

Doi: 10.20063/j.cnki.CN37-1452/C.2026.02.001

“规范性力量”的现实主义化:欧盟数字外交的转型

李佳兴

陕西师范大学 国家安全学院,西安 710119

摘要:《欧盟国际数字战略》的出台标志着欧盟在数字领域的战略布局进入新阶段。在全球数字竞争加剧后,欧盟在数字外交领域不再一味追求“规范性力量”,转而注重构建具有现实主义特征的数字外交体系。这种新态势与多方面因素密切相关,包括欧盟“规范性力量”无法适应复杂的数字地缘政治环境、科技公司的崛起对欧盟数字外交的冲击以及全球数字安全治理复杂性显著提升等。为适应当前全球数字竞争格局,欧盟强化数字传播建设,提升全球战略叙事能力;推动数字经济合作,维持市场竞争力;扩大国际伙伴关系网络,增强全球领导力;强化新型数字基础设施合作,构筑安全环境。诚然,欧盟数字转型也面临内部“隔阂”制约数字外交、外部存在“阻力”制约数字外交的认可度、数字安全能力“滞后”等限制。着眼未来,欧盟将加速推动数字外交朝着体系化与地缘化方向发展,着力提升数字话语权构建水平,推进技术自主与经济安全“双轮驱动”。

关键词: 欧盟数字外交;数字战略转型;数字主权;全球领导力;数字规范

中图分类号: D814.1 **文献标志码:** A **文章编号:** 1673-8039(2026)02-0001-10

以数字技术为核心支撑,数字外交涵盖网络外交、电子外交与数字公共外交等多种形态,融合网络安全、数字贸易、人工智能、数据治理与隐私保护等议题,逐渐演化为国家提升数字合作能力、强化数字权力结构并塑造全球影响力的重要战略工具^[1]。近年来,全球数字技术加速演进,大国战略竞争也同步深化,数字领域已从单纯的经济与技术议题,上升为关乎国家安全、产业竞争力以及国际秩序塑造的核心领域。人工智能、数据资源、半导体与数字基础设施的战略属性显著增强,日益成为地缘政治博弈的重要工具。世界经济论坛发布的《2024年全球竞争力报告》显示,欧洲在数字化和技术发展等关键领域落后于竞争对手,其在技术创新能力上的短板,显示出在全球科技竞争中处于相对被动的地位。在此背景下,欧盟逐渐意识到,以“规范性力量”塑造国际影响力的合作途径与外交模式,已难以有效应对全球数字竞争日益加剧所带来的现实挑战,遂转而探寻一条更具竞争性、战略韧性的数字外交之路。

欧盟理事会于2022年7月明确将数字外交视为对外行动的核心要素。2024年7月,欧盟外交事务理事会举行年度交流会讨论数字外交问题,此时欧盟认为数字问题已从纯粹的技术问题转变为具有关键战略和政治意义的问题。2025年6月,欧盟委员会发布《欧盟国际数字战略》,将数字议题界定为系统性韧性、经济竞争和安全战略。此时,欧盟数字外交更加关注地缘政治与安全,淡化对“规范性力量”的追求,采用更具现实性的数字战略工具。因此,通过探究欧盟推动数字外交转型的内在逻辑与行动特征,不仅有助于把握欧盟当前国际数字战略的立场,洞悉欧盟开展对外关系的新思维范式,而且有助于理解欧盟当下战略自主权与数字主权的延伸态势。

一、欧盟数字外交的转型

自俄乌冲突爆发以及全球数字竞争态势加剧以来,欧盟“规范性力量”受到冲击,其数字外交战略开始呈现出明显的现实主义转向。这一转型

收稿日期:2025-12-15

基金项目:2025年中央高校基本科研业务费专项资金项目“欧盟数字安全战略发展态势及对我国启示研究”(25JSQ083)

作者简介:李佳兴(1998—),男,陕西西安人,法学博士,陕西师范大学国家安全学院讲师,陕西师范大学元贞实验室研究员。

并非对“规范性力量”的完全摒弃,而是在坚持其核心价值观的基础上,更加强调权力的运用、利益

的维护以及对地缘政治现实的考量。欧盟数字外交转型的多维度对比见表1。

表1 欧盟数字外交转型的多维度对比

维度	2022年版《欧盟数字外交》	2025年版《欧盟国际数字战略》
主要关注点	以价值观为中心的数字外交	数字地缘政治和地缘经济学
战略框架	强调规范、人权和开放互联网原则	竞争力、安全性、供应链、值得信赖的合作伙伴关系
伙伴关系模式	广泛数字对话与合作,强调包容性与能力建设	数字伙伴关系、数字贸易协定、技术联盟
技术领导力观点	通过监管影响塑造全球规范	经济和安全方面的全面提升
关键技术	网络安全、数据治理、人工智能伦理、互联网治理	半导体、云与数据中心、海底光缆、量子技术
优先合作领域	监管力量、电子商务谈判、全球数字政策、隐私与人权	国防技术、经济与供应链安全、数字基础设施、海外投资
标准与规则制定	倡导价值导向的国际标准合作	主动抢占国际技术标准制定主导权
全球参与模式	普世主义,在全球范围内推广欧盟价值观,多边主义	基于利益和权力的数字战略,平衡全球数字竞争格局

(一)规范性力量:基于价值观的数字外交

“规范性力量”由英国学者伊安·曼纳斯(Ian Manners)于2002年提出,其定义为“在国际关系中塑造关于规范概念的能力”^[2],其强调规范的重要作用,重视发展欧盟作为规范本身的示范意义。“规范性力量”一方面将欧盟自身塑造为规范的成功实践者,通过发布政策倡议、战略沟通文件等途径,大力宣扬欧式“普世价值观”;另一方面,通过制定规范标准试图对他国进行改造,赋予欧盟行动合法性。受“规范性力量”理论影响,欧盟数字外交策略早期呈现明显的意识形态色彩,通常把价值观外交当作极为重要的手段来运用^[3]。

