网络空间大国关系面临的安全困境、错误知觉和路径选择

——以中欧网络合作为例*

鲁传颖

内容提要：网络空间大国合作不仅面临利益上的分歧，还面临更深层次的困境。网络空间作为一个新领域、新议题在认知层面对国家造成了挑战。只有在消除错误知觉、建立互信的基础上建立相应的合作和治理机制才能构建起良性的网络空间大国关系，维护网络空间稳定、和平与发展。本文以中欧在网络空间的互动为例，首先分析了大国网络空间安全困境的现状，随后深入分析了合作困境背后的错误知觉，最后提出了中欧在网络领域合作的路径选择。

关键词：中欧网络合作　中欧关系　错误知觉　网络空间治理

网络空间大国关系是物理世界大国关系在网络空间的映射，特殊的网络地缘政治属性消除了物理空间地理上的距离，增加了空间中行为体交往的频率，并且在技术上实现了全球互联网的统一，为人类的发展带来了极大的增长空间。网络空间也增加了国家之间的冲突的频度，降低了互信程度，加剧了不安全感，从而使得网络空间大国陷入了安全困境。① 中欧网络合作既受到中欧双边关系的影响，也面临大国网络安全困境的挑战。因此，研究中欧网络关系不仅对如何提升中欧网络合作具有重要意义，而且对探索构建良性网络空间大国互动模式也有一定的借鉴。

* 本研究得到教育部哲学社会科学研究重大课题攻关项目“构建全球化互联网治理体系研究”（项目编号：17JZD032）的资助。

① 参见鲁传颖：《国际政治视角下的网络安全治理困境与机制构建——以美国大选“黑客门”为例》，载《国际展望》，2017 年第 4 期，第 29-37 页。

一 中欧网络安全困境

中国与欧盟都是网络空间的重要行为体,在网络空间中互动频繁,也建立了多层次的网络对话机制,表明双方都有建立互信、增进合作的意愿。然而,中欧仍然面临网络秩序构建阵营化、信任缺失和战略猜疑等方面的挑战,从国际、双边和国内多个层面形成了网络安全困境。

(一)中欧面临网络空间国际治理困境,陷入秩序构建的阵营化对抗

秩序构建是网络空间国际治理的主要任务,也是中欧双方网络空间国际战略的重要目标。网络空间国际治理涉及网络安全、犯罪、军控、人权和数字贸易规则等多个领域。① 现实地看,中国与欧盟在上述领域既有共同利益,也难免存在分歧。如果基于务实理性的考量,中欧在网络空间国际治理中应既有合作,也有竞争。然而,实际上,几乎在所有网络空间治理领域,中欧都主动或被动陷入了西方国家与新兴国家之间阵营化的对抗进程。② 阵营化是国际关系领域常见的现象,由于发展阶段和意识形态的差异,国家往往被归为某一个阵营,如根据经济社会发展程度将国家划分为发展中国家和发达国家等。阵营的存在并不必然产生负面影响,阵营成员之间拥有共同的利益能够促成成员之间的共同立场,为谈判、协商做好准备。然而,过度的阵营化也会放大矛盾分歧,使国家间的治理合作面临低效化甚至无效化的困境。

具体而言,网络空间治理的阵营化带来了三方面的挑战。第一,阵营化会导致局部分歧的外溢,影响所有与网络相关的国际治理。一个治理议题上的分歧会影响其他治理领域,随后发生的连锁反应会使所有与网络治理相关的工作都陷入困境。目前,国际层面网络空间治理领域较有影响力的机制包括:联合国大会框架下的裁军和军控委员会(第一委员会)成立的联合国信息安全政府专家组机制,联合国司法与犯罪委员会组织的打击网络犯罪开放性政府专家组机制,联合国、巴西政府、互联网名称与数字地址分配机构(ICANN)共同举办的多利益攸关方大会(NetMundial),以及美国和欧洲国家推动的“伦敦进程”等机制。在上述机制中,一些专门针对特定领域,如信息安全政府专家组主要讨论国际法在网络空间的适用、负责任的国家行为准则和建立信任

① See Joseph Nye, “The Regime Complex for Managing Global Cyber Activities,” *Global Commission on Internet Governance Paper Series*, No. 1, 2014, pp. 5-13.

② See George Christou, “The EU's Approach to Cyber Security, EU-China Security Cooperation: Performance and Prospects,” *EUSC Policy Paper Series*, Autumn/Winter 2014.

措施三个方面。[①] 打击网络犯罪政府专家组主要负责制定全球性惩治网络犯罪的国际法律文本;另一些机制则涵盖更为广泛的议题,如多利益攸关方大会和伦敦进程的议题覆盖了从国际安全、隐私保护到能力建设等多个方面。由于网络治理阵营的分野,出现了大国在不同机制中相互制约的现象,导致网络空间国际治理进程陷入困境。例如,由于在网络空间军事化问题上中国、俄罗斯与美国、欧盟存在分歧,信息安全专家组的工作未能取得进展。中国与欧盟在打击网络犯罪的国际合作机制中也采取了不同的立场。中国支持制定全球性打击网络犯罪的国际法,却受到欧盟的抵制,而欧委会意图通过《布达佩斯网络犯罪公约》来取代联合国的作用,也受到中国的反对。多利益攸关方大会和伦敦进程因各方观点的分歧几乎失去了影响力。

