散有害隐藏功能
4	各国应致力于保障网络武器不扩散。	2016年，2017年，2018年	2021年	保障网络武器不扩散
5	披露或公开共享的技术信息类型，包括共享严重ICT事件的技术信息以及如何处理敏感数据并确保信息的安全性和机密性。	2013年，2014年，2016年，2017年	2015年，2021年	共享技术信息类型
6	各国应同意与国际伙伴合作，并在可行的范围内与私营企业合作，控制网络武器的扩散。	2014年，2017年，2018年	2021年	国际合作、与私营企业合作控制网络武器扩散

资料来源：笔者对UNGGE和OEWG的5份报告中负责任的国家行为规范文本和微软的

8份网络安全规范倡导文件进行文本分析所制。[1]

9项重合议题说明微软已经开始自主倡导约束网络空间国家行为的规范，6项规范先于UNGGE提出来虽然不能证明微软直接设置了UNGGE的议程，但在一定程度上可以说微软倡导的规范引起了主权国家的注意并可能获得了一定程度上的采纳，具备影响UNGGE议程中负责任国家行为规范的可能性。

3.联动主权国家主导的多边网络规范进程

微软利用网络空间多利益攸关方模式积极参与国家主导的多边治理进程，与主权国家主导的规范进行多领域互动推进规范扩散。在联合国框架下，微软借助Tech Accord平台积极参与UNGGE和OEWG开设的非国家行为体咨商会议，发布立场声明，将网络空间负责任的国家行为规范与微软倡导的网络规范相勾连。在联合国高级别数字经济工作组（High-level Panel on Digital Cooperation）进程中，Tech Accord从行业技术视角针对高级别工作组运作提出意见。[2]在OECD数字经济安全工作组进程中，微软参与工作组《加强数字产品安全》《负责任的管理和披露漏洞》等报告起草和对报告提出咨询意见。[3]Tech Accord也曾向美洲国家组织（Organization of American States，OAS）提交九项具体建议促进其网络空间信任措施倡议的落实。[4]

此外，微软积极与美国、法国、澳大利亚等网络安全规范倡导国保持互动。Tech Accord加入美国漏洞权益进程（US Vulnerability Equities Process），围绕防御

[1] 笔者与另一名编码者利用DiVo Miner数据挖掘平台对所选取的13份研究样本进行编码与数据分析，分析指标包括“网络安全规范议题”“发布主体”“发布年份”三个主要类目，其中“网络安全规范议题”类目下涵盖“鼓励各国避免使用ICT和ICT网络开展可能威胁国际和平的行动”等77个指标，“发布主体”类目下设“OEWG”“UNGGE”“微软”3个指标；“发布年份”下设8个不重复的年份指标。

[2] Tech Accord, “Cybersecurity Tech Accord Submission to the UN High Level Panel on Digital Cooperation”, https://cybertechaccord. org/uploads/prod/2018/12/Tech-Accord-HLP-Response-Dec-2018. pdf/[2020-01-22].

[3] Tech Accord, “Cybersecurity Tech Accord Letter to OECD Scoping Paper on Digital Security of Products”, January 10, 2020, https://cybertechaccord. org/cybersecurity-tech-accord-letter-to-oecd-scoping-paper-on-security-of-digital-products/[2023-04-21]; Tech Accord, “Cybersecurity Tech Accord Comments on OECD Work on Responsible Management and Disclosure of Vulnerabilities”, January 31, 2020, https://cybertechaccord. org/cybersecurity-tech-accord-comments-on-oecd-work-on-responsible-management-and-disclosure-of-vulnerabilities/[2023-04-23].

[4] Tech Accord, “Reducing Tensions in Cyberspace by Promoting Cooperation: Cybersecurity Tech Accord Publishes a Set of Recommendations on Confidence-building Measures in Cyberspace”, April 4, 2019, https://cybertechaccord. org/reducing-tensions-in-cyberspace-by-promoting-cooperation-cybersecurity-tech-accord-publishes-a-set-of-recommendations-on-confidence-building-measures-in-cyberspace/[2023-04-22].