一方面,欧盟将数字技术应用于公共外交层面,在虚拟空间互动中提升其国际形象与外部声誉。欧盟外交代表团利用多种社交媒体平台,吸引各国对欧盟外交动态的关注,同时监测数字媒体绩效指标,深入分析媒体互动环境,不断优化个性化传播手段,以此大力宣传欧盟的核心价值观。费代丽卡·莫盖里尼(Federica Mogherini)2015年就任欧盟(EU)外交与国防政策高级代表后,声称社交媒体平台代表了“外交和沟通的非凡渠道”,并致力于将其用作“外交的基本工具”^[4]⁴⁵⁸。2017年推出的“欧洲之路”,开展《欧盟全球战略》的宣传工作,借助话题标签、视觉内容、跨平台传播的形式来树立其“全球欧洲”和“规范性力量”的形象。新冠疫情时期,欧盟通过数字平台与技术构建规范话语体系,塑造欧盟作为团结合作的领导者与新冠疫情下的“常态欧洲”的国际形象^[5]。

另一方面,欧盟打造数字监管力量。欧盟自主制定高标准且具有强约束力的数字法规,借助其内部市场规模优势以及制度外溢效应,不仅对欧盟内部的数字行为加以规范,还凭借这些规范引领国际数字治理实践、设定国际数字标准,进而增强其在全球数字议题领域的领导力^[6]。2018年欧盟出台的《通用数据保护条例》引领国际社会数据保护立法趋势,增强欧盟在全球数字治理中的话语权^[7]。此后,欧盟在与第三国及国际组织进行数字治理谈判时,将《通用数据保护条例》嵌入其构建合作关系的议程中,作为数字合作的原则性前提。2022年欧盟陆续出台《数字服务法案》和《数字市场法案》,进一步强化了对数字平台的监管力度以及欧盟作为全球数字规则制定者的角色^[8]。

在总结过往数字外交实践经验的基础上,欧盟理事会在2022年7月发布解释数字外交的结论文件中明确将数字外交定位为欧盟对外行动的核心要素。该文件提出以价值观为内核的外交方法,着重强调维护规则、保障人权以及构建开放的互联网秩序,坚定秉持多边主义合作模式,借助数字监管能力来提升欧盟在全球的声誉^[9]。该文件是欧盟首次以正式政策文件的形式提出“数字外交”概念,标志着数字议题被系统地纳入欧盟对外关系与全球战略议程之中。

(二)现实主义化:基于权力和务实性的数字外交

近年来,欧盟加速推进“规范性力量”向现实主义的转向进程,在政策层面重新聚焦于地缘竞

争、权力政治、军事力量等经典概念。前任欧盟委员会副主席何塞普·博雷利(Josep Borrell)认为欧盟需要将自己视作“强权国家”,在国际政治压力下思考“硬实力”的重要性。“地缘政治欧洲”这一理念提出后,欧盟日益重视向全球投射战略力量,借助权力政治塑造威慑力,建立韧性、竞争力与安全并重的对外政策体系^[10]。同时,欧盟战略自主权愈发强调去风险化,以物质和技术为基础提高国际竞争力,大幅提升全球影响力与秩序塑造能力。因此,欧盟尝试将价值观融入权力构建之中,使规范性目标与物质能力相匹配,实现从全球秩序的“裁判员”向“地缘政治行为体”“全球领导者”的角色转变。

上述趋势也直接反映在欧盟数字外交层面。虽然欧盟2022年“数字外交”文件提出了指导性构想,但彼时欧盟对日益突出的数字安全与地缘政治挑战关注不足,导致其在全球数字竞争中陷入被动。随着“数字主权”觉醒,欧盟数字战略开始从权力政治逻辑看待国际数字竞争与合作,以战略化、安全化和意识形态化来看待国际数字环境^[11]。因此,欧盟于2025年正式出台《欧盟国际数字战略》,对其数字外交策略作出调整,展现出更为显著的“战略雄心”。该战略致力于升级外交工具,着重参与全球数字治理议程,构建相互依赖的伙伴关系网络,进而巩固欧盟在全球数字秩序中的领导地位。

与2022年欧盟理事会解释数字外交的指导性文件对比,欧盟数字外交转型趋势体现在如下方面。其一,强化地缘政治与战略竞争色彩。与欧盟2022年数字外交文件强调加强规范输出与数字监管能力不同,《欧盟国际数字战略》将数字问题界定为系统韧性、经济竞争和安全问题,强调提升欧盟数字技术能力,希图加强数字产业投资合作,优先建设数字伙伴关系网络,以实现平衡全球数字竞争格局。此时,欧盟显著提升数字战略在地缘政治博弈中的权重,将数字外交视为维护自身战略安全利益、应对大国竞争的核心工具,以更加积极、主动姿态参与全球数字治理主导权争夺。其二,布局、调整数字战略优先发展领域。《欧盟国际数字战略》弱化对“布鲁塞尔效应”“数字人权”“欧盟人工智能法案”等词汇的提及,转而优先关注数字国防技术、安全基础设施、数字供应链以及欧盟科技商业计划等领域。这种取舍印证欧盟致力于推动数字政策的安全化进程,将数

字战略与国防与安全议程深度嵌合,通过强化对关键数字基础设施与核心技术的自主可控能力,逐步塑造数字领域的“硬实力”基础。这种以技术控制力为核心的数字“硬实力”,不仅提升了欧盟应对外部安全风险的战略韧性,也为其在数字空间推进权力政治、塑造国际规则与竞争格局提供了物质支撑。其三,提升构建数字伙伴关系的务实性。《欧盟国际数字战略》要求欧盟构建新的数字伙伴网络,依托双边合作、区域框架、全球制度的多维度方法,构建覆盖“全球—区域—国家”的合作体系,凝聚更多、更广泛国家行为体的数字利益。同时,欧盟把数字合作纳入安全与防务合作体系之中,加大对军民两用先进技术能力的投入力度,并推动欧盟安全与防务科技产业在人工智能、量子技术及其他新兴技术领域,成为核心合作伙伴与创新驱动力。在全球门户框架下,欧盟着力加大对伙伴国家的投资力度,实现欧盟与数字增长中心的连接,并为欧盟的经济安全提供助力^[12]。

