科技企业倡导网络空间国际规范的传播策略
——以微软网络安全国际规范实践为例

崔保国[1,2]，杨 乐[1]
（1. 清华大学新闻与传播学院，北京 100084；2. 海南大学国际传播与艺术学院，海南海口 570228）

摘 要：当前，网络空间仍处于建章立制的关键时期，具备知识和技术资源的科技企业成为规则制定的重要参与方。面对短期内网络空间“硬法”难达成的现状，国际规范成为约束网络空间各方行为的有效“软法”。近年来，科技企业积极倡导网络空间规范，进入国家主导的网络规范国际议程成为其规范倡导有效性的关键。本研究基于议程设置理论、国家社会化理论和规范周期理论，对科技企业微软的规范倡导实践进行分析。研究发现，采用导向需求型规范、标杆式说服型规范和多议程联动型规范三种倡导策略，能够使科技企业与国家倡导的规范形成互动，在国际社会有效传播。对当前科技企业在国际社会倡导网络空间国际规则成功案例的理论化，将有利于我国企业参与网络空间国际治理的实践探索，提升我国网络空间国际规则制定的综合实力。

关键词：网络空间治理；国际规范扩散；科技企业；国际传播
中图分类号：G206 **文献标识码**：A **文章编号**：2096-8418（2024）01-0009-12

习近平主席在2015年第二届世界互联网大会上首次提出构建网络空间命运共同体的世界理念，主张构建互联网治理体系要坚持多边参与、多方参与，倡导政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各个主体发挥作用。[1] 2022年发布的《携手构建网络空间命运共同体》白皮书重申网络空间是人类共同的活动空间，倡导多方参与构建网络空间国际秩序。[2] 秩序离不开规则，网络空间秩序的构建离不开网络空间治理中规则的形成。然而，当前国际社会尚未形成网络空间具有强约束力的国际规则，构建网络空间国际规范成为国际社会维护网络空间和平与稳定的重要方式。科技企业在保障互联网安全运行方面发挥着关键作用，利用开发软件和硬件产品服务、提供专业知识、制定技术标准、建立服务认证和信任机制等技术优势，逐渐成为网络空间国际规范的新兴倡导者。正如玛莎·芬尼摩尔（Martha Finnemore）所言，“政府或许不是制定网络空间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。”[3] 与此同时，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。在百年未有之国际大变局下，国家间网络空间利益越发难以协调。作为网络空间具备制定国际规范能力的潜在行为者，科技企业如何进入网络空间国际规则议题进程，增强其国际规范倡导的传播能力成为本文关注的核心问题。

需要对研究对象进一步说明的是，本研究关注的是有能力参与网络空间国际规范倡导的科技企业，并非一般意义上的科技企业。该类企业具备较强的国际影响力，通常是在生产、经营、服务等重要环节具有占据优势地位的大型跨国企业，并且其产品、服务与国际安全和经济议题强相关。另外，作为国际规范的倡导者，该类科技企业有志于塑造网络空间国际规则，活跃于国际社会的网络空间治理活动。规范倡导者是积极创造规范的行为体。根据规范周期理论，在规范兴起初期，规范倡导者以个人或组织的形式框定议题，规范普及阶段国家、国际组织和联系网络进行规范扩散，规范内化阶段则由

基金项目：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”（21BXW008）。
作者简介：崔保国，男，教授，博士生导师；杨乐，女，博士研究生。

法律界、行业界和政府机构将规范习惯化和制度化。因此，规范倡导是覆盖规范演进的全过程活动。本研究是对科技企业倡导网络空间国际规范全进程的分析，但目前网络空间国际规范大多仍处于兴起和普及阶段，因此如何框定规范议题和传播策略是本研究的重点。

一、科技企业成为网络空间规范新兴倡导者

网络空间是以互联网为代表的信息通信技术发展到高度普及阶段后出现的人类社会现象和世界新空间。科学技术的创新与应用是网络空间形成的核心根基，具备科技产品和服务研发和销售的科技企业是重要推动者。主权国家和国际组织曾是国际社会中国际规范的传统倡导者，但在国家主导的网络规范进程滞后于日益增长的网络威胁之时，掌握技术资源的科技企业作为网络空间规范新兴倡导者的能力和动力不断增强。

（一）主权国家倡导网络空间规范进程缓慢

对于规范（Norm），一个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。[4]“采取适当的行为”表明规范能对特定群体的观念和行为产生影响。因此，规范具有“实然性”和“应然性”统一的特征，既能反映某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。[5] 当前网络空间安全的威胁因素日益增多，如网络脆弱性、网络攻击肆意、网络攻击难溯源、网络空间的军事化等直接影响着国际和平与稳定。然而，网络空间不同于传统物理空间，既有国际规则体系难以直接适用其中，新的网络空间“硬法”规则难以在短期内建立。因此，达成具备“软法”性质的国际规范成为保障网络空间秩序的可行路径。美国学者约瑟夫·奈（Joseph Nye）曾认为，网络空间的不安全促使网络空间有约束作用的规范产生，规范被寄希望于约束网络冲突。[6]

