欧盟网络空间战略调整与中欧网络空间合作的机遇

鲁传颖　范郑杰

【内容提要】在网络空间领域大国博弈态势加剧背景下，欧盟调整网络空间战略，注重维护自身的网络空间主权，提出要建立数字主权和技术主权；加大对成员国网络安全的统筹协调，先后出台了多部网络安全法律法规；主动参与网络空间全球治理进程，积极提升影响力与话语权。网络安全形势变化、网络空间大国博弈加剧以及“美国优先”对美欧网络合作带来巨大冲击，是欧盟调整其网络空间战略的主要影响因素。欧盟网络空间战略的调整有助于中欧双方在网络空间领域扩大共识、深化合作，同时为双方在网络空间全球治理层面加强政策协调与合作创造有利条件。

【关键词】欧盟网络战略；数字主权；技术主权；中欧关系

【DOI】10.19422/j.cnki.ddsj.2020.08.008

全球网络空间中一直存在着发展中国家与发达国家两个理念和立场差异较大的阵营。欧盟作为西方发达国家阵营的成员，在网络空间战略理念和能力上对美国高度依赖，一定程度上忽视了自身网络空间实力的建设。这不仅使欧盟在网络空间领域难以发挥重要作用，而且也阻碍了中欧在网络空间领域的合作。随着全球网络空间安全与发展形势的变化，欧盟对其网络空间战略进行了重大调整，这反映出欧盟正寻求更有效的治理理念来维护其网络安全利益，提升其在全球网络空间中的地位。这一变化也给中欧加强网络空间全球治理领域的政策协调和在网络安全、发展领域的双边务实合作带来了机遇。

欧盟网络空间战略的调整

网络空间大国博弈的态势正在发生急剧变化，从而引发欧盟调整其网络空间战略，这主要体现在欧盟在治理理念上开始关注网络空间主权，在战略层面注重构建统一的网络安全战略，以及更加积极地参与网络空间全球治理进程，并力求发挥领导作用。

第一，在网络空间治理理念上注重维护网络空间主权。传统上，欧盟一直强调网络的公域属性，关注网络自由、人权议题，积极支持政府之外的利益攸关方在治理中发挥主导作用。出于协调立场的需要，欧盟在很大程度上追随美国的网络空间治理理念，不太注重发挥领导作用。[1] 随着全球网络空间安全态势急剧恶化，欧盟面临的安全威胁和战略竞争不断上升，原有的治理理念已经不符合欧盟的利益。因此，欧盟重新审视网络空间的治理理念，从战略上重视维护网络空间主权，提出了数字主权和技术主权等新概念。

2018 年，欧盟委员会提出了数字主权（Digital Sovereignty）概念，为维护数字主权进行顶层设计。

数据是网络空间中最重要的战略资源，被认为是信息时代的“石油”。过去，欧盟与美国立场一致，主张数据应该在网络空间自由流动，国家不应当对数字流动设置障碍。然而，“斯诺登事件”爆出美国以“棱镜计划”为基础开展的大规模全球监听，特别是对欧盟及其成员国领导人的通信设备进行监听，侵犯了欧盟用户的隐私，严重危害了欧盟的数字主权。[2] 这一事件直接导致欧盟数据自由流动观念的转变，[3] 并于 2015 年废止了与美国签订的关于数据跨境流动的《安全港协议》。2016 年，欧盟与美国重新谈判制定了《欧美隐私盾》协定，但这一协定未能彻底打消欧盟对美国的疑虑。[4] 在此背景下，欧盟制定了具有全球影响力的《通用数据保护条例》(GDPR)，并将此视为维护数字主权的战略抓手。2018 年 5 月 25 日，在《通用数据保护条例》正式实施当天，欧盟委员会官方推特发文宣称重新掌控了自己的数字主权。

2020 年初，欧盟又提出要加强构建网络技术主权，减少对美国的依赖，保持在人工智能、数字经济等领域的独立自主。2 月，欧盟委员会发布了 3 份旨在建立和维护欧盟技术主权的网络战略文件，[5] 分别是《塑造欧洲的数字未来》(Shaping Europe’s Digital Future)、《人工智能白皮书》(The White Paper on Artificial Intelligence) 和《欧洲数据战略》(European Data Strategy)，从不同侧面对技术主权进行了阐述。技术主权的提出反映了欧盟希望摆脱长期依赖美国的现状，提升欧盟在网络空间领域的技术实力，其主要内涵包括：提升欧盟在与数字经济发展密切相关的数据基础设施和网络通信等领域的关键能力和关键技术独立自主的权力，以减少对外部的依赖。