第二,阵营化会引起政策的对立化。网络空间已经渗透到国家与社会生活的各个方面,各国在网络领域有不同的政策选择,差异性极大,所以很难形成统一的政策。而阵营化的存在使各方摈弃复杂多元的政策选择,为强调与对方政策的不同选择较为对立的政策,从而压缩了通过国际谈判进行协调的空间。如各国在网络空间上的基本立场分为支持"网络主权"和"网络公域",形成了国家主导的"多边谈判进程"模式和非国家行为体主导的"多利益攸关方"模式。如果深入考察中国与欧盟的政策,会发现双方虽属于不同的阵营,但在上述问题上的立场并非截然不同。中国虽然认为"多边"很重要,但"多方"的作用也不可忽视。欧盟虽然不支持广泛意义上的"网络主权"概念,但基本上认可国家在网络空间中拥有主权,对探索国家主权在网络空间中的适用也有浓厚的兴趣。然而,由于阵营的存在,中欧之间很难完全根据自身的立场来进行对话。可以说,阵营化约束了寻求共同利益的行为,缩小了双方合作的空间。

第三,阵营化会限制阵营成员依据自身利益采取立场。网络空间还处于不断的发展过程,对此,国际社会的未知大于已知。因此,不能简单沿用传统的国际政治思维来判断相关网络空间治理机制是否符合自身的利益。然而,身处特定阵营的成员,其利益判断的客观性却难免会受到阵营立场的左右。比较典型的案例是联合国信息安全政府专家组的工作。2016-2017 年,该专家组在是否赋予国家自主判定和反击网络攻击的权力问题上未能取得共识。中方明确反对网络空间军事化,反对赋予国家在网络空间合法使用武力的条款,这不仅符合中方的利益,也有利于网络空间的和平与发展。欧盟在很大程度上与中方拥有一致的利益,但由于美欧阵营的存在,欧盟受到美国影响较大,不得不支持美国的立场。专家组的失败也对欧盟在网络空间治理中发挥领导

① Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly Document A/70/174, July 22, 2015.

力的尝试造成了重大打击。[①] 本届专家组组长卡斯滕·吉尔(Karsten Geier)是德国外交部网络官员,外界普遍对他寄予厚望,希望能够通过欧盟的努力来弥合各方的政策立场分歧。而专家组未能如期发布报告,不仅使专家组组长的心血付之东流,也使得欧盟推动网络空间国际治理进程及提升自身领导力的战略未能如愿。[②]

(二)中欧双边合作面临信任不足的困境

中国与欧盟在网络领域开展了多层次的对话机制,涵盖了双方在网络空间中广泛存在的共同利益,也取得了一定的成果,并成为中欧关系中的重要组成部分。与此同时,中欧在网络领域的合作仍然面临信任不足的挑战。双方信任缺失主要表现在对话层级未能显示网络安全对中欧关系的重要性,对话成果和务实合作较少,网络对话在增信释疑、消弭误解及加强合作等方面的作用未能充分发挥。目前,中欧的网络对话分别是工业与信息化部与欧盟信息总司(DG Connect)开展的"中欧信息技术、电信和信息化对话";中国外交部与欧盟对外行动署合作的"中欧网络工作组";国家互联网信息办公室与欧盟信息总司设立的"中欧网络安全与数字经济专家组"。[③] 这三个对话机制基本上处于副部级或司局级层面。[④] 相比之下,中欧在战略、经贸以及其他全球治理领域的对话机制基本上要高两个层级。例如,中欧经贸高层对话由副总理和欧委会副主席主持,中欧高级别战略对话由中方国务委员和欧盟外交与安全政策高级代表领衔。[⑤] 显然,中欧网络对话的层级更低,使其被纳入其他对话机制而成为一个子议题,远未能反映网络对话的战略性地位。[⑥]

网络空间的战略性和不确定性也意味着信任对于合作而言具有重大意义,缺乏信任会导致双方在合作时过于谨慎,不愿展现合作意愿。因此,信任不足导致中欧双方缺乏合作动力,尤其是在一些具有共同利益的领域未能开展事实上的合作。例如,中欧双方在打击网络犯罪、反对网络空间军事化、促进数字经济贸易发展,以及加快网络安全产业、人才、技术合作等领域拥有广泛的共同利益,但却由于种种原因至今未能开

① Thomas Renard, "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain," *European Politics and Society*, Vol.19, No.3, 2018, pp.321-337.

② Karsten Geier, "Norms, Confidence And Capacity Building: Putting The UN Recommendations On Information And Communication Technologies In The Context Of International Security Into OSCE-Action," *European Cybersecurity Journal*, Vol.2, No.1, 2016.

③ 国家互联网信息办公室:《中欧数字经济和网络安全专家工作组第三次会议在比利时鲁汶成功举办》,2017 年 3 月 9 日,http://www.cac.gov.cn/2017-03/09/c_1120599476.htm,2019 年 4 月 2 日访问。

④ 中欧信息技术、电信和信息化对话中方是由工信部副部长牵头,包括工信部多个司局参与。

⑤ 中国政府网:《商务部介绍第七次中欧经贸高层对话有关情况并答问》,2018 年 6 月 21 日,http://www.gov.cn/xinwen/2018-06/21/content_5300260.htm,2019 年 4 月 2 日访问。

⑥ 新华社:《第十九次中国-欧盟领导人会晤成果清单》,2017 年 6 月 2 日,http://www.xinhuanet.com/world/2017-06/04/c_1121081995.htm,2019 年 4 月 2 日访问。

展合作。即便是完全基于利益的考量,今后双方也有必要进一步消除误解,增加互信,并在此基础上逐步加强沟通,围绕双方拥有共同利益的网络政治、经济和安全等方面的议题开展务实合作,提升中欧网络对话的有效性。