二、驱动欧盟数字外交战略转型的因素分析

随着欧盟在数字地缘政治中的话语权逐步下降,欧盟愈发意识到“规范性力量”不能有效提升其影响力。同时,科技巨头的成长也削弱了欧洲在数字技术与标准领域的主导地位,进而成为影响其数字外交自主性的关键因素之一。加之,全球范围内数字安全威胁的多样化与高频化,也迫使欧盟加快战略转型的步伐,以适应当前激烈的竞争环境。

(一)“规范性力量”受到全球数字竞争冲击

一方面,由于欧盟过于强调“规范性力量”反而限制了数字竞争力的提升,导致欧盟在数字产业面临投资规模滞后、创新活力不足以及产业转型困难等困境。在与美国的数字贸易服务中,欧盟存在超过约1000亿欧元的逆差,暴露了其在全球数字价值链中的不利地位。相较于美国科技巨头在云计算、大数据和人工智能等领域的强势输出,欧盟本土企业的竞争力则显得相对薄弱,难以在国际市场中占据主导地位。例如,在云计算市场上,三大美国云服务商谷歌(Google Cloud)、微软(Microsoft Azure)和亚马逊(AWS)占据全球65%市场份额,而欧洲供应商市场份额甚至不足1%^[13]。技术竞争领域的落后也会直接影响数字

伙伴关系建设,美国的“印太经济框架”和中国的“数字丝绸之路”在第三方国家中显示出更强的资源整合能力和政治动员能力,进一步削弱了欧盟对外开展数字合作的号召力。

另一方面,欧盟“规范性力量”受到地缘政治竞争的反制。美国与欧盟围绕数字监管问题产生摩擦,对欧盟的数字权益产生巨大冲击。特朗普政府上台后一改拜登政府时期对人工智能的监管律令,强烈反对欧盟主张的严格监管方式。美国副总统詹姆斯·戴维·万斯(James David Vance)在巴黎人工智能峰会上发表演讲,严厉批评欧洲监管规定,宣称美国在人工智能军备竞赛中占据主导地位。美国国务院谴责《数字服务法案》是一种“欧威尔主义”审查制度,忽视了技术发展的灵活性需求,可能对全球数字市场的自由流动造成阻碍。2025年11月,美国商务部部长卢特尼克在与欧盟贸易官员会谈后,公开将数字监管与钢铝关税挂钩,进一步迫使欧盟让步。然而,目前欧盟除了减少对美国数字产业依赖,向大型科技公司开具“罚单”之外,并未有行之有效应对措施。

(二) 科技公司崛起影响数字外交格局

一方面,欧洲科技公司拥有对政策议题设置、技术标准制定以及数字治理框架的塑造能力,在一定程度上冲击欧盟作为政府间组织的主导性。在跨境支付、云计算及内容分发平台等关键数字领域,欧洲科技公司往往率先部署和推广自身的技术标准,形成事实上的行业规范。这使得欧盟在相关政策的制定与实施过程中,需要参考企业既有的技术架构与运作规则^[14]。诺基亚(Nokia)和爱立信(Ericsson)曾对欧盟起草有关通信设备、联网汽车相关的专利标准持反对态度,这一施压最终导致欧盟撤回部分技术专利、AI责任、隐私议案等条款。此外,欧洲科技公司凭借其在数字跨国投资中的关键作用,获得左右欧盟对外投资政策的能力。2025年3月100余家欧洲科技公司向欧盟委员会提交公开信,要求设立“主权基础设施基金”,推行“购买欧洲货”(Buy European)政策,并减少与外国科技公司的投资合作^[15]。

另一方面,外国科技公司也削弱了欧盟数字外交的影响力。美国科技巨头凭借其在全球数字市场的垄断地位,通过游说、资本运作及技术转移等手段,深度介入欧盟数字政策制定过程。包括微软、苹果、亚马逊、高通和谷歌在内的科技公司

支出大额预算,对欧盟有关机构进行政策游说,加大对《数字市场法案》《数字服务法案》《人工智能法案》的抵制,逼迫欧盟放宽数字规则限制^[16]。埃隆·马斯克和马克·扎克伯格强烈抨击欧盟的审查制度,这种对抗情绪进一步加剧了欧盟与美国科技巨头之间的紧张关系。受这种趋势影响,欧盟内部已经出现了不一致声音,爱尔兰和意大利等成员国主张采取更为温和的方式,弱化对美国科技巨头的监管。

(三) 全球数字安全治理复杂性显著提升

全球数字治理的碎片化加剧,导致政策分歧频发、治理效率下降。当前国际社会还没有功能明确的专门的数字治理国际组织,这一治理工作主要依托于以联合国、二十国集团、亚太经合组织为代表的国际多边治理机构。这些机构在数字治理领域的职能往往分散且不够专注,难以应对日益复杂的数字安全问题。同时,排他性发展和数字霸权主义阻碍全球数字安全治理合作。美国凭借自身数字技术与产业优势推行数字霸权主义,实施技术封锁,加大司法干预和经济制裁,利用联盟政治高筑数字藩篱,竭力打压新兴国家的数字技术与产业^[17]。为了应对美国霸权主义威胁,各国纷纷制定严格的网络安全和隐私法规,形成复杂不透明的法律体系,造成复杂且混乱的全球数字监管环境。