第二，网络安全战略开始从成员国各自为战、强调非政府组织作用转向突出欧盟层面的顶层设计和统筹协调。近年来，随着治理理念的转变，欧盟开始制定区域层面的网络安全战略、政策和法规，强调区域层面的统筹协调。[6] 在早期网络安全治理中，欧盟对主权范畴进行划分并采取双层治理结构，如在涉及国家安全的领域往往是各成员国政府的主权范畴，因此各成员国的网络安全政策通常都由本国政府制定。但面对网络空间治理这样一个跨领域、跨部门的复杂议题，欧盟和各成员国之间的权力边界很难界定，传统的治理结构已经无法应对其中出现的安全问题。此外，随着全球网络安全形势恶化，欧盟各成员国难以独立应对，需要在欧盟层面进行资源配置和统筹协调才能有效解决。这一发展趋势使欧盟认识到原有治理模式已出现赤字，需要加强在欧盟层面的顶层设计加以应对。

从网络安全层面来看，欧盟近年来加强了顶层设计的力度，先后出台了《通用数据保护条例》和《网络安全法》，开始从欧盟层面统筹协调数据安全、网络安全问题。[7] 为了在欧盟内部更好地落实《通用数据保护条例》，欧盟还成立了数据保护委员会 (EDPB)，负责《通用数据保护条例》的解释工作，并对各国数据保护机构进行协调。此外，欧洲法院负责向各成员国法院就涉及网络安全的相关案件做出解释。《网络安全法》则将欧盟网络与信息安全署 (ENISA) 指定为永久性的网络安全职能机构，并且赋予其更多的网络安全职责。为了确保欧盟网络与信息安全署能够履行职责，欧盟大幅扩充了该机构的预算资源和人员配置。[8]

从发展新兴技术层面来看，欧盟一直致力于构建数字单一市场以方便数据在欧盟境内自由流动，为人工智能、云计算等新兴技术的发展提供基础保障。2015 年，欧盟通过了《数字单一市场战略》，

以保障数据在各成员国间自由流动。2020 年初发布的《欧洲数据战略》《人工智能白皮书》则为推动大数据和人工智能的进一步发展提供了保障。这些战略举措在很大程度上都离不开欧盟层面的统筹协调。一方面，欧盟通过区域层面的协调来克服成员国之间存在的差异，统一法律、标准和技术；另一方面，集中各成员国的优势，提升欧盟的网络空间治理能力。例如，欧盟通过集合德国的工业 4.0 和法国的网络安全技术等，试图在新兴技术领域获得领先优势。

第三，更加积极地参与网络空间全球治理并力求发挥领导作用。欧盟一度认为，国家或国际组织不应成为网络空间全球治理的主导力量，对于其他国家较为关注的网络主权、网络军备竞赛、数字鸿沟等议题也较少关注。然而，随着网络空间安全形势不断恶化，欧盟的这一立场越来越无法适应新的变化，并影响了欧盟在网络空间全球治理领域的话语权。在此背景下，欧盟的网络空间治理理念发生了转变，其对于参与网络空间全球治理的立场也发生了变化。

在对外交往层面，欧盟通过不断加强与其他国家的网络对话和交流实现了网络空间全球治理的全方位布局。欧盟不仅与传统盟友美国开展了网络对话合作，而且与日本、韩国这样价值观较为接近的国家以及印度、中国等新兴国家建立了网络对话机制。特别是欧盟与中国的网络对话机制，覆盖了全球治理、网络安全、数字经济、信息通信技术等多个领域，涉及双方之间的外交、网信和工信等多个部门。[9] 欧盟通过全方位的双边对话加强了与其他国家在网络空间全球治理和国内治理方面的政策协调，这有助于其价值观念和政策立场转化为网络空间治理领域的领导力。

在成员国层面，法国、德国等欧盟大国在网络空间全球治理中的影响力不断提升。欧盟虽然无法直接以国家身份参与到网络空间全球治理的多边进程，但是法国、德国等在欧盟发挥领导作用的国家，对网络空间全球治理的参与程度达到了前所未有的高度。法国政府在 2018 年推出了《网络空间信任与安全巴黎倡议》，系统阐述了法国在网络空间领域的政策立场，更多地平衡了发达国家和发展中国家的政策立场，同时对国家行为体和非国家行为体的不同理念持包容态度。德国则在慕尼黑安全会议平台上专门设立了网络安全会议，并且利用慕尼黑安全会议机制专门组织了年度性的网络安全对话，通过组织具有全球性影响的网络安全会议，增加欧盟在网络安全领域的领导力和话语权。