(三)中欧各自制定的网络战略,在未经充分协调的情况下加重了彼此的猜疑

网络空间拉近了国家之间的距离,增加了交往的频率。与此同时,战略与政策的外部效应也在加大,一国的网络战略和政策将不可避免对其他国家产生重要影响。这种影响如果得不到充分回应,将会加剧外部对本国战略的猜疑。伴随着中欧双方不断加快的网络战略与政策制定,彼此之间的猜疑也在不断上升。中国围绕网络强国的建设,相继出台了《国家网络空间战略》《网络空间国际合作战略》《国家信息化发展战略纲要》,并制定了《网络安全法》及配套的《网络安全审查办法》《关键基础设施保护条例》《数据出境评估办法》《个人信息安全规范》举措等。① 欧盟也先后发布了《欧盟网络空间安全战略》,通过了《网络与信息安全指令》("NIS 指令"),在数字经济层面提出建立"单一数字市场"战略,制定了《一般数据保护条例》(General Data Protection Regulation,GDPR)等。②

中欧的网络战略和政策在客观上带来了"长臂管辖"、市场准入和知识产权保护等一系列问题。如 GDPR 在实施过程中要求只要面向欧盟的用户,不管企业主体和产品是否在中国生产,都需要受 GDPR 的管辖,这就给中国带来了"司法长臂管辖"问题。同时,欧盟也认为,中国的《网络安全法》给欧盟企业在华运营带来市场准入和知识产权保护等方面的担忧。由此引发的猜忌进一步放大了对对方意图的疑虑。欧盟担心成为网络强国的中国将会给国际网络空间以及欧盟带来巨大冲击。例如,网络主权政策是否会造成互联网的分裂,以及中国是否会通过网络政策形成不公平的贸易政策等。中国也担心欧盟的相关做法是利用国内法律来影响国际规则,侵犯中国的网络主权,同时也增加了中国企业在欧盟运营的壁垒。相互之间对彼此的网络政策与战略的猜疑在今后一段时间还会持续,若不能妥善应对,将进一步影响中欧在网络空间的合作。

① 中华人民共和国外交部、国家互联网信息办公室:《网络空间国际合作战略》,新华网,2017 年 3 月 1 日,http://news.xinhuanet.com/politics/2017-03/01/c_1120552767.htm,2019 年 4 月 2 日访问。

② Iva Tasheva, "European Cybersecurity Policy – Trends and Prospects," 8 June 2017, http://www.epc.eu/documents/uploads/pub_7739_europeancybersecuritypolicy.pdf, last accessed on 7 April 2019.

二 网络安全困境中的错误知觉

中欧网络安全困境揭示了双方面临巨大的合作挑战,但也反映了中欧之间的问题并非结构性矛盾,导致困境的原因主要是双方对国际层面的网络空间秩序构建、双边信任,以及对对方政策意图的理解等方面存在一系列的错误知觉。下文拟从决策者的传统思维定式导致的错误知觉以及网络空间的新特性放大错误知觉两方面进行分析。

(一)思维定式导致的错误知觉

从中欧在网络空间中的互动可以看出,一系列的错误知觉影响了决策者的认知,增加了双方合作的障碍。网络是国际关系中的新兴议题,一方面,它所展现出来对国际体系和国家战略的颠覆性影响使决策者将面临更复杂的决策环境;另一方面,作为中欧关系中的新问题,如何客观地认知网络问题,并制定相应的政策举措也增加了决策者面临的挑战。决策者倾向于用传统的思维定式来理解网络空间,包括使用既有的理论、固化的知识框架、固有的观念等来解释网络空间中国家的行为和意图是产生错误知觉的主要原因。①

第一,以原有理论理解网络空间导致的错误知觉。理论通过对复杂现象进行抽象和逻辑推理,能够帮助决策者更好地理解决策环境,制定长期战略。换而言之,理论是一种简约,可以在纷繁复杂的现象中寻找变量之间的逻辑关系,并且屏蔽干扰因素。②在正常情况下,当旧的理论不能解决更多和更加重要的问题的时候,就失去了解释力,但理论的追随者却不愿轻易放弃,他们认为,“业已建立的理论如此成功地解释了许多现象,促进了如此多的新知识……放弃这些理论会造成极大的损失,而且坚信这些理论有能力解释比较麻烦的新现象。”③不同的理论会产生不同的知觉,原有的理论会使决策者不自觉地忽视重要的、有价值的信息,从而产生了认知的误差,并制定不明智的政策。④