性ICT技术和进攻性ICT技术概念提出一系列应对网络漏洞的建议。微软总裁施密特与法国网络外交和数字经济大使以及总统外事顾问有着密切的接触，使微软获得参与法国主导的《网络安全巴黎倡议》起草机会，[1]Tech Accord还担任着《网络安全巴黎倡议》第三工作组的联席主席。该倡议提出九项网络空间治理原则，在国际社会有着较大影响力，[2]截至2022年11月，该倡议已经获得81个国家政府、706家企业、390个社会组织和36个公共部门（Public Authority）的支持。此外，Tech Accord还曾为第六届UNGGE参与国澳大利亚的负责任国家行为议题提供咨询意见。[3]依托Tech Accord平台，微软以“准国家”的身份积极参与主权国家主导的网络空间治理进程，并凭借技术优势给予国家网络空间治理进程以技术方面的政策咨询和指导。

（二）西门子聚焦产业界倡导网络安全规范

2017年UNGGE未能达成共识性报告的组会失败结果，以及同年发生的WannaCry和Petya/NotPetya等跨国重大网络安全事件，使得应对网络安全威胁的迫切性日益上升。同年，法国总统马克龙（Emmanuel Macron）在索邦大学发表的演讲中首次提出“主权欧洲”，[4]2018年时任欧委会主席让·容克（Jean-Claude Juncker）宣布“欧洲主权的时刻已经到来”，[5]此后欧洲开始在国际社会不断谋求国际影响力，自主倡导国际规范和制定国际规则成为欧洲“战略自主”和建设“欧洲主权”的方式之一。成立于1847年的欧洲老牌科技企业西门子，是欧洲数字化转型企业中的领军者，较早认识到网络安全威胁的危害性。面对2017年美国微软在世界网络安全盛会RSA上提出“数字日内瓦公约”获得的巨大网络安全规范倡导影响力，以及国际社会对网络规范的迫切需求，西门子于

[1] Gorwa R. and Peez A.，“Big Tech Hits the Diplomatic Circuit Norm Entrepreneurship, Policy Advocacy, and Microsoft’s Cybersecurity Tech Accord”, in *Governing Cyberspace. Behavior, Power and Diplomacy*, Edited by Broeders D.,and Van Den Berg B., Rowman & Littlefield Publishers,2020.

[2]《巴黎倡议》提出的九项网络空间治理的原则分别为应对网络空间恶意行为、保护互联网公共核心、预防恶意网络活动破坏政治选举、反对ICT技术用于知识窃取、防止恶意ICT技术扩散、加强ICT供应链安全、提高网络清洁、降低网络冲突、促进负责任的国家行为规范等。

[3] Tech Accord, “Cybersecurity Tech Accord Submission to Australian Consultation on Responsible State Behavior in Cyberspace”, March 2, 2020, https://cybertechaccord.org/cybersecurity-tech-accord-submission-to-australian-consultation-on-responsible-state-behavior-in-cyberspace/[2023-05-21].

[4] France Diplomacy, “President Macron‘s Initiative for Europe: A Sovereign,United,Democratic Europe”, September 26, 2017, https://www.diplomatie.gouv.fr/en/french-foreign-policy/europe/president-macron-s-initiative-for-europe-a-sovereign-united-democratic-europe/[2023-10-01].

[5] European Commission, The State of the Union 2018: The Hour of European Sovereignty, September 12, 2018. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_5808/[2023-10-10].

2018年在全球安全议题领域极具影响力的慕尼黑安全会议（MSC）上作为发起方与8个产业界合作伙伴共同提出《信任宪章》（Charter of Trust），旨在拟定数字世界安全基础原则，呼吁制定网络信息安全领域的规则和标准以建立信任，[1]欲通过《信任宪章》塑造欧洲科技企业在网络空间建章立制捍卫主权的雄心。

1.倡导《信任宪章》网络安全规范

西门子主导的《信任宪章》倡议提出“保护个人和公司的数据；防止对人员、公司和基础设施造成损害；在网络数字世界中打造可靠的信任基础”三个主要目标。倡导在网络信息安全方面政府和企业必须积极开展行动的十项原则，包括网络和IT安全归属、数字供应链责任、默认安全、以用户为中心、创新与共创、教育、关键基础设施和解决方案认证、透明度和响应、监管框架以及联合倡议。[2]十项原则的落实主要面向网络安全的产业界，如呼吁企业设置特定的网络安全部门和首席信息安全官；从身份和访问管理、设备加密和系统服务升级等方面设置基准标准；建立强制性网络安全的独立第三方认证等。《信任宪章》的参与者聚焦科技产业界，空客（Airbus）、安联（Allianz）、戴尔（Dell）、IBM等8家老牌科技企业参与其中，截至2023年8月，共有15家企业签署加入。[3]从《信任宪章》倡导的规范内容到参与方，可以看出西门子作为网络规范倡导者更聚焦通过规范倡导在产业界达成保障网络安全的共识，约束和指导产业界的行为与合作。