面对网络空间可能面临无序的挑战，20世纪90年代，国际社会就开启了遏制网络空间恶意行为的国际规范进程，但进展缓慢。2004年成立的联合国信息安全政府专家组（Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security，简称UNGGE）是目前主权国家推进网络空间国际规范的核心进程，主要围绕网络空间国家负责任行为、网络军事化和打击网络犯罪等议题。然而，被寄予厚望的2017年组会未能形成共识性报告。在网络军事方面，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，核心议题在东西方国家中存在分歧，较难发展成为国家间普遍承认的国际法。2019年的《联合国打击网络犯罪公约》旨在达成打击网络犯罪中具有法律约束力的国际公约，但主权国家各方在术语使用、基本原则、定罪范围和国际合作等核心议题仍然未达成共识，公约进程举步维艰。[7] 数字贸易规则方面，以世界贸易组织、二十国集团和经济合作与发展组织等既有政府间组织主导推进，同时与《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，但隐私保护、网络安全、大国博弈相互交织充斥于此，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。总体而言，在网络安全与国家安全深度捆绑，网络空间规则主导权成为国家间竞争的重要领域的背景下，国家主导的网络规范进程严重受阻。

（二）科技企业具备规范倡导的能力和动力

以互联网为代表的科技创新是网络空间发展的核心动力，科技企业是技术创新的重要来源，科技企业凭借自身的技术资源、数据优势和创新能力等已逐渐具备推动网络空间国际规范的能力。约瑟夫·奈曾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，权力正在从国家行为体向非国家行为体扩散。[8] 在数字时代，谁拥有数据，谁掌握技术，谁就拥有更多的权力。数字资源竞争成为国家间竞争的核心，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。[9] 目前，科技企业已然成为数字资源的掌控者，以ICT科技企业、社交媒体平台和电子商务巨头为代表的科技企业其产品和用户遍布全

球，一家企业的产品技术规则可以全球应用。在技术和知识资源能力上，科技企业不断提高其研发能力增强产品竞争力，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。在占据数据资源、技术创新和广阔市场的优势下，科技企业的权力渗透至政治、社会、军事和经济等诸多领域。

网络安全威胁与科技企业自身利益密切相关，科技企业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。2017 年，微软参照《日内瓦公约》，发起《数字日内瓦公约》。2018 年，西门子发布《数字信任宪章》，呼吁产业界建立信任。2019 年，联合国开展的与 UNGGE 进程双轨并行的开放式工作小组（Open-Ended Working Group，简称 OEWG），囊括了微软、西门子、赛门铁克、卡巴斯基、腾讯和华为等科技企业。[10] 在“没有网络安全，就没有国家安全”的战略指导下，网络安全国际规范成为国家和非国家行为体共同关注的网络空间规则建立核心方式。与网络安全相关的科技企业凭借专业知识和技术资源优势，在网络安全国际规范倡导进程中发挥着日益增强的影响力。其倡导议题不断与主权国家规范进程互动，以微软为代表的科技企业成为网络安全国际规范倡导的典范。

二、微软倡导网络安全国际规范的实践

成立于 1975 年的科技公司微软是世界上最大的软件制造商之一，在信息化浪潮中不断拓宽网络空间的应用场景，其产品和服务已经对现实社会产生深刻影响。然而，2013 年的“斯诺登事件”揭秘了包括微软在内的 9 家美国科技巨头企业加入美国国家安全局的“棱镜”计划，允许国家安全局能够直接访问其用户个人信息和其他数据。[11] 一时间，微软陷入巨大的用户信任风波，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。自 2013 年开始，微软为恢复公司信誉、增强用户信任和降低国家间政治博弈对其经营的影响，作为网络空间规范倡导者积极推动网络安全规范已近十载。

（一）倡导平台自主建立网络安全规范

“斯诺登事件”后，微软于同年提出《制定网络安全规范的五项原则》网络安全规范，呼吁各界在网络安全问题上协同共治。[12] 2014 年，微软内部组建专门团队开始打造网络空间的规范与原则。[13] 从 2013 年至今，微软共发布 8 份网络安全国际规范（如表 1 所示）。2014 年的《国际网络安全规范——减少网络世界的冲突》报告，针对国家行为提出了 6 项减少网络冲突的具体规范。[14] 微软领导网络规范倡导的总裁布拉德·史密斯（Brad Smith）还发布了《政府与网络威胁：规范的必要性》文章，构建了行动者、合法性、行动和影响的四维分析框架，用于指导政府应对网络威胁。[15] 2016 年，微软发布《从表述到实施：推动网络安全规范进程》报告，在提出政府应对网络威胁分析框架的基础上，将全球主要的网络安全规范进程分为防御性规范、进攻性规范和产业规范，并从企业侧提出了 6 项如何应对网络安全攻击的原则倡议。[16] 2017 年 3 月，史密斯在世界网络安全盛会 RSA 上提出“数字日内瓦公约”的倡议，呼吁如 1949 年各国政府承诺在战争时期保护平民一样，政府需要在和平时期保护互联网平民，呼吁各国政府放弃对企业的网络攻击。[17] 演讲中，史密斯还呼吁产业界的科技公司成为网络空间的中立“数字瑞士”，提出了数字日内瓦公约的 10 项基本规范。2018 年发布的国际网络安全规范政策文件，提出在全球网络安全产业界建立私营企业在网络空间负责任的行为规范①，奠定了微软网络安全规范的核心原则，此后的网络规范发展基本都是对其的进一步发展。