欧盟网络空间战略转变的动因

欧盟网络空间战略调整是其对外战略转型的延续，是“主权欧洲”战略在网络空间领域的延伸。一方面，欧盟通过不断出台战略、法律和政策，提升在网络空间领域对内和对外的权威；[10] 另一方面，网络空间地缘政治变化，如全球网络安全形势恶化、大国博弈加剧和“美国优先”政策等因素是欧盟网络空间战略转型的直接推动力量。[11]

第一，网络安全形势急剧恶化，传统手段无法有效应对新威胁与新挑战。与传统国家安全威胁相比，网络安全更加复杂，来源也更加广泛（如黑客通过综合应用窃取网络信息、社交媒体操纵等手段影响各成员国的大选），给欧盟及其成员国的安全带来了严峻挑战。传统的国家安全工具和网络安全政策都无法有效应对类似新挑战。因此，欧盟通过不断出台新政策以提升管控和协调能力，如出台《反对虚假信息行为准则》（Code of Practice Against

Disinformation），加大对社交媒体平台的监管；发布《网络安全法》，在加强欧盟层面网络安全政策协调的同时，通过欧盟网络与信息安全署来协助增强对各成员国的网络安全能力建设。[12]

不仅如此，欧盟面临的网络安全威胁也越来越多，既要打击网络犯罪组织、恐怖主义，也要防范竞争对手（如俄罗斯、伊朗），甚至连美国这样的传统盟友也给欧盟的网络安全带来了挑战。2013年的“斯诺登事件”几乎摧毁了美欧在网络安全领域的互信；2020年2月11日，美国《华盛顿邮报》联合德国电视二台（ZDF）又爆出美国中央情报局（CIA）60年来一直秘密操纵全球知名加密公司，向包括欧盟在内的盟友提供安装有后门的加密产品，以此来获取他们的安全机密。这些事件让欧盟意识到，在网络安全领域，美国并未视其为盟友，而是将自身利益凌驾于欧盟利益之上。因此，欧盟必须要提升维护自身网络安全的能力，以使网络主权不受侵犯。[13]为实现这一目标，2020年2月23日，欧盟成员国建立了新的情报合作机构——欧洲情报学院（ICE）。法国总统马克龙公开表示，这是为了摆脱对美国在信息技术领域的依赖。[14]

第二，作为整体参与网络空间领域的大国博弈。网络空间已经成为全球战略性新疆域，大国在网络安全、经济和政治等方面开展了全方位的博弈。美国、中国、俄罗斯等大国纷纷加大在网络空间治理领域的投入。相比其他大国对网络空间的重视程度，欧盟自认为已经在这场大国博弈进程中处于下风。例如，欧洲外交关系委员会研究员优莱克·弗兰克（Ulrike Franke）指出，“在慕尼黑安全会议关于人工智能、5G领域的讨论中，中美垄断了所有的议程和讨论，没有给包括欧盟在内的其他国家和国际组织留下任何空间。”[15]

因此，为改变落后状态，获取主动权，欧盟必须要整合各成员国的力量，以统一立场参与到网络空间大国博弈的进程中。欧盟发布的《人工智能白皮书》《数据安全战略》等战略性文件，均强调欧盟对成员国的统一领导，同时将中美作为人工智能领域竞争的参照对象，提出要建立欧盟在人工智能领域的全球领导权，在10年时间内将欧盟建设成为全世界最具竞争力和活力的新兴技术经济体。这就要求欧盟与各成员国加强协调，在人工智能、数据安全等领域加大欧盟层级的预算投入，制定统一的法律和标准，强化欧盟在新兴技术领域的统一领导权，克服过去由于欧盟与成员国双重治理结构导致的效率低下问题。