2.打造联盟平台与政企学界保持交流

西门子借助《信任宪章》签署者的多方力量与政府部门和产业界保持交流。2019年，《信任宪章》合作伙伴与欧盟委员会代表讨论了《欧盟网络安全法》的最新进展，并提出进一步落实的方案。[4]2020年合作伙伴与法国、澳大利亚的网

[1] Charter of Trust, Siemens and Partners Sign Joint Charter on Cybersecurity, February 16, 2018, https://www.charteroftrust.com/news/siemens-and-partners-sign-joint-charter-on-cybersecurity/[2022-10-20].

[2] Charter of Trust, “信任宪章 迈向安全的数字世界”, https://assets.new.siemens.com/siemens/assets/api/uuid:94751ca88f4946d3bcd1736fad3507c7b888df33/shi-13378-cot-dok-narrative-online-chn-2018-05-08-sbi.pdf?ste_sid=a89c09ee62991c8772822c53052eab3a./[2023-10-12].

[3] 14个参与方分别为：AES, Airbus, Allianz, Atos, Bosch, Dell Technologies, Deutsche Post DHL Group, IBM, Infineon Technologies AG, Mitsubishi Heavy Industries, NTT, NXP Semiconductors, SGS, Total Energies, TÜV SÜD, Microsoft。2019年2月15日，德国联邦信息安全办公室(BSI)、西班牙CCN国家密码学中心和奥地利格拉茨科技大学作为准成员加入。

[4] Charter of Trust, “Charter of Trust Talks to Europe”, April 2, 2019, https://www.charteroftrust.com/news/charter-of-trust-talks-to-europe/[2022-11-22].

络安全政策制定者进行了直接交流。[1]2022年，《信任宪章》签署方参与了欧盟—美国贸易和技术理事会部长级会议中三个工作组的筹备工作。[2]在与产业界的交流中，《信任宪章》的签署企业通过线上线下结合的路演形式，分别主导就互联网世界中的网络安全问题进行讨论。[3]

此外，为进一步推广《信任宪章》倡议，2019年西门子启动了第一届《信任宪章》联合伙伴论坛（Associated Partner Forum），旨在为政府、研究机构和产业联盟等多主体打造交流平台，共同探讨网络空间安全问题的解决方案，截至2023年8月，共有14个伙伴参与其中。[4]具体包括加拿大网络安全中心、西班牙国家加密中心、德国联邦信息安全办公室、日本内务和通信部等6个国家政府部门，网络就绪研究所与网络和平研究所等4个研究机构，全球网络联盟和云安全联盟，以及2个高等院校。作为欧洲企业，西门子通过联合伙伴论坛与欧盟和其他欧洲国家保持联系，维持该公司在欧洲的影响力，通过与美国、澳大利亚和日本等其他国家的互动不断增强《信任宪章》的国际影响力。

（三）华为有限倡导国际规范关切产品与服务安全

创立于1987年的中国民营企业华为是全球领先的ICT基础设施和智能终端提供商，业务覆盖170多个国家和地区，为全球30多亿人口提供服务，[5]成为中国具有国际竞争力的科技企业代表。2019年开始中美关系急剧恶化，从“贸易战”到“科技战”，美国对华突出全面竞争态势。在此背景下，华为国际市场的不断拓展和以5G为代表的新兴技术领先地位，使其成为中美竞争态势下美国重点打压的科技企业。美国开始将华为视为国家安全威胁，通过颁布总统行政令、出台国家法案、推出“清洁网络”（Clean Network）计划、施压欧洲盟友国等方式，渲染华为安全威胁论、切断华为供应链、限制华为进入美国市场，对华为开展了

[1] Charter of Trust, “Charter of Trust Meets French Policy Makers”, March 3, 2020, https://www.charteroftrust.com/news/charter-of-trust-meets-french-policy-makers/[2022-11-09];Charter of Trust, “Charter of Trust statement to the Australian Government”, September 30, 2021, https://www.charteroftrust.com/news/charter-of-trust-statement-to-the-australian-government/[2022-11-09].

[2] Charter of Trust, “The Charter of Trust contributes to the EU-US Trade and Technology Council (TTC)”, May 13,2022, https://www.charteroftrust.com/news/cot-contributes-to-eu-us-ttc/[2023-10-10].