① 四项规范具体内容为：承诺保护我们所有的客户和世界各地的客户，承诺反对从任何地方发起对无辜公民和企业进行的网络攻击，承诺将帮助用户、客户和开发者加强网络安全保护的能力，以及承诺将相互合作并与志同道合的团体合作加强网络安全。

表 1 微软倡导的网络安全国际规范

微软公司	《制定网络安全规范的五项原则》（*Five Principles for Shaping Cybersecurity Norms*）	2013 年
	《国际网络安全规范——减少网络世界的冲突》（*International Cybersecurity Norms——Reducing conflict in an Internet-dependent world*）	2014 年
	《政府与网络威胁：规范的必要性》（*Governments and APTs: The Need for Norms*）	2014 年
	《从表述到实施：推动网络安全规范进程》（*From Articulation to Implementation: Enabling progress on cybersecurity norms*）	2016 年
	《巴黎倡议：为了网络空间的信任与安全》（*Paris call for trust and security in cyberspace*）	2017 年
	微软总裁 RSA 主旨演讲（*The Need for a Digital Geneva Convention*）	2017 年
	《数字日内瓦公约》（*Digital Geneva Convention*）	2017 年
	《国际网络安全规范——微软政策文件》（*International Cybersecurity Norms——Microsoft Policy Papers*）	2018 年

通过近五年在构建网络安全规范的投入后，微软在 2018 年 4 月联合 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广和运作规范倡议。在微软的倡导下，Tech Accord 的签署成员快速增长，截至 2023 年 8 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（如图 1 所示）。作为倡导保障网络安全的产业联盟，Tech Accord 纳入了网络安全、IT 企业和云数据安全领域的诸多核心企业。160 多家企业的加入有效增强了 Tech Accord 其作为网络安全规范倡导者的合法性，也增强了其代表性，使其能够获得主权国家的关注，并被给予准国家主体的协商谈判地位。

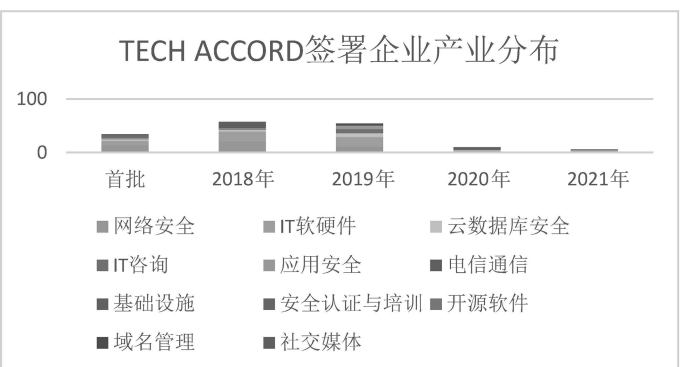

图 1 Tech Accord 网络安全产业联盟签署企业的行业分布

Tech Accord 的影响力不仅体现在签署成员的产业领域多样化，也体现在签署成员的国际化。在 Tech Accod 的 161 家签署企业中，总部位于美国的企业最多。但除美国之外，也涵盖了 23 个非美国本土企业，包括了北美、拉丁美洲、欧洲、亚洲和非洲地区。电信运营商维护着各国互联网的关键信息基础设施资源。Tech Accord 获得了 8 个国家电信巨头企业的签署，分别是美国的 Telelink、英国的 BT、法国的 Orange、日本的 NTT、荷兰的 Kpn、瑞士的 Swisscom、意大利的 Telecom Italia、智利的 Entel。国际化的签署成员、关键行业的企业签署，使 Tech Accord 扩散到了全球的产业界。

（二）对接主权国家主导的核心网络规范进程

主权国家仍然是国际规范的主要倡导者。微软通过倡导主权国家关注的网络安全规范核心议题增强其规范影响力。UNGGE 是当前主权国家主导的网络安全国际规范的主要进程，讨论对国家使用 ICT

技术所适用的有约束力和无约束力的行为规范，涵盖面从现行国际法在信通技术环境中的适用到国家在网络空间的责任和义务，问题涉及关键基础设施保护、网络安全事件防范、信任和能力建设以及人权保护等。议题经讨论后，由区域、次区域、双边、多边或专门机构进行运作和实践。截至目前，UNGGE 共发布 4 份共识性组会报告。2019 年开启的 OEWG 与 UNGGE 并行，其进程的主要议题与 UNGGE 相似，于 2021 年初发布 1 份组会报告。

本研究对 UNGGE 和 OEWG 发布的 5 份共识性报告和微软发布的与网络规范相关的 8 份报告作文本比较分析后发现，微软倡导的网络安全国际规范与 UNGGE 和 OEWG 倡导的网络规范在负责任的国家行为规范议题中有较多重合。对 13 项文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。研究发现，在 UNGGE 和微软重合关注的 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、共享技术信息类型和国际合作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 2）。9 项微软和 UNGGE 重合规范议题表明微软与国家主导的网络安全规范已经展示出一定程度的对接现象，6 项微软先于 UNGGE 提出来的规范虽然不能证明微软直接设置 UNGGE 的议程，但可以间接说明微软的网络安全规范倡导活动可能已经引起了主权国家的注意并获得了一定程度上的采纳。

表 2　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	政府专家组提出时间	议题主题	导向需求策略
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	相关性+不确定性策略
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的做法，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	相关性策略
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	相关性+不确定性策略
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	相关性+不确定性策略
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	相关性策略