网络空间的战略性和复杂性恰恰需要新的理论来辅助决策者对其进行解释,但由于这一领域影响范围太大,演变速度太快,使得新理论的构建速度远远跟不上实践的

① 参见[美]罗伯特·杰维斯:《国际政治中的知觉与错误知觉》,秦亚青译,世界知识出版社 2003 年版,第 112-205 页。

② 参见[美]詹姆斯·多尔蒂、小罗伯特·普法尔茨格拉芙:《争论中的国际关系理论》,阎学通、陈寒溪等译,世界知识出版社 2003 年版,第 18-24 页。

③ [美]罗伯特·杰维斯:《国际政治中的知觉与错误知觉》,第 168 页。

④ 同上书,第 140-172 页。

发展。当缺乏新的理论来解释新现象时,决策者往往会基于原有的理论来进行解释。① 比较典型的就是用地缘政治理论来解释网络空间大国关系。② 网络空间秩序构建的阵营化思维明显受到地缘政治理论的影响,各国自然而然地把自己划归到特定的阵营,并且认为只有这一阵营提出的治理理念和方法才有利于自身的利益。从理性认知的角度来看,中国与欧盟并非网络领域"中俄阵营"与"西方阵营"的主导者。③ 即便在所谓的阵营内部,各国之间也存在很大的差异。从国家利益的角度来看,阵营之间的界限与国家的身份之间并不匹配。欧盟与美国在网络空间军事化上存在根本性的分歧,"斯诺登事件"表明美国并不信任欧盟,并且损害了欧盟国家的国家安全。美欧在网络军事力量的发展上也不存在一致的利益。美国为了追求在网络空间的霸权推动网络空间的军事化,不仅会给欧盟带来安全隐患,也会导致其被动卷入网络军备竞赛中。④ 同理,中国与俄罗斯虽然在网络领域的合作很多,但双方对现存网络空间治理体系认知上存在较大差异,俄罗斯寻求推翻或者另建一套互联网体系。⑤ 中国的诉求是在现有体系下推动变革,让其更加多边、民主和透明。⑥ 但是,地缘政治思维会让中欧轻易做出选择,并且相互把对方归为某一阵营,从而过滤了各方在网络领域不同的政策立场,增加了错误知觉。⑦

决策者使用地缘政治理论来解释网络空间国家行为的更深层次原因是为了寻求认知相符,比如倾向于认为我们喜欢的国家会做我们喜欢的事情,如果一个国家是我们的敌人,它提出的建议一定会伤害我们,一定会损害我们朋友的利益。⑧ 由于中国与俄罗斯是网络空间的朋友,自然就是欧盟的敌人;反之,欧盟与美国的盟友关系也导致中国在网络治理中对欧盟存有戒心。任何一方在网络领域的行动都会加深这一认知。如中俄加强在网络安全领域的合作就会引起欧盟的警惕。同理,北约开展的网络

① [美]罗伯特·杰维斯:《国际政治中的知觉与错误知觉》,第 140-141 页。

② See John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," *American Foreign Policy Interests*, Vol.36, No.5, 2014, pp. 286-293.

③ Andrey Krutskikh, "Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere," June 29, 2017, http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288, last accessed on 2 April 2019.

④ George Christou, "Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?" in George Christou, *Cybersecurity in the European Union*, Palgrave Macmillan, 2016.

⑤ 班婕、鲁传颖:《从"联邦政府信息安全学说"看俄罗斯网络空间战略的调整》,载《信息安全与通信保密》,2017 年第 2 期,第 81 页。

⑥ Lu Chuanying, "China's Emerging Cyberspace Strategy," May 24, 2016, *The Diplomat*, https://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/, last accessed on 21 March 2019.

⑦ 参见[美]罗伯特·杰维斯:《国际政治中的知觉与错误知觉》,第 120-122 页。

⑧ 同上书,第 113 页。

军事演习也会引起中国的高度关注。实际上,现阶段的网络攻击更多的是由非国家行为体和恐怖主义分子实施。而网络军事演习更多的是为了提升网络安全能力,增加网络安全的韧性,对他国的针对性并没有那么明显。地缘政治理论认为,中国与俄罗斯的合作会增加欧盟对中欧合作的担忧,美国与欧盟以及北约的合作也会增加中国对欧盟的不信任感,这种错误知觉阻碍了中欧在网络领域的合作。

第二,用固化的知识框架理解对方政策产生的错误知觉。认识框架一旦建立起来,人们就会顽固地坚持自己的认识,即便事后证明事实与他们的认识截然相反。[①] 在面对网络这一新议题时,决策者需要不断更新知识框架,才能更好地应对新挑战。在实践中,建立客观认知网络空间的知识框架面临多重挑战:一是网络技术专业性带来的挑战;二是理解网络议题时需要跨学科的知识框架带来的挑战,大多数网络议题涉及的都是跨领域的,需要有外交、经济、法律和安全等不同领域的知识才能完整地理解问题;三是理解对方决策体制的困难。在涉及网络政策时,各国往往都有自己的政策实践,在决策体制、理念和原则上各不相同;即使在国内层面,也面临"九龙治水"的问题,各部门具有不同主张。[②] 在双边层面的对话中,决策者对对方网络政策的决策机制、理念和原则的理解不足经常成为阻碍对话有效性的障碍。当无法构建合理的认知模式时,为了达到认知平衡,决策者会不自觉地运用已有的知识框架来试图理解新问题;[③]在网络领域通常表现为为了寻求物理世界与网络世界的认知平衡,倾向于用物理世界建立的知识框架来理解网络空间的问题。

在中欧网络对话中,经常会出现类似的错误知觉。一方面,双方对对方网络领域的决策体制缺乏了解,不清楚不同政府部门之间的角色。如欧盟的学者和官员就曾反复询问中国的国家互联网信息办公室在网络领域究竟扮演什么角色,并经常会认为其仅仅是一个宣传部门。中国的决策者对欧盟复杂的网络决策体系也不是特别清楚,如欧盟与成员国之间在网络政策领域各有哪些职能,又是如何协调的,等等。尽管双方在对话中都进行了解释,但效果并不明显。双方的决策者还是倾向于用自身的经验去理解对方的决策体制。另一方面,由于网络空间还在不断演进,国家在制定相应的战略和制度时需要对各种情况进行权衡。如《网络安全法》是中国维护网络安全、国家安全的基础性法律,是对多方利益的平衡,例如安全与发展、开放与自主,但其真正的实施需要在实践中进行探索完善,也需要相应的配套措施。从欧盟的角度来看,很难

① [美]罗伯特·杰维斯:《国际政治中的知觉与错误知觉》,第140页。

② 周秋君:《欧洲网络安全战略解析》,载《欧洲研究》,2015年第3期,第77页。

③ See Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare*, Vol.15, No. 2, 2016, pp.66-73.