[3] Charter of Trust, “Charter of Trust to host four Roadshows in the second half of 2020”, September 4, 2020, https://www.charteroftrust.com/news/charter-of-trust-to-host-four-roadshows-in-the-second-half-of-2020/[2022-12-01].

[4] Charter of Trust Website,https://www.charteroftrust.com/about/[2023-07-21].

[5] “华为投资控股有限公司2022年年度报告”, https://www-file. huawei. com/minisite/media/annual_report/annual_report_2022_cn.pdf/[2023-09-28]。

全方位的打压。在欧美大肆渲染华为产品威胁国家安全的国际舆论下，华为通过倡导网络安全规范彰显其安全理念，呼吁产业界通过技术合作保障网络安全。然而，在欧美围追打压的境况下，华为难以如微软和西门子一般打造有影响力的网络安全国际规范，更多是跟随联合国框架下的网络安全规范进程，从保障自身产品和服务安全的技术方面倡导网络安全规范。

1.跟随参与而非主动倡导网络安全规范

在网络安全国际规范倡导进程中，华为更多采取的是参与而非引领的方式。以联合国框架下的网络规范进程为例，华为更多是跟随参与为主。2019年，华为的两名代表参与了OEWG第一次非正式会议的讨论，但并未发表相关提案和声明。[1]2020年OEWG非正式多利益攸关方网络对话中，华为西欧执行副总裁兼副网络安全官吉米·桑普森（Jeremy Thompson）在现有和新兴网络威胁讨论环节发言。[2]2020年联合国裁军研究所（UNIDIR）举办的“数字时代供应链安全”论坛上，华为欧盟公共事务高级经理马克·斯密斯（Mark Smitham）参与讨论发言。[3]2021年，华为代表参与了由瑞士联邦外交部牵头、外交基金会举办的日内瓦网络空间负责任行为对话。[4]总体而言，华为参与联合国框架下网络安全规范进程的力度有限，主要以跟随参与讨论为主，尚未独立提出较有影响力的规范倡议。

2.打造保障产品和服务安全的网络规范

为消除美国对华为产品与服务不安全的诋毁，增强华为产品与服务的信任度，华为从自身产品与服务的安全保障出发，倡导网络安全规范理念。华为在网络安全上秉持不作假设、不轻信任何人以及检查一切的三个原则。[5]为落实该理

[1]Reaching Critical Will,Statements from the Open-ended Working Group on ICTs,https://reachingcriticalwill.org/disarmament-fora/ict/oewg/statements/[2022-11-23].

[2]Informal Multistakeholder Cyber Dialogue Summary report, December, 2020, https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/Multistakeholder/OEWG+Informal+Multi-Stakeholder+Cyber+Dialogue+Summary+Report.pdf/[2022-10-26].

[3] UNIDIR Side Event, Supply Chain Security in The Digital Age, https://unidir.org/events/unidir-side-event-supply-chain-security-digital-age/[2022-10-22].

[4] Contribution to the First Substantive Session of the Open-Ended Working Group on the security of and in the use of information and communications technologies 2021-2025 (OEWG) Contribution by DiploFoundation,10 December 2021, https://documents. unoda. org/wp-content/uploads/2021/12/DiploFoundation-Contribution-to-the-OEWG-First-Substantive-Session-2021.pdf/[2022-10-01].

[5] “华为在布鲁塞尔成立网络安全透明中心”，2019年3月5日，https://www.huawei.com/cn/news/2019/3/huawei-cyber-security-transparency-centre-brussels/[2022-10-24]。

念，华为打造了布鲁塞尔“欧洲网络安全透明中心”和华为东莞“全球网络安全与隐私保护透明中心”，将安全中心定位为加强与所有利益相关者沟通和联合创新的平台，开放、透明和合作是安全中心的三个重要愿景。[1]2021年“全球网络安全与隐私保护透明中心”成立之时，来自GSMA协会、阿联酋、印度尼西亚的监管机构及英国标准协会、SUSE等机构代表出席活动并发言。可以看出，华为力图通过安全中心的建立，加强与安全专家、政府机构、客户和其他行业利益相关者的沟通和协作。