续表

序号	议题内容	微软提出时间	政府专家组提出时间	议题主题	导向需求策略
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	相关性+不确定性策略

（三）联动国际网络规范的多边进程

微软不仅积极参与主权国家主导的联合国框架下的网络规范进程，也积极利用网络空间多利益攸关方模式多线程参与网络空间治理进程，将自身倡导的网络安全规范与单个主权国家主导、政府间组织主导以及非政府组织主导的规范进行多领域互动，推进其规范扩散。具体互动进程如图 2 所示。

图 2 微软和 Tech Accord 平台与网络空间国际规范进程的互动

微软与政府间网络规范进程的互动。微软与其主导的 Tech Accord 产业联盟积极参与 UNGGE 和 OEWG 开设的非国家行为体的咨商会议，发布对 UNGGE 和 OEWG 的立场声明，将网络空间负责任的国家行为规范与微软和 Tech Accord 倡导的网络规范相勾连，不断强调禁止政府支持的网络攻击，加强对关键基础设施、ICT 企业和无辜公民的保护。在联合国高级别数字合作小组进程中，Tech Accord 将自身打造为效仿者，引导高级别小组关注的议题向 Tech Accord 靠拢。运行模式也遵循 Tech Accord 倡导的多利益相关方模式，强调私营企业参与治理的不可或缺性。在区域性政府组织中，Tech Accord 与 OECD 的数字经济安全工作组频繁互动，通过为工作组提供报告咨询意见的方式，将自身倡导的网络安全规范融入其中。

微软与主权国家主导的网络安全规范进程互动。通过与法国高层的互动，微软非正式地参与草拟了《巴黎倡议》。《巴黎倡议》提出 9 项网络空间治理原则①。截至 2022 年 11 月，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。2020 年 11 月，法国的欧洲和外交事务部宣布成立六个工作组，促进落实《巴黎倡议》提出的网络空间原则。其中，Tech Accord 成为第三工作组——在联合国网络谈判中促进多方利益攸关方——的联席主席。此外，Tech Accord 加入了美国漏洞权益进程（US Vulnerability Equities Process），该进程旨在为各国如何处理网络安全漏洞

① 《巴黎倡议》提出的 9 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。

方面提出一个决策框架。在与该进程的互动中，Tech Accord 围绕其提出的防御性 ICT 技术和进攻性 ICT 技术概念，提出了一系列政府携手应对网络漏洞的技术性建议。

微软与非政府组织倡导的网络安全规范进程互动。在由专家学者搭建的全球网络安全专家论坛（Global Forum on Cybersecurity Expertise，GFCE）中，Tech Accord 的两个签署成员微软和思科已经作为 GFCE 的工作做出了贡献。微软作为网络安全规范的倡导者代表，还参加了 2016 年由海牙战略研究中心及东西方研究所共同发起的全球网络稳定委员会进程（GCSG），委员会委员囊括了中国、美国、俄罗斯等多国负责网络事务的政要，以及网络规范研究的资深学者、IT 企业巨头和知名智库等。2018 年，Tech Accord 背书由互联网协会管理网络运营商在 2014 年发起的路由安全规范 MANRS，目前该倡议有 880 家签署方，旨在提高互联网全球路由系统的弹性和安全性。[18] 2019 年 3 月，Tech Accord 表态声明支持英国政府提出的《消费物联网安全实践守则》（Code of Practice for consumer IoT security）。该守则现已被欧洲电信标准协会（ETSI）采纳为技术规范，为互联网连接的消费产品建立安全基准，为欧洲物联网认证计划提供基础。2022 年，Tech Accord 与 Consumers International、I Am the Cavalry 两个机构发布联合声明，达成物联网安全优先事项的全球共识，提升物联网安全的重要性。[19]

微软作为 ICT 产业的领军企业，面对网络空间中的新型安全威胁，自 2013 开始倡导网络安全国际规范，已近十载。凭借强大的企业综合实力和丰富的国际事务参与经验，微软已经形成了以“数字日内瓦公约”和 Tech Accord 产业联盟为代表的一系列具有国际影响力的国际规范和规范倡导平台。作为非国家行为体，科技企业如何以不同的身份和资源与国家进行互动，进入网络空间国际规范的主流进程，微软的网络空间国际规范倡导实践值得深入研究。接下来将以微软实践为基础结合国际规范周期、议程设置和社会化理论，从国际规范内容和传播策略两方面探寻怎样的国际规范内容更利于传播，以及采取怎样的倡导策略更利于规范扩散。

三、科技企业倡导网络国际规范的传播策略

微软与单个主权国家主导、政府间组织主导以及非政府组织主导的网络安全国际规范的多进程互动已近十载。不论是规范倡导的数量或规范影响力，微软在科技企业倡导规范的进程中都位居前列。对微软网络规范倡导实践的理论化挖掘有利于提炼出科技企业普适性的规范倡导策略，对我国科技企业倡导国际规范大有裨益。