理解这种平衡,更多的是基于对自身法律的理解来看待中国的法律,过度夸大相应条款对其造成的影响。① 由于对对方决策体系和机制缺乏理解,把对方网络政策视为统一的、经过谋划的策略,从而导致了误解的加深,这显然不利于双方的合作。

第三,用固有观念解释网络空间战略形成的错误知觉。固有观念是对事物采取先入为主的看法,并在长期互动过程中形成的观念,一旦形成就很难改变。在国际关系中,观念的意义还包括意识形态、价值观和身份认同等深层次的因素。欧盟与中国在政治体制、主权和人权等领域都已形成了一系列的观念。这些固有观念有时会成为双方理解对方网络战略的障碍,比如先入为主地从固有的观念来演绎和理解对方的网络战略,忽略许多重要的信息,从而形成错误的知觉。如欧盟认为,中国对网络主权的强调是要分裂互联网,造成网络空间"巴尔干化"。这种观念反映了欧盟将中国视为所谓"威权体制"的延伸。实际上,中国提出网络主权不仅是为了捍卫国家的主权权益,也是为了维护网络安全的需要,特别是在"斯诺登事件"之后,中国作为受害者对网络主权受到侵犯更加敏感,希望能在国际法层面得到安全的保障。此外,中国不仅强调网络主权,同时也强调建立网络空间命运共同体,但并未受到应有的关注。在双边对话合作中,中国提出的网络主权主张被欧盟持有的"威权国家"的固有观念进行了刻板的解读,忽视了其丰富、广泛和平衡的内涵。

欧盟传统上认为中国是一个强政府、弱公民社会的国家,政府加强网络管理的任何政策都会引起欧方从人权角度的批评。在双边合作中,一旦有了这样的思维定式,就会对其他领域的合作产生影响。固有观念还体现在对对方网络政策的认知上。在看待双方的网络政策目标时,对自己的政策总能找出合理的解释,对对方同样的政策却有不同的看法。这种双重标准的认知障碍被带入网络领域。欧盟认为自己加强数据安全的保护是为了保护人权和隐私权,而中国加强数据管理则是为了强化监控,尽管双方的管理政策客观上都会给企业带来成本的增加和商业模式上的挑战,但是前者是合理、合法的,后者的政策则会受到人权和市场两方面的质疑。从中方的角度来看待欧方的政策,也会简单地使用"双重标准"这一固有观念来理解欧盟的对华网络政策,缺乏对"双重标准"背后深层次原因的分析和认识。实际上,欧洲社会对隐私的诉求很大程度上源自对纳粹大屠杀以及苏联极权时期的集体记忆,即政府对私人信息的滥用给社会带来的巨大灾难。② 欧盟的做法在某种意义上也是平衡社会的关切和经

① Sui-Lee Wee, "China's New Cybersecurity Law Leaves Foreign Firms Guessing," *The New York Times*, May 31, 2017.

② See F. Bignami, "European versus American Liberty: A Comparative Privacy Analysis of Anti-terrorism Datamining," pp.609-688.

济发展。例如,在GDPR生效的第一天,欧盟委员会官方推特就发布了一条消息,“欧洲的数字主权回到了欧洲人手里”。此外,欧盟一方面在国际上高调批评中国的网络内容管理政策,自身却建立了多部法律和使用多种手段来应对网络舆情挑战,特别是在虚假新闻、外国信息干预等方面制定了多部相关法律。这一系列做法的背后反映了欧盟内部政府与社会之间的不同关切。用双重标准这一固有观念去解释欧盟看似矛盾的行为与中方的认知体系更加相符,但却忽视了欧盟作为后现代国家组织的根本特性,从而影响了双方在网络领域的合作。

(二)网络空间新特性导致的错误知觉

网络空间给国际关系和国家战略带来的颠覆性变化在挑战决策者的认知,也是影响中欧在网络空间中合作的重要变量。网络技术的进步、应用的渗透在不断推动网络空间的演进。这种演进具有双重含义:一方面,大数据、人工智能、物联网和云计算等新科技,即所谓“大智物云”在不断推动网络空间自身的变化;另一方面,新科技也在推动网络空间与物理世界进行深度互动,不断地颠覆物理世界中建立的秩序、规范和伦理。这一过程引发了国家对网络安全的焦虑以及对伦理问题的担忧,也带来了身份认同的困惑,很多错误知觉由此产生。

第一,安全焦虑引发的错误知觉。越来越多的网络安全事件的发生加剧了国家对网络安全的关切,也加大了资源的投入。网络安全与传统安全相比具有泛在性、虚拟性(测量难)和抵赖性(核查难),给国家带来了认知挑战,容易引发安全焦虑。网络空间的基础是由人编写的代码,这就导致了网络安全具有泛在性,即所有的设备都有可能面临未知的安全漏洞,从而被对手利用开展网络攻击。以美国国家安全局、网络司令部为代表的国家安全机构对“零日漏洞”的囤积加剧了各国政府对国家安全、经济发展和社会稳定所高度依赖的网络设备安全性的担忧。网络武器的虚拟性导致决策者无法对对手网络武器库的规模、先进程度及危害程度等获得准确的答案,从而放大了国家的不安全感,产生新的安全焦虑。此外,网络的隐蔽性、匿名性和跨国界增加了对网络攻击溯源的难度,因此,发起网络攻击的国家可以轻易对其行为进行抵赖。① 从已有的网络安全案例来看,国际社会与当事方围绕溯源问题产生纠纷,无法确认攻击者身份,导致其无法受到应有的惩罚,受害者也无从维权,从而进一步放大了国家对于网络安全的焦虑。

安全焦虑增加了理性决策的难度,决策者也容易放大自身面临的网络威胁,夸大对手的实力以及给自身带来的威胁,在双边的互动中易于向对方提出过高的要求而不

① See Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” pp.4-37.