此外，华为在2021年开发者大会（Together）上，发布了网络安全与隐私保护的“四大主张”和“三大承诺”，以此共建安全可信的数字世界。“四大主张”：自上而下的组织与流程保障、制定严苛的隐私安全原则、与业界权威机构合作构建安全验证体系、向生态伙伴开放华为安全与隐私能力。“三大承诺”：用户的隐私安全在华为是作为最高优先级；未经用户允许，任何人无法访问用户数据；用户掌控自己的信息。在欧美的打压下，华为自研的鸿蒙系统快速迭代发展，这“四大主张”和“三大承诺”是华为为鸿蒙生态打造的隐私安全规范标杆。在以“求生存”为首要目标的严峻发展环境下，华为倡导网络安全规范的路径与微软和西门子截然不同，基于自身产品与服务实力倡导技术层面的网络安全规范是其构建网络空间国际秩序的主要方式。

科技企业影响网络空间秩序的有效性

科技企业规范倡导成功路径的普适性、对网络规范核心议题的参与能力以及国家地缘政治带来的挑战，将直接影响科技企业倡导网络安全规范、影响网络空间秩序的有效性。科技企业作为技术应用者，深知保障网络安全的重要性和紧迫性，微软、西门子和华为作为全球科技企业的领先者，是科技产业界网络安全规范倡导的先行者。因此对具有代表性的科技企业网络规范倡导效果的评估，将有助于对当前科技企业影响网络空间秩序的有效性作出较为客观的判断。

（一）科技企业网络规范倡导的成功路径难以普及

微软作为最早的倡导网络安全规范的科技企业，经过十年的努力，在国际社会开展了一系列较有影响力的网络安全规范倡导活动。Tech Accord规范倡导平台

[1] 华为网络安全透明中心：“致力于保护我们共享的数字未来的安全”，https://www.huawei.com/cn/trust-center/transparency/huawei-cyber-security-transparency-centre-brochure/[2022-11-12]。

几乎囊括了全球网络安全产业的龙头企业，通过参与网络规范的联合国进程、国家进程和多边进程，微软成为科技企业倡导网络规范的成功代表。作为科技企业倡导网络规范的先行者，微软的成功路径能否推广，将决定着科技企业能否作为群体行为者影响网络空间国际秩序。

微软的综合能力是规范倡导成功的关键，但难以在行业内普及。倡导规范的关键是规范扩散，微软的行业领先地位是其规范扩散的基础，“数字日内瓦公约”号召了161家科技企业联名签署，Tech Accord的参加者覆盖了北美、拉丁美洲、欧洲、亚洲和非洲地区。但行业领先者并非只具备行业号召力即可，如西门子的《信任宪章》自2018年提出至今只有14个企业签署，规范扩散能力远不如微软。微软规范倡导具有如此影响力的核心是其具备将技术创新、市场竞争和企业管理等硬实力转化为议程设置、规则制定和规范倡导等软实力的综合能力。有研究者认为，在网络安全事务中微软的这种综合能力体现为通过实施网络外交、倡导规范、制定政策、技术标准等方式塑造网络安全议题，利用企业的产品服务、商业模式、组织历史和结构、领导力等内部能力设置议程和参与国际规范制定，并通过人道主义话语技巧、服务条款、技术安排、知识和专业技能等将其议程落地。[1]微软硬实力与软实力的互促是一种综合能力的体现，但这是企业中的一种高级竞争力，难以在行业内普及。

微软丰富的规范倡导经验其他科技企业难具备。十年前微软曾以倡导规范的方式发布《Windows原则：促进竞争的十二项宗旨》，以解决微软对政府的反垄断诉讼，其高层管理者深知通过倡导规范影响国家行为的可行性。面对2013年的“棱镜门事件”，2014年微软首席执行官萨提亚·纳德拉（Satya Nadella）上任后就提出要采取一个原则性的方法解决监听问题，要求微软负责法务的总裁布拉德·史密斯（Brad Smith）带领团队制定能够应用于从操作系统到Xbox整个业务板块且简单易记的网络规范原则。[2]自此微软正式开启了史密斯领导下的微软网络安全规范进程，提出一系列有影响力的网络安全规范，并打造Tech Accord平

[1] Gorwa R. and Peez A.,“Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft’s Cybersecurity Tech Accord”,2018, https://osf.io/preprints/socarxiv/g56c9/[2023-10-10]; Hurel L. M. and Lobato L. C.,“Cyber-norms Entrepreneurship? Understanding Microsoft’s Advocacy on Cybersecurity”, in *Governing Cyberspace. Behavior, Power and Diplomacy*, Edited by Broeders D. and Van Den Berg B., Rowman & Littlefield Publishers,2020.