（一）塑造导向需求的网络安全国际规范

随着网络空间威胁的加剧，2017 年后网络空间国际规范愈发增多，但并非所有的规范议程都引起了主权国家的关注和接受。美国传播学学者大卫·韦弗（David Weaver）的导向需求理论从规范议程属性（内容）方面解释规范议程受关注度不均的现象。[20] 其中，相关性（relevance）和不确定性（uncertainty）是导向需求的两个子概念，相关性是议题内容与受众利益的关系，不确定性代表受众对该议题领域缺乏掌控力，缺乏了解难以控制议题的影响后果。导向需求理论认为相关性低意味着导向需求低，相关性高与不确定感低导致中等导向需求，相关性高与不确定感高则导致高导向需求。也就是说，具备高相关性和高不确定性属性的议题更容易受到关注和接受。

在微软对接国家主导的 UNGGE 和 OEWG 进程中，微软提出的受到主权国家关注的规范明显满足与主权国家利益高相关性以及主权国家对该议题高不确定性的导向需求。在表 2 所反映的微软先于 UNGGE 和 OEWG 提出的网络安全国际规范议题中，呼吁“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”“促进国际合作与私营企业合作控制网络武器扩散”6 项议题与国家安全直接相关。网络攻击的匿名性、技术多样性及其带来的损失严重性等特点使网络空间充满高度不确定性，而主权国家保障网络空间稳定的有

效途径之一是消除其不确定性。在微软提出的网络安全国际倡议中，“避免国家使用ICT技术威胁国际和平”“禁止开发或扩散有害隐藏功能”“保障网络武器不扩散”“国际合作、与私营企业合作控制网络武器扩散”4项网络安全规范体现出其对减少网络空间不确定性的努力。

网络空间的安全治理充斥着大量的高相关性和高不确定性议题，为科技企业倡导网络国际规范议题创造了机会。科技发展塑造的新型国家能力、国家新安全观的形成以及网络空间对社会全方位的影响，使科技企业倡导的网络安全规范与主权国家的国家能力、国家安全以及经济发展和社会稳定存在者高关联性。网络空间的匿名性、行为主体多样化、对现实世界影响范围与程度的广泛性使主权国家对网络空间充斥着大量的不确定性。造成网络空间不安全的行为者包括黑客、有组织的犯罪集团、国家政府等多主体，但互联网技术的匿名性使追溯网络行为的负责人面临现实困境。溯源难是主权国家面临的关于网络空间的首要不确定性难题。网络空间的安全风险泛在的现象使主权国家面临巨大的不确定性，但作为具备网络安全能力的非国家行为体，可以通过专业知识和技术的资源来减少国家在网络空间的不确定性。因此，主权国家的网络空间国际规范议题天然具有高不确定性和高相关性的特征，科技企业若能满足主权国家的规范议题需求，则更利于其国际规范的传播。

（二）自主倡导标杆型规范激发模仿效应

国际规范是国际社会成员通过互动形成的国家认可、接受的国际社会期望的思维方式和行动方式。[21] 传统的国际规范接受过程被视为国家社会化的方式之一。社会化是指新晋者与有组织的社会互动从而融入社会的过程，它依赖于社会关系、身份建构和社会价值与期望的认同。在国家社会化过程中，加拿大学者江忆恩（Alastair Lain Johnston）将说服（persuasion）、模仿（mimicking）和社会影响（social influence）视为社会化微观过程中的三种典型方式。[22] 在规范周期理论中，玛莎·芬妮莫尔（Martha Finnemore）强调在规范兴起阶段，说服是主要机制，并且认为说服关键国家能快速促进大部分相关国家接受规范。[23] 模仿作为较低程度的另一种社会化方式，源于新手对制度的程序、惯例和互动语言的不熟悉。说服和模仿体现出行为体主体被动和主动社会化的两种方式，是激发行为体与其他行为体发生互动的内在动力核心。

在微软规范倡导的实践中发现，微软通过自主倡导系列网络安全国际规范和形成较为成熟的规范倡导平台后，开始将其网络安全规范内容和Tech Accord运作模式作为标杆劝服主权国家，促进主权国家对其网络安全规范的认可和采纳。在2018年联合国秘书长古特雷斯召集成立联合国高级别数字经济工作组的进程中，Tech Accord从技术行业视角，通过自身的产业联盟经验，向高级别工作组运作提出意见。意见书中Tech Accord强调了多利益攸关方参与的有效模式，认为高级别小组制定的原则规范与其有相似之处，建议工作组参照Tech Accord与其他组织开展的多维合作模式。[24] 2020年1月，Tech Accord向经济合作与发展组织（OECD）数字经济安全工作组的《加强数字产品安全》（*Enhancing the Digital Security of Products*）报告提交了建议书。[25] 2019年4月，在美洲国家组织（Organization of American States，OAS）建立网络空间信任措施的进程中，Tech Accord向OAS提交了9项具体建议来促进该倡议的落实。[26] 澳大利亚作为第六届UNGGE的参与国家之一，其外交和贸易部曾邀请Tech Accord向其参与的UNGGE和OEWG进程中的负责任国家行为议题提咨询意见。[27] 在微软与主权国家倡导的网络安全国际规范互动中，微软以网络规范熟练者的身份，基于自身网络安全规范倡导的经验，给予意见指导。

当前，网络空间依然被认为是欠规制空间，[28] 其制度、惯例和互动语言尚处于形成阶段，主权国家和科技企业都是该领域的规范制定新手。因此，科技企业将更有可能对主权国家进行说服并激发其模仿动力。一方面，网络空间科技企业与主权国家之间具有较为平等的治理地位，有利于其说服战略。相较于传统治理领域，主权国家占据较强的主导性。但网络空间治理以多利益攸关方治理模式主导，