第三，美国网络空间战略调整迫使欧盟不得不采取更加独立自主的网络空间战略。“美国优先”不仅导致了自由主义国际秩序的消亡，网络安全领域的“大西洋鸿沟”也已经成为欧盟领导人的主要担忧之一。[16]从“主权欧洲”到数字主权和技术主权，欧盟不断对美欧之间的分歧做出政策回应，通过加大投入重新建立自己在网络领域的竞争优势。特朗普政府为维持其对新兴技术的垄断，通过修订《出口管制法案》，收紧了对国外企业和机构获取美国新兴技术产品和服务的管制。[17]在此背景下，缺乏技术主权将会使欧盟在与包括美国在内的全球大国开展竞争时处于不利地位。因此，欧盟需要通过加大在数字技术和基础设施建设等方面的投资，构建在数字经济领域的技术主权，降低对包括美国在内的全球网络技术供应链的依赖。

欧盟网络空间战略调整对中欧网络空间合作的影响

欧盟网络空间战略调整既是对全球网络空间战

略形势发展的回应，同时也表明欧盟有意重新构建网络空间领域的大国关系。欧盟更加关注网络主权，加强网络治理内部统筹协调，寻求在网络空间全球治理领域发挥领导作用等，在一定程度上为中欧在网络空间领域加强合作带来机遇。

第一，欧盟对网络空间主权进行重新定义，有助于中欧双方完善对话机制、增强合作共识。目前，中欧已经建立了三个网络对话机制，包括中欧信息技术、电信和信息化对话、中欧网络工作组和中欧网络安全与数字经济专家组等。这些机制对双方在产业和技术领域深化合作作出了积极贡献。例如，双方在中欧信息技术、电信和信息化对话框架下开展了“中欧物联网与 5G”联合研究项目，就物联网与 5G 领域的技术、产业和政策展开深入研究和分析，探索合作的潜在方式。中欧网络安全与数字经济专家组围绕中国与欧盟在网络安全、数字经济领域的法律法规、制度建设以及如何进一步推动双方在产业发展、人才培养和科学研究等方面的合作开展对话。

但是，受制于欧盟在网络空间领域排斥中方主张的网络主权观念，双方未能就网络军事、关键信息基础设施保护、数据安全等敏感议题开展深入探讨。中国与欧盟在网络主权这一核心议题上达成某种程度的共识，将会有利于双方在网络空间领域开展深入的对话与合作。一是明确国家在网络空间中的主导地位，提升国家在网络事务中的合法性和权威性，这有利于双方从政府层面加强在网络安全等复杂议题上开展合作的整体设计。二是在网络治理理念方面共同认知的扩大，可以增加双方在网络空间战略层面的互信，避免由于互信缺失而导致对对方政策的误判。三是中欧在网络空间全球治理立场方面共识的增加，有助于网络空间秩序的建立，为全球网络空间的建章立制打下良好的合作基础。

第二，欧盟对网络安全的重视程度提升，有助于中欧双方在广泛的网络安全领域深化对话与合作。一方面，欧盟新的网络安全战略调整展现出双方在网络安全领域面临的共同威胁与挑战。例如，欧盟在其《网络安全法》中将保护关键信息基础设施、保护数据安全、打击网络虚假信息列为网络安全领域面临的主要挑战，这与中国《网络安全法》中对网络安全威胁的描述一致，为双方寻求合作与共识开辟了空间。另一方面，欧盟网络安全机构职能的调整为中欧双方网络安全机构之间开展合作创造了机会。欧盟网络与信息安全署职能的扩张和资源的增长，有助于其与中方的合作伙伴中国国家互联网应急中心、中国网络安全审查技术与认证中心等机构在有害信息共享、网络安全产品和服务认证等方面开展技术层面的交流与合作。

第三，欧盟网络空间自主意识的上升，有助于维护网络空间战略稳定。网络空间大国博弈阻碍网络空间秩序构建，加剧全球网络安全形势的恶化，影响了网络空间的战略稳定。一方面，随着欧盟战略定位的变化，其在网络空间地缘政治中的地位和作用会上升，加强中欧之间的合作对于维护网络空间战略稳定具有重要价值。[18] 另一方面，网络空间领域“去美国化”已经成为中欧面临的共同课题。对欧盟而言，“去美国化”是指美国在网络空间全球治理领域的“退群”。特朗普政府上台后，取消了负责美国网络外交和国际合作的国务院网络事务协调员一职，撤并了协调员办公室；不再支持奥巴马政府一手打造的“伦敦进程”，使这一曾经在网络空间全球治理领域最重要的机制面临解体；拒绝签署法国政府提出的《网络空间信任与安全巴黎倡议》，让欧盟大失颜面。对中国而言，“去美国化”