[2] [美]布拉德·史密斯、卡罗尔·安·布朗著，杨静娴、赵磊译：《工具还是武器》，北京：中信出版社，2020年。

台进行规范倡导的国际化运作，微软网络安全规范倡导者的身份备受国家关注。然而，对于其他科技企业而言，尚不具备如此丰富的国际规范倡导经验，从规范生产到规范传播再到规范落实，整个过程需要企业内部专业团队和外部政府资源的支持，一般的科技企业难以具备国际规范运作的能力。

微软规范倡导团队具备的资深政府关系属于稀缺性资源。作为与国家身份不对等的科技企业，倡导国际规范需要与国家政府保持密切联系。微软规范倡导的领导者史密斯凭借自身专业能力和政治资源与世界各国政要密切接触，某种意义上已经成为全球“网络安全政治家”。微软负责执法和国家安全团队的艾米·霍根伯尼（Amy Hogan-Burney）此前在联邦调查局总部的国家安全部门做过三年的律师，内特·琼斯（Nate Jones）负责公司整体合规战略、与其他科技公司的联系以及与各国政府的谈判，曾就职于美国参议院司法委员会和司法部，还在奥巴马（Barack Obama）总统的国家安全委员会负责反恐工作。在微软准备启动Tech Accord发布网络安全规范之前，微软曾向白宫和几国政府要员告知这一计划，在白宫层面获得积极反响，但美国情报界担心用词不当会有碍对网络恶意行为的打击，最终微软将规范中的不使用ICT技术攻击“普通公民”改为了“无辜公民”。[1]在美国“旋转门”机制下，微软网络安全团队的人员有着丰富的政府资源，对微软规范倡导获得国内外政府背书发挥着重要作用，但此类人才的稀缺性使得并非所有企业都能打造有影响力的规范倡导团队。

（二）科技企业较难倡导影响国家行为的网络规范

从规范落实的行为主体来看，网络安全领域的规范可以区分为两种类型：一种只能由国家行为体落实，如国家承诺不对他国进行恶意网络活动、受到网络攻击时是否进行自卫反击等，此类规范将直接影响国家行为；另一种是国家和企业都可落实，如国家或企业在发现漏洞时应及时披露等，此类规范通常间接影响国家行为。通过对微软、西门子和华为的规范倡导实践的梳理发现，科技企业倡导第一种类型的网络规范较难得到广泛支持，而倡导第二种类型的网络规范在国际社会更容易获得关注和认可。

微软倡导的获得主权国家和政府间组织认可的网络安全规范主要包括安全管理、漏洞披露、防止装置有害隐藏功能、公开共享技术信息、最佳实践案例共享、网络安全场景演练等非国家主体亦可落实的网络规范。西门子提出的《信任

[1] [美]布拉德·史密斯、卡罗尔·安·布朗著，杨静娴、赵磊译：《工具还是武器》，北京：中信出版社，2020年。

宪章》呼吁提升网络安全技术、提高用户自主性和加强网络安全企业之间的协同合作，其网络规范的落实主体也主要是产业界。华为的规范倡导则更加以企业落实为导向，以保障产品与服务的网络安全和隐私保护为先。

微软曾试图倡导影响国家在网络空间军事行为的规范，但从UNGGE进程可以看出科技企业仍难以影响网络军控这一网络安全核心议题。关于网络武器军控，微软早在2016年就明确提出各国应致力于与网络武器有关的防扩散活动（Nonproliferation Activities rRelated to Cyber Weapons）和各国应限制其参与网络攻击行动（Cyber Offensive Operations）。然而，直到2021年的UNGGE报告，才将国家应防止恶意ICT工具和技术的扩散（Prevent the Proliferation of malicious ICT Tools and Techniques）纳入其中，并且使用的是恶意ICT工具和技术而非使用具有军控含义的网络武器（Cyber Weapon）一词。这反映出关于网络空间的军控议题主权国家之间依然存在较大分歧，以微软为代表的科技企业难以对国家行为规范产生实质性的影响。

（三）科技企业规范倡导易受国家间地缘政治影响

科技竞争已经成为数字时代国家竞争力的核心，科技企业常面临着被过度安全化和政治化的困境，其规范倡导活动能够一定程度的扩散到国家主体，但也易受国家间地缘政治影响。微软Tech Accord被OEWG进程排除在外的窘境和华为在国际社会的孤立无援一定程度上都是大国间政治博弈的结果。