国际社会已经形成主权国家、技术社群、私营企业、社会团体共同参与网络空间治理的共识。[29] 另一方面，主权国家和科技强企业在网络空间同属于新人的身份，让科技企业有望成为被模仿者。科技企业若能提出内容质量高、传播范围广的网络空间国际规范，就能以熟练者身份成为主权国家学习的对象，激发主权国家的模仿动力，增大主权国家接受其倡导的规范的可能性。

（三）构建多议程联动的网络式规范传播

如上文所述，微软成功地将自身倡导的网络安全规范与主权国家主导、政府间组织主导以及非政府组织主导的规范进行多领域互动推进其规范扩散。这种多议程联动的网络式规范传播成为科技企业倡导规范的有效渠道。自 2017 年以来，以国际政府组织、技术标准组织、国际机构和全球性专家论坛等开启了多进程的网络规范治理。在众多的网络规范发展过程中，有学者观察到网络空间规范已经形成了一套松散耦合的制度。各进程之间可以相互互补而非完全零和博弈，且认为网络规范专家是联结各进程的关键。[30] 新规范的倡导若能与既有议程进行关联互动，则将更有利于规范倡导的传播。在说服战略与国际规范传播研究中，也有学者曾提出支持性规范联系策略，认为规范倡导者通过构建与已被广泛采纳的规范和该规范观念之间的联系，可增强新规范的合法性，从而推动更多行为体接受该规范。[31] 有学者在跨国倡议网络研究中也发现，倡导者提出的问题若能符合已有的观念和意识形态，则问题更易引起人们的关注。[32] 芬妮摩尔在规范扩散研究中也提出“相互加强和一致的规范将相互巩固”，认为在规范倡导过程中，将新规范与既有规范相联系，新规范将更容易被传播。[33] 理查德·普赖斯（Richard Price）指出“新观念如果与特定历史环境下的既存话语衔接得较好，那么新观念就能获得更大的影响”[34]。

另外，多议程联动式的规范传播将有利于形成一种网络空间国际规范的网络，制定议程设置网络。传播学议程设置理论的第三层级网络议程设置模式揭示了媒体议程和公众议程之间的网络议程存在显著性，表明不同议程的“捆绑”能对受众认知产生更为全面的影响。[35] 网络空间议题的多样性和相互之间的关联性使网络式议程联动成为可能。总体而言，科技企业倡导国际规范若能与既有网络空间规范进程相关联，形成网络式的国际规范议程设置，则将增强其规范倡导的关注度和接受度。

四、我国科技企业倡导国际规范的思考与启示

微软的网络规范倡导经验与规范周期、议程设置和社会化理论的结合表明，科技企业通过塑造导向需求的规范、打造自主型标杆规范和构建多议程联动规范，能够更好地促进规范在国际层面的传播。这为我国科技企业倡导网络空间规范提供了参考。虽然我国科技企业的科技创新力和市场竞争力不断增强，但仍需在国际社会参与网络空间国际规则制定进程中发挥更大影响力。自主倡导导向需求的规范内容、打造产业联盟推广规范以及参与网络空间治理多边进程，成为我国科技企业可以尝试的实践参考。

（一）自主倡导导向需求型网络空间规范

倡导网络规范的核心是规范内容。我国科技企业可以凭借自身的强专业性，打造导向需求型规范，迎合主权国家的专业性需求。科技企业是探索技术、应用技术的前沿阵地，掌握着科技创新和发展的核心人力物力资源。网络空间治理中，私营企业参与治理已经成为共识。微软的规范倡导案例也表明，科技企业依托自身技术优势自主倡导网络规范能够引起国际社会的广泛关注。我国以腾讯、字节跳动、阿里巴巴、拼多多、美团、滴滴等为代表的互联网企业，和以华为、中兴、科大讯飞、大疆和 360 安全为代表的 ICT 企业，已经具备领先的技术能力、丰富的产品应用以及务实的技术治理方案。可凭借其技术专业性积极自主倡导网络空间的国际规范，提升企业国际影响力。

在规范倡导内容方面，我国科技企业应该关注国际社会对网络规范的现实需求。紧贴“相关性”

和“不确定性”两大规范议题属性，围绕数据治理、网络安全、信息治理、网络犯罪等重要议题自主倡导网络规范。我国科技企业目前处于倡导国际规范的初步阶段，应当立足自身业务，从技术领域出发倡导普适性的网络空间多方行为规范。从规范落实的行为主体来看，当前网络安全领域的规范可以区分为两种类型：一种类型的规范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。另一类型的规范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漏洞等。此类规范通常间接影响国家行为。我国科技企业现阶段可以重点倡导国家和企业都可落实的规范，使规范具有更强的务实性，先从行业层面达成共识，进而影响国家行为。

（二）打造产业联盟建立规范倡导平台

建立规范倡导平台是倡导国际规范的核心要素之一，科技企业倡导国际规范若能依托产业联盟，将更有利于其建立专业性、合法性和影响力。微软凭借 Tech Accord 规范倡导平台囊括了全球顶尖的科技企业，为其规范倡导活动起到极大的背书作用。在我国互联网产业迅速发展过程中，科技行业已形成了具有一定规模的产业联盟。如 2015 年成立的中国网络安全产业联盟、2016 年成立的工业互联网产业联盟、2018 年华为成立的服务产业联盟、2022 年腾讯成立腾讯云出海生态联盟等。既有的产业联盟形成了较为成熟的运作机制，我国科技企业可基于此统筹资源，开展网络规范倡导活动，通过本地化的行业同盟形成具有行业属性的网络规范向国际社会推广。