轻易做出让步,最终导致政策的误判。在中欧网络对话中,欧方就曾要求中欧双方参照中美在打击网络攻击行为和网络商业窃密的声明,开展类似合作。对中方而言,中欧之间并不存在所谓的网络商业窃密问题,签署类似的声明毫无必要。对此,前德国驻华大使柯慕贤曾公开抱怨,指责中国缺乏对话意愿,导致相关对话未能如期开展。中国外交部也进行了反驳,认为其讲话不符合事实,颠倒黑白。① 欧方的政策反映了其在网络安全领域的焦虑情绪,对中欧之间的网络合作和对话产生了很大的负面影响。

第二,伦理担忧产生的错误知觉。网络空间崛起推动人类社会从工业社会向信息社会和智能社会转型。网络时代的数字经济范式与工业文明下建立的经济、法律和政治制度产生了新的冲突,引发了在伦理层面对数字经济发展导致的个人隐私保护、算法歧视、机器取代人类等伦理现象的担忧。各国政府纷纷从法律、规范和标准等相应的公共政策入手来应对这些问题。伦理问题不仅是中国与欧盟各自网络政策的重要领域,同时也是中欧网络合作面临的重要挑战之一。双方都面临各种担忧,如欧盟认为,中国的网络政策对伦理关注程度不够,而中国认为,欧盟会利用伦理借口来限制中国的发展。处理好伦理问题对新技术的应用具有重要意义,但网络空间中伦理的内涵和标准还处于非常模糊的境地,包括中欧在内的各方还存在不同的看法。例如,隐私问题是数字经济时代最重要的伦理问题之一,但隐私保护与数据利用之间的平衡点没有明确的界限,过度的隐私保护会限制数字经济发展。同理,人工智能的发展不仅会提高劳动生产率,也会取代人类的就业,决策者也面临选择的难题。

中欧双方在伦理以及围绕伦理产生的一系列法律、规范和标准等问题上的差异成为双方合作今后面临的挑战。欧盟于 2018 年 5 月实施的《一般数据保护条例》被认为是全球最严格的数据保护政策,它对数据跨境流动做了相关的要求,明确表示对数据伦理问题的关注。欧盟要求数据接收方必须“尊重人权和基本自由、相关立法、独立监督机构的存在和有效运作,以及第三国或国际组织已签订的国际承诺”。在物理世界中,中欧对人权的理解存在一定的分歧,这会进一步加剧双方在伦理问题上的分歧,也会对今后中欧在数据保护和数据跨境流动方面的合作带来疑虑。伦理问题在中欧之间会长期存在,随着数字经济的发展,双方企业进入对方市场会更加频繁,对双方企业的产品和服务的伦理关切也会成为政府博弈的重点。

第三,身份认同产生的错觉。在网络空间中,国家面临与其他行为体之间的身份认同挑战。国家与其他行为体之间究竟是平等的关系,还是管制与被管制的关系?如

① 青木:《外交部批德国驻华大使涉华不当言论:颠倒黑白》,载《环球时报》,2017 年 12 月 28 日。

果视角定位不同会直接影响政府看待自身在网络空间中的身份差异。网络空间中存在众多的行为体,包括国家、互联网社群和私营部门等。① 社群和私营部门在网络空间创造和发展过程中扮演着重要角色,而国家在某种意义上是网络空间的后来者。② 例如,一系列以 I 为开头的互联网国际组织(如 ICANN、IETF、IAB、ISOC 等)被称为互联网社群的国际组织设计了互联网的整体架构、发明了基础协议,并一直掌管着互联网关键资源的分配。这就产生了两种不同身份认同的观点:一种认为在网络治理中国家与其他行为体是平等的,即所谓"多利益攸关方"模式;另一种观点尽管认可互联网社群和私营部门的作用,但强调政府应发挥主导作用。欧盟更倾向于采取"多利益攸关方"模式,中国则更青睐政府主导的多边模式。③

两种不同的身份认同对中欧网络对话交流带来了障碍。例如在中欧网络安全与数字经济工作组中,中方希望能够与欧方在战略层面就网络安全与数字经济问题进行对话。但在实际对话过程中,欧方遵循多利益攸关方模式,邀请了诸多私营部门代表参与甚至主导对话,特别是在华经营的企业,希望能够通过对话解决欧方个别企业在华经营中遇到的一些具体问题。这使得双方难以就影响双方网络关系总体局面的战略性议题进行深入对话。这种身份的错觉解释了双方现有对话中出现的"不相称"现象,中方希望能够通过政府间的合作来推动双边合作,欧盟则希望搭建平台来使市场和非政府组织开展对话合作。实际上,"多方"与"多边"不应成为合作的障碍,中欧可以通过对话机制的设计加强协调,在不同的议题中采取不同的对话形式,从而避免网络空间中政府和非政府的身份认同给双方合作带来障碍。④

三 以多层次的合作举措应对错误知觉

错误知觉对于构建良性的网络空间大国关系产生了干扰,影响了中欧在网络领域的合作。因此,中欧在开展网络合作时,应着重消除错误认知,建立双方在网络领域中的信任。同时,加强对话机制的设计,有针对性地增加合作性举措,以此为基础,构建合作共赢的中欧网络关系,为探索网络空间大国关系良性互动做出示范。

第一,积极消除中欧网络互动中出现的错误知觉。随着网络安全、数字经济的战

① See Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization*, Vol.52, No.4, 1998, pp.887-917.