OEWG是对UNGGE代表性不足的弥补，给予非国家行为参与联合国框架下网络安全规范进程的机会。2019-2021年OEWG进程中微软主导的Tech Accord积极参与其中，然而OEWG 2021-2025年进程开启之时，参与国就新进程是否设立非国家行为参与的利益相关方的方式产生分歧。[1]伊朗和俄罗斯指出，利益相关方的参与方式议题正在分散OEWG的注意力，阻碍了其内部工作。[2]2022年6月30日，Tech Accord和其他几十个非政府组织参与2021-2025OEWG进程的申请被代表团政府的否决票驳回。在Tech Accord联合发起的致OEWG主席公开信中，Tech Accord联合各成员强烈表明了非政府组织被政治化的不满，认为东西方国家

[1] Digital Watch, “UN OEWG 2021-2025-Organisation of Work”,28 March 2022, https://ig.watch/event/un-oewg-2021-2025-2nd-substantive-session/oewg-2021-2025-organisation-of-work/[2023-10-10].

[2] Commentary of the Russian Federation on the Initial “Pre-draft” of the Final Report of the United Nations Opened Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. April 27, 2020, https://front. un-arm. org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zerodraft-report-eng.pdf.[2022-07-22].

以企业所在国的地理位置和文化背景，将其拉入阵营化的地缘政治斗争中。[1]UNGGE和OEWG是目前联合国框架下网络安全规范的核心进程之一，充斥着网络发达国家与网络发展中国家之间的博弈和网络空间多边治理和多方治理的治理模式之争，企业作为非国家行为体参与其中难以摆脱国家主导的政治博弈。

华为作为全球领先的ICT科技企业，本应在国际社会网络规范形成过程中发挥重要作用，但却在中美关系恶化的国际环境下成为美国政府重点打压的科技企业，使华为在国际社会面临孤立无援的困境。一方面，美国通过政府和媒体将华为塑造为会威胁国家安全的企业，使其难以拥有网络安全规范倡导者的合法性。自2018年以来美国不断宣称中国政府可以通过华为实现对其驻在国的监控，质疑华为创始人任正非个人的背景身份，以及假设华为危害国家安全的各种可能性，将华为塑造为不可信的安全威胁。[2]另一方面，美国通过联盟体系将华为排除在全球科技市场外，使其难以获得国际社会的规范倡导支持。在美国的施压下，聚集网络安全政治资源和产业资源的欧洲国家和“五眼联盟”纷纷封锁华为。规范倡导的关键是规范扩散，但由于美国政府和行业的重重打压，华为倡导的网络规范难以获得国际社会的认可和支持，使其倡导全球有影响力的网络安全规范举步维艰。

科技企业与网络空间秩序的未来

科技企业已经具备倡导网络空间国际规范的能力和动力，通过打造规范倡导平台是其未来倡导网络空间国际规范的可行路径。虽然主权国家依然是国际秩序建构的核心，但科技企业在保障网络空间有序运转中发挥着不可替代的作用。在国家间数字竞争日益激烈的背景下，科技企业倡导国际规范将会被赋予更加浓厚的地缘政治博弈色彩。未来网络空间主权国家与科技企业的协同共治才是网络空间有序发展的可行路径。

[1] Tech Accord,Industry Perspective Rejected: Cybersecurity Tech Accord Releases Joint Statement on Veto by UN Cyber Working Group. July 21, 2022, https://cybertechaccord. org/industry-perspective-rejected-cybersecurity-tech-accord-regrets-decision-by-states-to-reject-participation-in-un-open-ended-working-group-on-cybersecurity/[2022-10-21].

[2] 汪利华：《话语、实践与安全化——特朗普政府对华5G政策安全化研究》，外交学院2022年博士论文。

（一）科技企业打造平台倡导规范成为可行路径

规范周期理论曾表明规范倡导者和规范运作平台是规范兴起阶段的必备要素。[1]通过微软、西门子和华为倡导网络安全规范实践的梳理也发现，获得国际社会一定影响力的规范倡导活动都有规范倡导平台的保障。微软的“数字日内瓦公约”和“网络空间产业界负责任的行为规范”配有Tech Accord产业联盟，西门子的《信任宪章》配有联合伙伴论坛，这种打造产业联盟平台的方式将有利于增强规范倡导的合法性。聚集产业界头部科技企业能够保障规范内容的权威性，而且形成联盟使科技企业更容易获得主权国家的关注度从而参与国际网络规范核心进程。在规范扩散方面，打造产业联盟平台有助于扩大规范参与主体的多样性。通过微软和西门子的规范倡导实践可以发现，产业联盟创立初期主要是产业界的企业为主要参与者，但随着平台的不断壮大和成熟，以不同国家的政府部门、非政府组织、研究机构、非营利组织等多样化的行为体都参与其中，大大提升了规范倡导的国际影响力。因此，科技企业在参与网络空间治理的各类议题中，打造产业联盟平台更容易与主权国家互动，获得更广泛的国际影响力。