同时，随着我国科技企业全球竞争力和国际化能力的增强，也可以打造全球化的产业联盟，依托联盟成员的多样化和国际化来倡导国际网络规范。具有国际领先地位的科技企业应该充分利用其国际影响力，搭建国际化的规范倡导平台。一方面有利于将国内规范国际化，另一方面将直接输出具有国际影响力的国际规范。目前，在中国、美国和欧盟等大国竞相争夺网络空间规则制定权的背景下，我国科技企业可以以东南亚和中东地区的科技企业作为产业联盟发展对象，依托国家间的政治稳定关系，达成规范倡导合作。

（三）参与网络空间国际规范多边进程

网络空间治理是多边和多方进程并行的治理。自 2003 年联合国 WSIS 将互联网治理正式提出之后，主权国家、私营部门、技术社群和个人组织等都以不同的形式参与到互联网治理中。当前，网络空间治理的议题多样性和治理主体多样性开创了多平台的网络空间治理进程。我国的科技企业腾讯、360 安全、华为等，曾经多次参与过联合国框架下的网络空间进程，如联合国信息安全专家组（UNGGE）的多边会议和打击网络犯罪专家组（IEG）的多边会议等。但参与力度有限，尚未提出有代表性的提案和规范。随着数字治理议题重要性的提升，网络空间的多边规范进程将更加活跃。我国科技企业可以充分利用既有平台多线程参与治理活动，倡导自主性网络规范。

目前，在网络空间规范治理进程中，主要平台包括政府间的治理进程，如联合国框架下的 IGF、UNGGE、OEWG、IEG、数字经济高级别领导小组等，国家间的国际组织如 G20、APEC、OECD 等，以及非国家行为建立的全球网络空间委员会（GCSC）、网络空间信任与安全巴黎倡议等。这些进程基本都面向私营企业开放了参与渠道，我国科技企业可以密切关注其发展动态并积极参与其中。此外，我国科技企业也可以利用我国主导的世界互联网大会治理进程。自 2014 年首届世界互联网大会召开以来，世界互联网大会进程已运行近十载。2022 年 7 月，该进程正式设立世界互联网大会国际组织。目前已有来自六大洲近 20 个国家的百家互联网领域的机构、组织、企业及个人加入其中。世界互联网大会进程是我国主导的核心网络空间治理进程，在议程设置和组织运营等方面有着主导性。我国科技企业应该充分利用世界互联网大会国际组织这一平台倡导国际规范，参与既有的网络空间国际规范进程，探索多议程联动的规范传播方式，促进我国科技企业规范倡导的实质性影响力。

五、结　语

网络空间治理议题的激增为科技企业参与网络空间治理带来了更多的机会，企业凭借自身的专业性资源可以参与更多的国际网络治理活动。在各主权国家竞相于网络空间谋求规则制定权之时，科技企业在国际社会倡导有影响力的网络国际规范，成为国家国际实力提升和国际话语权争夺的有效方式。目前，以微软为代表的科技企业已经探索出一条企业在国际社会倡导网络规范的有效路径。我国科技企业应该借鉴其实践经验，结合自身情况，倡导有国际影响力的国际规范。这不仅有利于保障企业自身利益，也有利于提升我国网络空间规则制定的话语权。

参考文献：

[1] 新华社. 习近平在第二届世界互联网大会开幕式上的讲话（全文）[EB/OL]. http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm.

[2] 新华社. 携手构建网络空间命运共同体 [EB/OL]. https://www.gov.cn/zhengce/2022-11/07/content_5725117.htm.

[3] Martha, F. Cultivating. international cyber norms, America's cyber future: Security and prosperity in the information age. Retrieved June 15, 2011, from https://citizenlab.ca/cybernorms2011/cultivating.pdf.

[4] [美] 罗纳德·吉普森，[美] 亚历山大·温特，[美] 彼得·卡赞斯坦. 规范、认同和国家安全文化 [A]. [美] 彼得·卡赞斯坦. 国家安全的文化：世界政治中的规范与认同 [M]. 宋伟，刘铁娃，译. 北京：北京大学出版社，2009：56.

[5] 曹玮. 国际关系理论教程 [M]. 北京：中国社会科学出版社，2020：218-220.

[6] Nye, J. S. Normative restraints on cyber conflict. Cyber Security Project. Harvard Kennedy School Belfer Center for Science and International Affairs Retrieved. Augest 1, 2018, from https://www.belfercenter.org/sites/default/files/files/publication/Nye%20Normative%20Restraints%20Final.pdf.

[7] 姜博谦，王渊结. 2022 年度联合国打击网络犯罪公约谈判进展 [J]. 中国信息安全，2023（1）：70-72.

[8] [美] 约瑟夫·奈. 权力大未来 [M]. 王吉美，译. 北京：中信出版社，2012：160-176.

[9] 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 [J]，外交评论，2022（2）：110-132.