数字安全与防务议题迅速升级,成为国家安全的巨大威胁。在当下的国际安全格局中,数字安全与防务议题迅速成为全球关注的战略焦点,其威胁性质和影响力已超越传统安全领域。人工智能驱动的网络攻击,如深度伪造、对抗性样本、自动化渗透工具正在重塑网络攻防格局。近期研究表明,大语言模型可被操纵生成欺骗性攻击样本,对传统检测体系构成挑战^[18]。2025年,来自92个国家的报告显示受到过与人工智能相关的攻击;人工智能推动的数据泄露平均成本达到572万美元,同比增长约13%^[19]。数字技术的进步推动了战争形态的演变,使全球安全面临更为严峻的“混合战争”风险。当前,针对关键基础设施的攻击日益复杂,网络威胁已突破传统的服务器边界,延伸至货舱控制系统、港口运营设施、电网调度节点以及国防工业供应链,形成跨领域、跨系统的安全挑战。

当前全球主要大国已将数字安全纳入国防事业与对外合作事务之中,这也启示欧盟必须重新

审视其数字外交的安全维度,提升数字竞争力,以权力政治思维应对全球数字安全领域的复杂博弈。

三、欧盟数字外交战略转型的路径解析

为适应全球数字竞争格局发展,欧盟调整数字外交战略,强化数字传播建设,推动全球范围内的数字经济合作,打造新型数字伙伴关系网络,增强新兴数字基础设施建设,构筑数字安全环境。

(一)强化数字传播建设,提升全球战略叙事能力

随着数字外交工具的不断迭代升级,欧盟愈加重视数字传播体系的建设,通过强化战略传播与信息影响力手段,致力于在全球舆论竞争中重塑国际形象、增强话语权,并重建与国际社会的信任关系。

欧盟组建、调整负责数字外交的职能机构,强化跨部门协调力度。欧盟对外行动规划署(EEAS)设立“战略传播”和“传播政策与公共外交”机构宣传其战略形象:“战略传播司”承担抵御国外情报操纵和干扰(Foreign Information Manipulation and Interference)的职责,领导东部战略传播工作组、西巴尔干工作组、南方工作组、撒哈拉以南非洲战略传播工作组开展跨区域合作;“传播政策与公共外交司”推动人工智能、社交媒体分析与数字外交工具结合,利用定向传播、数据舆情监控优化外交信息。此外,欧盟加快机构调整与重组,服务于数字外交建设。2023年11月,欧盟“信息总司”(DG Informatics)正式改组为“数字服务总司”(DG DIGIT),突出在现代化数字战略服务职能。2025年2月,欧盟委员会成立负责战略沟通和打击信息操纵的特别工作组,隶属于欧盟通讯总司,旨在提高应对信息操纵的态势感知能力。

欧盟在主流社交平台上构建了覆盖全球的传播体系,在地区冲突中,这些平台承担议题设置与危机叙事功能。2024年10月巴以冲突升级时,欧盟驻以色列及驻巴勒斯坦使团以人道主义援助与国际法为核心话语,通过Instagram、Facebook、Twitter传播信息,一边介绍欧盟与以色列科技合作成果,另一边发布欧盟向巴勒斯坦提供人道主义援助信息,塑造欧盟的“冲突调停者”形象。欧盟驻乌克兰代表团打造如“在一起,我们是欧洲”(Together, We Are Europe)、“我们一起学习与成

长”(Together We Learn & Grow)的官方网站与社媒话题矩阵,以数字化形式讲述欧盟对乌克兰支持的具体项目与成果,强化“欧盟—乌克兰战略伙伴关系”叙事指引。

地缘政治竞争加剧背景下,欧盟警惕“认知入侵”,建立对抗信息战、情报战的外交工具,即欧盟混合工具箱(EU Hybrid Toolbox)、欧盟网络外交工具箱(EU Cyber-Diplomatic Toolbox)和国外情报操纵和干扰工具箱(Foreign Information Manipulation and Interference Toolbox)^[20]。欧盟混合工具箱鼓励欧盟与北约等伙伴建立对话与协调关系,在网络安全、战略传播、关键基础设施保护等领域形成防御网络。欧盟网络外交工具箱旨在增强网络韧性、防护与危机管理能力,强化与全球伙伴的关系,深化“共享态势感知”合作^[21]。国外情报操纵和干扰工具箱将外交行动视作核心策略,与七国集团和北约建立反国外情报操纵和干扰合作议程,推动情报信息的共享。

(二)推动数字经济合作,维持市场竞争力

《欧盟国际数字战略》将经济安全定位为欧盟数字伙伴关系的核心目标,致力于利用数字技术创新、数字贸易自由化、数字投资环境优化等手段降低对外部供应链的依赖,重新实现对全球数字市场的控制。

欧盟数字贸易协定是其数字经济政策的重要组成部分。制定协定的方式可分为以下两类:一是在其自由贸易协定中加入数字经济章节;二是与目标一致的伙伴直接签订数字贸易协定。欧盟已与加拿大、智利、日本、新西兰、墨西哥、越南等国完成自由贸易谈判,并在协定中纳入数字贸易条款,将《通用数据保护条例》等规范扩展至贸易关系中。此外,欧盟与新加坡、韩国就数字贸易协定谈判取得突破性进展。欧盟与韩国已完成数字贸易协定谈判,围绕数据和数字技术制定互惠互利规则达成共识。欧盟与新加坡正式签订首份数字贸易协定,在数据流通、在线服务、网络安全及电子认证等领域确立高标准规则,提升全球数字贸易规则制定的“门槛”。

欧盟高度重视数字供应链韧性建设,打造全球性数字产业生态。2025年6月的东南亚半导体展览会上,欧盟与东南亚近100名官员、企业领袖、研究人员共同举办研讨会,探讨加快半导体产业合作,展示欧盟作为半导体投资与合作伙伴的地位。欧盟GAIA-X项目与加勒比地区企业建