（二）科技企业参与构建有序网络空间不可或缺

虽然本文论证了科技企业作为独立行为体构建网络空间国际秩序的有限性，但并非否认其作为国际规范倡导者的价值作用，对微软、西门子和华为的深入分析旨在说明科技企业参与网络空间国际治理的可行性和必要性。面对网络空间ICT技术的军民两用性、行为主体多样性以及主体匿名性等特征，主权国家难以独自建立和维护网络空间的和平与稳定，作为拥有专业网络知识和技术的科技企业将发挥不可或缺的作用。微软、西门子、华为等在网络安全行业已经倡导了较有影响力的行业规范和标准，这对保障网络空间安全有着重要作用，技术问题最终还是需要产业界的技术解决方案。

随着全球化和数字化的进一步发展，将会产生更多需要科技企业参与的协同共治的全球性议题，如数据流动、信息内容治理、打击网络犯罪等问题都难以凭主权国家一己之力进行治理。科技企业的数据技术资源优势决定着前沿技术的发展、新技术的应用和技术应用带来的风险。技术应用场景丰富着网络空间的各种活动，在为人类带来便利、促进社会经济发展的同时，网络空间治理成为人类面

[1] [美]玛莎·芬尼摩尔 凯瑟琳·斯金克：“国际规范的动力与政治变革”，载[美]彼得·卡赞斯坦、罗伯特·基欧汉、斯蒂芬·克拉斯纳主编，秦亚青、苏长和、门洪华、魏玲 译：《世界政治理论的探索与争鸣》，上海：上海人民出版社，2018年。

临的新挑战，科技企业已然是当前数字治理的核心参与者。

（三）科技企业倡导国际规范体现国家数字竞争

2019年中美拉开的数字领域战略竞争已经成为当前国际竞争格局的新样态，不同于冷战期间国家间的意识形态竞争，本轮“科技新冷战”的主要动力是国家间数字战略竞争，科技产业竞争力、数字领域国际规则制定权和价值观的塑造权成为竞争核心。从特朗普政府的“对华技术封锁”“全面脱钩”到拜登政府的“小院高墙”“技术联盟”等对华科技遏制战略的实施，美国对中国科技产业的打压范围更广、力度更大。科技企业发展成为国家关注的重点，因此科技企业倡导国际规范的行为较易蒙上地缘政治的色彩，成为国家间数字竞争实力的体现。

国际规范的作用不仅在于塑造共同的价值理念，也希望将其理念原则上升为行为标准，成为约束国际社会成员行为的准则。因此，科技企业倡导国际规范不仅彰显着企业自身实力和国际影响力，也体现出其在数字领域的价值理念和建章立制权。微软、西门子和华为通过不同的方式参与网络安全国际规范倡导，表层展现出科技企业的国际影响力，但深层体现出的是美国、欧盟、中国三者在国际竞争大格局中科技综合实力。企业在国际社会影响力的增强将有助于企业所属国的软实力提升以及国家利益的保障，因此未来科技企业倡导国际规范将可能被赋予更加浓厚的政治博弈。

（四）多方网络规范对接构建网络空间国际秩序

当前网络空间的国际硬规则依然不足，国际规范仍然是推动网络空间秩序形成的主要方式。联合国框架下UNGGE和OEWG并行机制的不断推进展示出主权国家希望保障网络空间安全作出的努力，但也应该充分认识到主权国家规范倡导进程与非国家行为体规范倡导进程对接的重要意义，即主权国家应以更加开放包容的规范倡导态度吸纳更多的非国家行为的规范倡导成果。如今ICT软硬件产品已经成为网络黑客攻击者的重点对象，成为网络军事化进程中国家打造网络武器的广泛载体，网络安全威胁已对科技企业的切身利益产生直接影响，促使其参与网络空间规范制定约束网络空间各方行为的动力不断增强。数字时代分散了传统国家垄断的部分权力，非国家行为体的权力得到扩张，使其有更强的能力和动力参与到国际事务中。面对非国家行为体的崛起，主权国家更加需要思考的是如何与非国家行为体的治理能力对接而非对其过度防范，只有协同各方力量、汇集各方智慧才能应对人类面临的全球性挑战，维护有序的世界秩序。

（责任编辑：崔秀梅）