[10] 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 [J]，中国信息安全，2022（12）：53-56.

[11] Greenwald, G. & MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others. Retrieved June 7, 2013, from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[12] Microsoft. Five principles for shaping cybersecurity norms. Retrieved March 13, 2013, from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc9.

[13] [美] 布拉德·史密斯，[美] 卡罗尔·安·布朗. 工具，还是武器？[M]，杨静娴，赵磊，译. 北京：中信出版社，2020：21-25.

[14] Microsoft. International Cybersecurity Norms——Reducing Conflict in an Internet-Dependent World. December 15, 2014. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA.

[15] Microsoft. Governments and APTs: The need for norms. Retrieved September 1, 2015. from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtU.

[16] Mcrosoft. From articulation to implementation: Enabling progress on cybersecurity norms. Retrieved June 24, 2016. from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

[17] Smith, B. The Need for a Digital Geneva Convention. Transcript of Keynote Address at the RSA Conference. February 14, 2017. p. 10. Retrieved from https://blogs.microsoft.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

[18] Tech, A. Cybersecurity Tech Accord endorses the MANRS initiative, joining efforts to eliminate the most common threats to the Internet's routing system. Retrieved August 9, 2018. from https://cybertechaccord.org/cybersecurity-tech-accord-endorses-manrs.

[19] Tech, A. Securing the next generation of connected consumer products. Retrieved February 15, 2022. from https://cybertechaccord.org/securing-the-next-generation-of-connected-consumer-products.

[20] Weaver, H. (1980). Audience need for orientation and media effects. *Communication Research*, 7 (3): 361-373.

[21] 钟龙彪. 国家社会化：国际关系的一项研究议程［J］，欧洲研究，2009（2）：125-137.

[22] Johnston，A. I.（2008）. Social states：China in international institutions，New Jersey，Princeton University Press.

[23] ［美］玛莎·芬尼摩尔，［美］凯瑟琳·斯金克. 国际规范的动力与政治变革［A］.［美］彼得·卡赞斯坦，［美］罗伯特·基欧汉，［美］斯蒂芬·克. 世界政治理论的探索与争鸣［M］.［美］. 秦亚清，等译，上海：上海人民出版社，2018：203-205.

[24] Tech，A. Cybersecurity Tech Accord submission to the UN High Level Panel on Digital Cooperation. Retrieved December 21，2018. from https：//cybertechaccord. org/uploads/prod/2018/12/Tech-Accord-HLP-Response-Dec-2018. pdf.

[25] Tech，A. Cybersecurity Tech Accord letter to OECD scoping paper on digital security of products. Retrieved January 10 ，2020. from https：//cybertechaccord. org/cybersecurity-tech-accord-letter-to-oecd-scoping-paper-on-security-of-digital-products.

[26] Tech ，A. Reducing tensions in cyberspace by promoting cooperation：Cybersecurity Tech Accord publishes a set of recommendations on confidence-building measures in cyberspace. Retrieved April 4 ，2019. from https：//cybertechaccord. org/reducing-tensions-in-cyberspace-by-promoting-cooperation-cybersecurity-tech-accord-publishes-a-set-of-recommendations-on-confidence-building-measures-in-cyberspace.

[27] Tech，A. Cybersecurity Tech Accord submission to Australian consultation on responsible state behavior in cyberspace. Retrieved March 2 ，2020. from https：//cybertechaccord. org/cybersecurity-tech-accord-submission-to-australian-consultation-on-responsible-state-behavior-in-cyberspace.

[28] Anja，P. J. & Klaus D. W.（Eds. ）（2013）. Transnational Governance of Violence and Crime. London，Palgrave Macmillan，London. ：129-148. Jeutner，V.（2019）. The digital geneva convention：A critical appraisal of Microsoft's proposal. Journal of International Humanitarian Legal Studies . 2019（10）：158-170. Available at SSRN：https：//ssrn. com/abstract=3402565.

[29] 鲁传颖. 网络空间治理与多利益攸关方理论［M］. 北京：时事出版社，2016：199.

[30] Christian，R. ，Duncan，H. ，Wyatt，H. & Tim，M.（2020）：Cyberspace and Geopolitics：Assessing Global Cybersecurity Norm Processes at a Crossroads，Carnegie Endowment for International Peace，February，2020. Retrieved from https：//carnegieendowment. org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

[31] 黄超. 说服战略与国际规范传播［J］. 世界经济与政治，2010（9）：72-87.

[32] ［美］玛格丽特·凯克，［美］凯瑟琳·辛金克. 超越国界的活动家：国际政治中的倡议网络［M］. 韩召颖，孙英丽，译. 北京：北京大学出版社，2005：100.

[33] Martha，F.（2003）. *The purpose of intervention*：*Changing beliefs about the use of force*，London：Cornel University Press.

[34] Richard，P.（1998）. Reversing the gun sights：transnational civil society targets land mines，*International Organization*，52（3）：613-644.

[35] Guo，L. & Chris，V.（2015）. The power of message networks：A Big-data analysis of the network agenda setting model and issue ownership. *Mass Communication and Society*，18（5）：557-576. Vu，T. ，Lei ，G. & Maxwell，M.（2014）. Exploring "the world outside and the pictures in our heads" a network agenda-setting study. *Journalism & Mass Communication Quarterly*，91（4）：669-686.

［责任编辑：高辛凡］