② Laura DeNardis and Mark Raymond, "Thinking Clearly about Multi-stakeholder Internet Governance," Paper Presented at Eighth Annual GigaNet Symposium, November 14, 2013, pp.1-2.

③ See Laura DeNardis, *The Global War For Internet Governance*, Yale University Press, 2014, pp.20-25.

④ 参见鲁传颖:《网络空间治理与多利益攸关方理论》,时事出版社 2016 年版,第 91-99 页。

略性意义不断提升,网络议题在中欧关系中的比重将会不断增加,消除误解、增加合作符合双方的共同利益。首先,要建立理性的中欧网络知识框架。这可以帮助决策者避免受到思维定式和错误知觉的影响,更加客观地看待对方的网络政策和更准确地研判对方的政策意图。① 中欧在物理世界的战略、经济、政治和安全领域建立的知识框架难以简单适用于网络空间,还需依据网络空间的特殊属性来构建更具有解释力的认知框架。例如,网络安全是全球共同面临的长期威胁,中欧网络安全合作应充分考虑网络安全的泛在性、全球性等特点,重点关注双方在保护金融、能源和交通等全球关键基础设施安全上的共同责任。上述关键基础设施一旦遭受攻击将会给包括中欧在内的全球经济带来重大危害。网络武器的易扩散性、暗网交易的隐秘性使各国在打击网络恐怖主义、网络有组织犯罪等方面面临很大的技术性挑战,需要加强在技术、执法和信息共享等领域的深度合作。② 许多恐怖分子和犯罪组织正是利用了国家间合作困境来规避打击。例如,欧盟的犯罪组织在中国设立服务器来攻击欧盟国家的网络,或是中国的恐怖分子、犯罪组织在欧盟国家设立针对中国的网络犯罪中心等。构建基于网络属性、特性的知识框架对决策者更好地理解中欧网络关系具有重要作用。

此外,网络议题还需具有动态性、实时性和全局性等特点,出现的问题往往复杂多变,从而增加了决策者的认知难度。智库和研究机构提供的“智力支撑”在辅助决策者建立理性的认识框架上具有重要作用。目前,中欧网络领域有大量的问题需要研究,但学术界对此的关注程度却并不高,高质量的研究报告和论文寥寥无几,未能给决策者提供足够的知识。因此,双方的学术机构应加大对中欧网络事务的关注程度,围绕中欧双方的共同利益和网络空间国际治理形势开展合作研究;在理论层面加强对网络空间统一的术语体系、网络空间战略稳定机制、国际法在网络空间上的适用等方面的深入研究。这不仅有助于决策者更加系统地理解网络空间的复杂性和深刻性,同时也能克服双方思维定式导致的错误知觉。在战略层面,双方智库和研究机构可以加大对网络主权、数据主权以及网络空间命运共同体等双方网络空间战略中具有基础性作用的领域的研究,帮助决策者更好地理解对方的决策过程和主要关切。在具体政策层面,可以加大对建立信任措施、保护关键基础设施、数据安全以及负责任国家行为准则等领域的合作路径的研究,为决策者提供一个较为具体、可落实的合作框架。上述研究取得的成果对构建中欧之间客观、理性的知识框架具有重要的参考价值。

其次,要建立更多的信息交流渠道来消除错误知觉。“理智决策……需要主动寻

① 参见[美]罗伯特·杰维斯:《国际政治中的知觉与错误知觉》,第 114-160 页。

② See Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” pp.4-37.

找信息。如果不能捕捉到明显重要的信息,就会导致非理性的信息处理。”①特别是在网络这一错综复杂的领域,需要中欧双方加强有效沟通,通过对话来获取更多的有价值信息,为理性决策提供依据。现有的中欧网络对话机制与其他领域的政府间对话机制一样,往往采取高峰论坛、圆桌对话等方式。作为典型的政府间对话模式,上述对话机制还不能完全满足网络领域的信息供给。由于网络涉及的议题十分广泛,有大量需要沟通的领域,但对话的参与部门和人员毕竟有限,许多重要的部门和工作人员无法在圆桌和高峰对话中开展有效交流。因此,双方可以探索建立合作点名录,将双方网络领域的负责任对等列入名录,并且为工作层面的对话交流提供指导框架,形成有效的信息交流的制度保障。此外,由于网络的技术性特征强,双方需要的信息获取不仅包括相互了解,还包括一些技术层面的执法信息、情报信息的共享。例如,对网络攻击的调查工作应实时展开,相关有价值的信息也应快速共享。就像地震过后,抢救受害者有“黄金时间”一样,网络攻击的取证工作也会伴随着时间的消逝出现价值递减。一般各国在国内调查时采取 7/24 的应急响应机制,但涉及跨国合作时,往往通过传统外交或国际合作机制,需要国际、国内多个部门之间的审批,基本无法达到有效信息共享。中欧可在双方负责网络安全的机构中建立相应的信息共享机制,如中国的公安、网信部门与欧盟警察、数据保护等机构之间建立专门的网络信息共享机制。