立战略伙伴关系,构建以开源框架为核心的云服务体系,联合打造数字生态系统,该系统参照欧盟《通用数据保护条例》标准,为加勒比地区医疗保健、教育、金融和政府提供数字服务,重塑地区数字格局。

为扭转“布鲁塞尔效应”影响力减弱的趋势,欧盟调整数字规则制定模式,以便利化、精简化与可操作性为导向,强化与国际伙伴的协调。近期,欧盟与美国就《互惠、公平和平衡贸易协定框架》达成一致,双方就电子传输关税、贸易数字化流程、海关改革立法等数字经济标准问题达成共识,有助于缓和双方紧张的贸易关系。欧盟还积极推动在国际组织内建立“欧式”数字经济标准。欧盟统计局与联合国贸易和发展会议就跨境电子商务统计口径与技术开展多轮对话,向东南亚、非洲等地区的国家提供数字治理能力支持,帮助受援国建立符合欧盟标准的跨境电子商务数据管理体系。

(三)扩大国际伙伴关系网络,增强全球领导力

为进一步扩大国际伙伴关系,欧盟正致力于深化既有数字伙伴关系与对话机制、构建新的合作平台,打造多层次的新型数字伙伴关系网络,支持伙伴国家的数字化转型,提升技术竞争力与数字安全水平。

其一,欧盟积极打造双边数字伙伴关系,与相关国家构建数字联盟。欧盟先后与日本、韩国、新加坡、加拿大签署数字伙伴关系协定。这些协定并未采用单一、封闭的模式,而是允许各方根据自身关切与优先领域纳入特别感兴趣的议题,从而形成多元化的合作框架。与传统的侧重于国际货物和服务贸易市场准入的协议不同,这些协议更侧重于电子商务便利化、跨境数据流动、网络消费者保护、隐私和个人数据保护以及技术创新合作等方面。此外,中国是欧盟数字发展的机遇以及维持技术主权的伙伴,双方互为关键市场,在自动驾驶、人工智能等创新科技产业领域以及跨境数据流动、数据保护与科技监管政策领域的合作不断深化,正成为全球数字合作的范例^[22]。

其二,欧盟积极打造区域间数字伙伴关系,向拥有数字发展潜力的地区提供制度与技术支持。2023年3月,欧盟—拉美和加勒比地区数字联盟成立,欧盟委员会提供1300万欧元资金,推动Bella第二阶段项目向中美洲国家拓展,支持该地区数字生态系统建设。欧盟与东盟近年来先

后发布《欧盟—东盟网络安全合作声明》《欧盟—东盟数字工作计划》等战略文件,向外界展示双方深化数字合作的决心。2025年8月,欧盟与东盟举办数字贸易和供应链韧性研讨会,与会代表重申当前数字合作对提升双方战略伙伴关系发展势头的重要性。欧盟依托“地平线2020”设立AfriConEU、HUBiquitous和ENRICH in Africa项目,支持加强数字基础设施建设。欧盟委员会执行副主席亨娜·维克库宁(Henna Virkkunen)表示未来欧盟将继续拓展与智能非洲联盟和非盟联盟的数字伙伴关系,加强彼此间的经济联系^[23]。

其三,欧盟积极打造企业间数字合作伙伴关系,建立跨国企业联盟和产业合作平台。一方面,欧洲企业以合作伙伴身份参与欧盟推动的“数字伙伴关系”倡议,承担技术供应者和政策执行者的角色,赋能公私伙伴关系(PPP)。例如,诺基亚与日本、加拿大等国企业开发5G、云无线接入网(Cloud RAN)、开放式无线接入网(Open RAN)等网络架构,推动欧盟“数字伙伴关系”从政策对话走向技术共建和标准协同。另一方面,欧洲企业通过对外投资、跨国并购以及在海外设立研发中心,推动技术与市场的双向流动,强化欧盟与合作国之间数字产业纽带。例如,思爱普(SAP)和OVH cloud在亚太地区和美洲设立云数据中心,助力数字产业跨区域融合,为欧洲企业开辟新的国际市场空间。

(四)强化新兴数字基础设施合作,构筑安全环境

数字基础设施在国防安全与应急响应体系中发挥着关键作用。为增强欧盟的集体防御能力、降低对高风险供应链的依赖,在关键技术领域实现自主可控,欧盟积极推动新兴数字基础设施的合作。

欧盟将量子通信视作其经济安全战略中的关键技术。2025年5月,欧盟与日本签署“量子科学技术合作意向书”,征集先进算法和混合计算应用的项目,推进量子人工智能在生物医学和气候建模等领域的应用。2025年7月,欧盟与加拿大联合推动“超空间”(HyperSpace)的国际项目正在突破基于光纤的量子链路的极限,构建量子光源、信号编码器、探测器以及兼容空间的光学系统。2025年6月,欧盟与韩国启动支持量子技术的数字合作伙伴关系,投资800万欧元研发加速量子计算和模拟应用的软件和硬件,制定量子安全通信协议,攻关开发特定应用的量子传感器。

6G 是数智时代的关键基础设施,尽管欧盟在 6G 技术方面的竞争力并不领先,但其仍是全球电信行业中的强大参与者。美国电信行业解决联盟(ATIS)的“下一个 G 联盟”(Next G Alliance)同欧盟 6G 产业协会联合发布了《欧盟—美国超越 5G/6G 路线图》,联合构建 6G 无线数据集与模型库,推动 6G“安全可验证”设计与公共信任评估合作。欧洲航天局(ESA)与日本国家信息通信技术研究所(NICT)建立 5G/6G 技术伙伴关系,提升 5G 核心网技术能力。未来,欧盟与日本的合作将重点拓展 5G 和 6G 非地面网络,强化航天与航空产业的竞争力,巩固双方在新一代数字基础设施与空间通信格局中的战略关系。^[24]