是指美国阻断中国企业使用美国企业生产的设备、软件和技术，并且在网络战略层面对中国进行威慑和打压。可以预见，今后中欧在网络战略层面的相互需求会进一步扩大。在“去美国化”的进程中，中欧需要共同确保信息通信技术供应链的安全和完整。同时，中方也期望欧方能够顶住美国压力，平等对待华为技术有限公司和中兴通讯股份有限公司等中方信息通信技术企业，欧盟则希望中方能够给欧盟的信息通信技术产品和服务提供更大的市场便利，使其更好地分享全球最大的互联网市场红利。

欧盟网络空间战略的调整意味着中欧双方在网络治理领域的认知更加接近，网络意识形态领域的差异有所减小，建立互信的基础在增大。网络空间中“去美国化”的进程也在客观上促使中欧走近。但是，如何将这种缩小转变为促进中欧合作的动力，还需要双方采取切实的举措。中欧要以“求同存异”的精神加强对彼此网络政策的理解，以平等、合作的姿态来探索在网络安全、政治、经济、外交等多个层面的对话合作，共同维护网络空间的和平、发展与稳定。

【本文是国家社科基金一般项目“网络空间大国关系与战略稳定研究”（项目批准号：19BGJ083）的阶段性成果】

（第一作者系上海国际问题研究院网络空间国际治理研究中心秘书长、研究员；第二作者单位：中国国际问题研究院欧洲研究所）

（责任编辑：甘冲）

[1] See Thomas Renard, “EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain,” *European Politics and Society*, 19:3, pp.321-337.

[2] 汪晓风：《斯诺登事件后美国网络情报政策的调整》，载《现代国际关系》2018 年第 11 期，56-58 页。

[3] 孟威：《大数据下的国家网络安全战略博弈》，载《当代世界》2014 年第 8 期，第 66-69 页。

[4] 刘杨钺、徐能武：《新战略空间安全：一个初步分析框架》，载《太平洋学报》2018 年第 2 期，第 4-7 页。

[5] 这里的技术更多的是指以信息通信技术最新发展为代表的新兴技术（Emerging Technology），例如大数据、人工智能、云计算基于互联网产生的新技术与应用。

[6] European Parliamentary Research Service, “Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU,” 2017, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf.

[7] Convington Report, “The EU Gets Serious About Cyber: The EU Cybersecurity Act and Other Elements of the ‘Cyber Package’,” September 18, 2017, https://www.cov.com/-/media/files/corporate/publications/2017/09/the_eu_gets_serious_about_cyber.pdf.

[8] European Commission, “Proposal for the Cybersecurity Act,” September 13, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN.

[9] Khalil Rouhana, “8th EU-China ICT Dialogue,” July 11, 2017, https://ec.europa.eu/digital-single-market/en/blog/8th-eu-china-ict-dialogue-11-july-2017.

[10] 茅孝军：《从临时措施到贸易保护：‘欧盟数字税’的兴起、演化与省思》，载《欧洲研究》2019 年第 6 期，第 59-76 页。

[11] See John B. Sheldon, “Geopolitics and Cyber Power: Why Geography Still Matters,” *American Foreign Policy Interests*, Vol.36, No.5, 2014, pp.286-293.

[12] Mar Negreiro, “ENISA and a New Cybersecurity Act,” February 26, 2019, http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf.

[13] George Christou, “Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?” *Cybersecurity in the European Union*, London, Palgrave Macmillan, pp.144-147.

[14] Hina, “Officials of 23 Countries Pledge Support to Form Europe’s Intelligence College,” February 27, 2020, http://ba.n1info.com/English/NEWS/a412873/Officials-of-23-countries-pledge-support-to-form-Europe-s-Intelligence-College.html.

[15] Ulrike Esther Franke, “Europe’s Struggles to Play the Great Tech Game,” February 25, 2020, https://www.ecfr.eu/article/commentary_upstaged_europes_struggles_to_play_the_great_tech_game.

[16] See Joseph S. Nye, “Will the Liberal Order Survive?” *Foreign Affairs*, January/February 2017, pp.10-13.

[17] 鲁传颖：《中美关系中的网络安全困境及其影响》，载《现代国际关系》2019 年第 12 期，第 16-22 页。

[18] European Court of Auditors, “Challenges to effective EU cybersecurity policy,” March, 2019, https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.