高性能计算设备是欧盟数字转型的技术引擎。欧盟与日本已启动 HANAMI 项目,整合欧洲与日本领先的超级计算中心,在气候模拟、材料研究和生物医学领域开发高性能计算应用程序。2025 年 1 月“欧盟—日本高性能计算合作”高级别研讨会上,双方在共享科研基础设施、规划未来联合项目以及联合申请科研经费方面达成共识。欧盟与印度依托 GANANA 项目建立了科学高性能计算(HPC)伙伴关系,通过共享高性能计算资源与基础设施,并扩展其功能来开发若干关键的软件工具,从而提升高性能计算的可扩展性与应用深度。

海底光缆成为欧盟延伸数字外交影响力的重要途径。欧盟提出建立“领先的电缆外交”的概念,主张与邻国、战略伙伴和第三国开展安全、可信任以及具有韧性的海底电缆基础设施合作,塑造欧盟维护全球海底基础设施安全的积极形象^[25]。黑海沿岸国家、地中海沿岸以及“印太”地区是欧盟开展海底电缆外交的重点。2022 年 12 月,欧盟与阿塞拜疆、格鲁吉亚以及匈牙利领导人签署《黑海能源海底电缆建设谅解备忘录》,规划在黑海地区建设长达 1195 公里的海底电缆。2023 年欧盟投入 3.42 亿欧元推动“美杜莎计划”,该项目连接北非五个国家(摩洛哥、阿尔及利亚、突尼斯、利比亚和埃及)的海底电缆,有效提升欧盟与北非地区跨境数字服务,重塑数字地缘政治格局。

四、欧盟数字外交转型的限制因素及前景展望

欧盟数字外交转型需要充分的条件,而欧盟

内部的“隔阂”与外部的“阻力”及其数字安全能力“滞后”成为无法忽视的限制因素。未来,欧盟将继续推动数字外交的体系化与地缘化,提升数字话语权构建,推进技术自主和经济安全“双轮驱动”。

(一) 欧盟数字外交转型的限制因素

其一,欧盟内部存在的“隔阂”制约数字外交的协同性。一方面,欧盟有关数字领域的法律存在碎片化、重叠化的情况,并与成员国法律存在不一致性的问题,影响数字一体化建设。例如,2022 年欧盟通过《数字市场法》,该法案特别允许欧盟成员国在数字领域制定更具针对性的补充性法规,然而由于各成员国在数字经济发展水平、产业侧重点以及政策理念等方面存在差异,且缺乏统一协调机制,导致德国、法国在继续推进法律改革的过程中,产生监管碎片化和法规冲突的问题。另一方面,欧盟内部对于数字主权的理解存在分歧,难以形成统一立场。东欧国家出于地缘安全考虑而期望欧盟加强网络安全控制,强化数字基础设施的防御能力;瑞典和丹麦等国注重实现跨大西洋情报信息的自由流动,保障欧盟的信息安全。法国、德国、西班牙、意大利更强调产业保护,有强烈的重商主义思维,而荷兰、爱尔兰等国主张保持开放原则,担心过度强调“主权化”会削弱创新能力与跨大西洋合作水平。^[26]

其二,欧盟外部存在“阻力”制约数字外交的认可度。美国与欧盟在数字监管问题上的摩擦上升至地缘政治层面的博弈,加剧跨大西洋科技合作关系的紧张局势。英国“脱欧”后更倾向采用灵活监管与促进创新并举的模式,日本在人工智能和数据流动治理上强调自愿框架与可信跨境数据流动(DFFT),两者与欧盟的强制合规模式存在明显差异。在亚太地区,包括韩国、澳大利亚及东盟部分成员国,普遍关注数字经济发展红利与基础设施投资便利,担忧欧盟严格的合规要求会抬高市场准入门槛、降低数字创新活力。另外,非洲与拉美国家的学者批评欧盟将自身标准作为“全球公共品”强行推行,形成事实上的“数字殖民主义”^[27]。

其三,欧盟数字安全能力“滞后”制约数字外交的影响力。欧盟缺乏一体化的军事数字基础设施与网络防御能力。一项研究评估了 75 个欧盟机构的网络安全状态,发现其中 67%得分 D 或 F(较低安全等级),没有一个机构达到 A 或 B 等级。在

欧盟网络安全局的《2024年网络安全状态报告》中,也明确指出欧盟及成员国在很多方面的网络安全成熟度仍不足^[28]。同时,欧盟在先进数字防务技术研发方面亦处于相对滞后状态。例如,由于侦察卫星数量不足,在军事太空应用能力方面较弱,其军事卫星在关键数据、服务以及发射能力上严重依赖美国,特别是对太空探索技术公司(Space X)发射系统的依赖,使欧盟难以在危机环境下独立运作,影响其向伙伴国家提供安全支持的能力。

(二) 欧盟数字外交转型的前景研判

一方面,欧盟将加速推动数字外交向体系化与地缘化的转化。通过数字伙伴关系、数字贸易协定和“欧洲科技团队”倡议等机制,欧盟构建覆盖战略协商、技术合作、规则制定、产业投资的全链条式数字外交模式,并尝试进一步以数字互动深化与伙伴国家的政治信任,促进产业协同与市场一体化。为巩固其在全球数字治理中的领导地位,欧盟正着手构建更大范围的“数字联盟”,重点深化与新兴数字经济体及具有潜力的数字市场合作,同时在制度设计上有意排除中美等全球数字强国,刻意减少对中国和美国的依赖性,确保欧盟在合作框架中的主导权与议程控制力。

另一方面,欧盟将推进技术自主和经济安全“双轮驱动”,遵循价值、收益、安全并重的竞争导向^[29]。《欧盟国际数字战略》将技术合作视作优先选项,引导欧盟提升技术能力,强化其在全球数字秩序中的战略自主性与竞争力。当前,欧盟加大对关键数字技术投资力度,推动云计算与人工智能基础设施本地化布局,推广关键数字工具的应用,制定针对中小企业的数字赋能政策,并与日本、韩国等保持数字技术采购关系,获取国际前沿先进技术。^[30]此外,欧盟将供应链韧性视作维护数字经济安全的关键手段,着手与全球伙伴建立稳固、可信赖的价值链,减少对单一供应来源的依赖。欧盟委员会2025年设立国际半导体合作项目,与主要半导体国家开展合作,加强欧洲产业在全球半导体价值链中的地位。

尽管欧盟数字外交的现实程度有所提高,但某些领域欧盟仍保持着强规范性的特征,成为其数字外交转型的“未竟之业”。欧盟在国际场合持续推广“以人为中心的数字化”“数字人权”“可信AI”等理念,构建区别于美国和中国的数字治理范式,将数字合作嵌入欧盟单一市场准入、数据充分性认定、供应链合规等制度框架之中。第三

国为进入欧盟市场,往往被动接受欧盟数字规范^[31]。例如,欧盟支持非洲制定同欧盟《一般数据保护条例》类似的法律标准,要求非洲国家建立数字身份系统以推广个人权利保护理念^[32]。同时,欧盟数字战略尽管明确加强对大型科技公司的监管,但是在增强公民对国家的力量方面投入不足,导致数字技术领域官僚化、封闭化严重,影响欧盟提升数字创新力^[33]。

五、中国的启示及应对

欧盟数字外交转型背景下,中国需要以更加审慎和务实的策略促进双方合作。

首先,中国应继续推进与欧盟的数字治理对话机制建设,重点聚焦跨境数据流动、人工智能治理、平台监管与技术伦理等规范化程度较高的领域。通过议题协商、政策沟通和监管经验交流,降低欧盟数字规则对中国技术与企业的制度性排斥风险。鉴于欧盟数字外交正从规范输出转向战略工具运用,中国需重视欧盟在数字政策中“安全化”“战略化”的逻辑变化。在参与国际数字规则制定时,既要坚守数据主权、网络安全等核心利益底线,也要展现开放合作的姿态,积极探索与欧盟在数字规则上的兼容性与对接点。

其次,中国应充分发挥自身在数字市场规模和产业链完整性方面的结构性优势,巩固在人工智能、自动驾驶、智能制造和数字基础设施等领域作为欧盟关键合作伙伴与重要市场的地位。欧盟数字外交转型的重要目标在于推动“去风险化”而非全面“脱钩”,中国可通过深化产业合作、扩大技术应用对接,强化中欧在数字经济领域的相互依赖性,避免欧盟在数字供应链和技术合作上与中国“脱钩”。

再次,中国应深度参与全球数字治理,通过多边和区域合作机制,构建更加多元化的数字治理网络。当前全球数字治理呈现出明显的碎片化特征,欧盟虽力图通过数字伙伴关系和数字贸易协定扩大制度影响力,但其全球数字治理模式仍受到广泛质疑。中国可依托联合国、二十国集团、上海合作组织以及“数字丝绸之路”等合作平台,推行更具包容性、以发展为导向的数字治理理念,构建兼顾各国发展利益诉求的数字规则体系,提升发展中国家在全球数字治理中的话语权^[34]。

最后,在战略认知与外交叙事层面,中国应保持克制和稳定的对欧数字外交表述,避免被动卷

入欧盟主导的话语竞争。欧盟当前高度重视数字传播、信息安全与认知防御,将数字外交视为塑造国际舆论和战略认同的重要工具。对此,中国更应强调技术发展权、数字包容性与“全球南方”国家数字能力建设,弱化对抗性叙事,通过务实合作与公共产品供给提升自身在全球数字治理中的形象与影响力。

欧盟推动数字外交转型是在全球数字竞争加剧背景下对自身战略定位的深刻反思与调整。欧盟意识到仅依靠传统的“规范性力量”已不足以应对复杂的数字地缘政治挑战。因此,欧盟数字外交逐渐从强调价值观输出、维持监管能力转向更加务实的战略布局,提升战略竞争力与安全能力,试图在全球数字秩序竞争中占据主动地位。通过强化数字传播建设,推动数字经济合作提质升级,扩大数字伙伴关系网络,打造跨国新兴数字基础设施合作高地,欧盟的数字外交展现出全新的面貌。在可预见的未来,欧盟将继续推进现实主义化的数字外交策略,坚定维持战略自主性,实现技术自主和经济安全“双轮驱动”,力争在中美数字竞争格局下成为“第三极”力量。此外,随着数字技术的快速发展和地缘政治环境的变化,中国也需灵活调整策略,既保持竞争意识,又注重合作机会,以实现互利共赢的数字外交新格局。

参考文献:

- [1] 赵鸿燕,沈伊扬.英国对华数字公共外交的布局与策略[J].现代国际关系,2024(10).
- [2] Manners I. Normative power Europe: a contradiction in terms? [J]. Journal of common market studies, 2002(2).
- [3] 殷佳章.规范性力量的现实主义转向:欧盟人工智能政策的演进[J].国际论坛,2025(6).
- [4] Zaiotti, Ruben. The European Union and Digital Diplomacy[M]. London: Oxford University Press, 2024.
- [5] 张莉,崔杨臻.新冠疫情期间欧盟形象的“自塑”——对话理论视角下欧盟在华数字公共外交的实践与效果研究[J].欧洲研究,2021(1).
- [6] Chayanis Aueamnuay, Carmen Berjón, Stella Galehr, Luca Graf and Andreas Heinemann. Digital Regulation in the European Union[R]. EuZ - Zeitschrift für Europarecht, 2024.
- [7] 田晓萍.欧盟GDPR的域外效力:管辖依据、实施路径、制度效应及启示[J].国际经济法学刊,2023(1).
- [8] 王丹娜.欧盟数字外交战略和措施的影响因素分

析[J].中国信息安全,2024(6).

- [9] Council of the European Union. EU Digital Diplomacy: Council Conclusions, Foreign Affairs Council[EB/OL]. (2022-07-18) [2025-11-13]. <https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf>.
- [10] Anghel V. Why the EU is a geopolitical power: Wartime enlargement, integration, and reform[J]. Journal of European Public Policy, 2025(12).
- [11] 张成新.战略自主、技术权力与欧盟数字战略的权力政治转向[J].世界经济与政治论坛,2025(2).
- [12] European Commission. An International Digital Strategy for the European Union[EB/OL]. (2025-06-05) [2025-12-02]. <https://digital-strategy.ec.europa.eu/en/policies/international-digital-strategy>.
- [13] Informa TechTarget. Global cloud infrastructure spending rose 21% in Q1 2025[EB/OL]. (2025-06-12) [2026-03-09]. <https://omdia.tech.informa.com/pr/2025/jun/global-cloud-infrastructure-spending-rose-21percent-in-q1-2025>.
- [14] Khanal S, Zhang H, Taeiagh A. Why and how is the power of Big Tech increasing in the policy process? The case of generative AI[J]. Policy and Society, 2025(1).
- [15] The Consumer News and Business Channel. 'Buy European': Airbus and others call for sovereign fund and higher Europe tech autonomy [EB/OL]. (2025-03-17) [2026-03-10]. <https://www.cnbc.com/2025/03/17/buy-european-airbus-and-others-call-for-sovereign-fund-and-higher-europe-tech-autonomy.html>.
- [16] 曹飞翠,董青岭.美国科技公司数字霸权的缘起、逻辑与影响[J].现代国际关系,2025(8).
- [17] 蔡翠红,李煜华.全球数字治理赤字:表现、成因与中国的应对[J].国际展望,2024(2).
- [18] Werisha Ibrar, et al. Generative AI: A Double-edged Sword in the Cyber Threat Landscape [J]. Artificial Intelligence Review, 2025, 58(9).
- [19] World Economic. Global Cybersecurity Outlook 2026[EB/OL]. (2026-01-12) [2026-03-10]. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.
- [20] Federica Iannó. The Rise of E-Diplomacy: Redefining EU Foreign Affairs Through the Lens of the Digital Age[J]. IE International Policy Review. 2025(2).
- [21] 吕蕊.欧盟网络外交:战略基础、政策向度与安全竞争[J].同济大学学报(社会科学版),2022(4).
- [22] 高乔.中欧数字合作如何“数”造未来[N].人民日报(海外版),2025-07-16(8).
- [23] The Digital for Development. EU and Smart Africa Strengthen Partnership for Africa's Digital Transformation

[EB/OL]. (2024-03-12)[2025-10-11]. <https://d4dhub.eu/news/eu-and-smart-africa-strengthen-partnership-for-africas-digital-transformation>.

[24]王飘.欧盟6G通信技术研发动态与进展[J].全球科技经济瞭望,2024(4).

[25]王丛,孙远.大国数字竞争下欧盟海底电缆的地缘政治化分析[J].德国研究,2025(3).

[26] Adler-Nissen R and Eggeling K A. The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X[J]. Journal of Common Market Studies, 2024, 62(4).

[27]Nothias T. An intellectual history of digital colonialism[J]. Journal of Communication, 2025(3).

[28] European Union Agency for Cybersecurity. 2024 Report on the State of Cybersecurity in the Union[EB/OL]. (2024-12)[2025-10-29]. <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>.

[29]冯存万.欧盟数字转型的战略成效及未来路径[J].欧洲研究,2025(6).

[30] Guinea O, et al. Breaking Barriers, Boosting Growth: Unlocking the Power of Digital Technology for Europe's Competitiveness[R]. ECIPE Policy Brief, 2025.

[31] Arslan S. Strategic Approach to the Role of Normative Power and its Instruments in Eu Foreign Policy in the Digital Age: 2010—2025[J]. International Journal of Academic Reserach in Economics and Management Sciences, 2025(4)

[32]Tafese T. Advancing EU-Africa Digital Partnerships amid Growing Geopolitical Competition[J]. Digital Cooperation with Global Partners—Policy Study, 2025.

[33] Youngs R. Rethinking Eu Digital Policies: From Tech Sovereignty to Tech Citizenship[J]. Carnegie Europe, 2025.

[34]刘宏松.全球治理中的数字外交:兴起、赋能与挑战[J].人民论坛·学术前沿,2025(22).

Realism of “Normative Power”: Transformation of the EU’s Digital Diplomacy

LI Jiaying

School of National Security, Shaanxi Normal University, Xi'an 710119, China

Abstract: The release of *An International Digital Strategy for the European Union* marks a new stage in the EU’s strategic layout in the digital field. Since the intensification of global digital competition, the EU has adjusted its pursuit of “normative power” in digital diplomacy and shifted its focus toward building a digital diplomacy system characterized by realist inclinations. This new trend is closely related to many factors such as the EU’s “normative power” being unable to adapt to the complex digital geopolitical environment, the rise of technology companies undermining the EU’s influence in digital diplomacy, and the significantly increased complexity of global digital security governance. To adapt to the current global digital competition landscape, the EU is strengthening digital communication construction to enhance its global strategic narrative ability, promoting digital economic cooperation to maintain its market competitiveness, expanding international partnership network to enhance its global leadership, and reinforcing cooperation on emerging digital infrastructure to build its secure environment. It is true that the EU’s digital transformation is also constrained by such limiting factors as internal “divisions” hindering its digital diplomacy, external “resistance” undermining the recognition of its digital diplomacy, and “lagging” digital security capabilities. Looking ahead, the EU will accelerate the development of its digital diplomacy toward institutionalization and geopoliticalization, strive to enhance the capacity for its digital discourse power, and advance the “dual-wheel drive” of technological autonomy and economic security.

Key words: EU’s digital diplomacy; digital strategy transformation; digital sovereignty; global leadership; digital norm

(责任编辑 宇 瞻)