最后,通过加强议程设置来消除错误知觉。网络具有议题广泛、行为体多元的特点,加之欧方有支持“多利益攸关方”治理模式的传统,企业、互联网社群都试图根据自身的利益来影响中欧在网络领域的合作,从而增加彼此合作的协调难度。这就需要双方政府掌握对中欧网络议程设置的主导权,避免受“众声喧哗”的干扰,明确双方合作的战略方向,框定合作的内容,引导企业、互联网社群积极参与,并在合作中寻求利益保障。网络议题的对话十分专业,也极为广泛,在物理世界数字转型的大背景下,几乎所有的议题都可与网络相关。所以议题的选择和范畴对对话合作的有效性而言具有重要意义。具体而言,一方面要为双方的企业、机构之间的交流合作提供对话平台;另一方面,对中欧在网络领域的合作要有全局性的掌控力。特别是避免双方在人权、自由、知识产权保护等物理世界的分歧,影响中欧在网络领域的合作。因此,中欧双方的对话议题,应尽量围绕网络空间中出现的新问题、新机遇开展,而非将原本在物理世界就分歧很大的议题拿到网络领域进行讨论。如双方在构建数字贸易规则、保护全球关键基础设施领域、负责任的国家行为准则等领域合作的可能性,要远远大于意识形

① [美]罗伯特·杰维斯:《国际政治中的知觉与错误知觉》,第 175 页。

态等双方长期以来具有很大分歧的领域。

第二,通过在重点议题中的相互理解来建立信任。中欧网络关系中有一些关键的议题对于双方建立互信具有重要意义,如国际法在网络空间适用的问题、打击网络犯罪的全球性法律文本协定等。网络空间国际法不仅是欧盟关注的重点议题,也是中国高度重视的领域,中欧之间可以就网络空间国际法领域涉及的重要议题如网络主权、人权问题开展更多的对话。① 妥协和合作是外交谈判永恒的艺术。在物理空间中,国际社会在主权和人权问题上也存在并不完全一致的看法,《联合国宪章》和《联合国人权公约》作为两份重要的国际法准则也有着不同的侧重。中欧可以通过加深相互理解,推动在网络主权和网络人权问题上取得平衡。此外,中欧还可以围绕打击网络犯罪的国际立法进程开展合作,探索如何在"联合国打击网络犯罪政府专家组"和"布达佩斯网络犯罪公约"之间取得共识。双方可以探讨将"布达佩斯网络犯罪做公约"的一些重要条款作为专家组机制的谈判基础,也可以将欧盟在打击网络犯罪领域的实践作为联合国开展全球性打击网络犯罪能力建设的基础,探索将区域性公约在文本和实践领域与联合国的合法性、程序正当性结合,为打击全球网络犯罪做出贡献。此外,在反对网络空间军事化领域,加强联合国在网络安全溯源等方面的合作,中欧双方立场相近,可以共同推动联合国和区域性组织发挥积极作用,为国际社会提供维护网络空间和平稳定的制度方案。

第三,通过网络领域的务实合作增加共识。双方政府在发挥战略协调作用的同时,还要为彼此的网络安全产业、技术和人才提供交流的平台,为双方数字经济发展创造机遇。如为了应对网络安全人才的稀缺性问题,中欧双方可积极推进网络安全领域的人才交流与合作,成立相应的网络人才合作工作组。中方近年来开展了网络安全一级学科和建设一流网络安全学院的发展计划,这在全球具有一定的创新性,中欧双方可围绕网络安全的高等教育开展合作,鼓励双方的网络安全学院加强机制性合作,互派访问学者,交流学生。② 此外,中欧双方都有针对网络安全意识的活动,如中国的网络安全宣传周和欧洲的网络安全月。双方开展了许多类似的活动,可进一步加强这些机制之间的合作。目前,中方的网络安全宣传周邀请了大量来自欧洲的官员、学者和企业参与,欧方也可采取同样的举措,邀请来自中方的官员、学者和企业参与欧方网络安全月相关活动。

① See Madeline Carr, "Power Plays in Global Internet Governance," pp. 640-659.

② 中央网络安全与信息化领导小组办公室秘书局、教育部办公厅:《关于印发"一流网络安全学院建设示范项目管理办法"的通知》(中网办秘字〔2017〕573 号), 2017 年 8 月 14 日。

四 结语

网络空间的崛起推动着人类社会从信息化、数字化向智能化转型,并不断颠覆现存国际秩序的基础,国家在网络空间的实力对比已成为决定未来国际力量格局和治理体系演变的核心要素。中欧网络关系在这一宏大的变革趋势中面临重要抉择:是继续在错误知觉的影响下不断重复困境,还是努力建立客观的认知模式,通过多层次的合作举措将中欧网络关系打造为大国关系中的典范?

在当前国际体系大变局中,中欧作为网络大国和重要行为体具有重要的影响力。中国与欧盟分别围绕《网络强国战略》与《数字单一市场》开展战略布局,未来中欧双方在战略层面是相互借力还是相互抵制,不仅对各自战略的实施产生影响,也会对未来的国际体系产生影响。欧盟通过GDPR已经打响了维护数据主权、建立数据保护规则的第一枪。《网络安全法》以及网络强国战略也在不断提升中国在网络空间的影响力与话语权。在中美、美俄、俄欧网络关系受到各种因素制约的背景下,中欧可通过合作为网络空间提供制度保障,引领网络空间治理体系变革,为网络空间的稳定、和平与发展奠定基石。网络领域的合作将会推动中欧关系的深入发展。网络空间正处于与物理空间深度融合的阶段,对政治、经济、安全、技术、教育和人文等多个方面产生重要影响。中欧若能在网络空间合作中取得进展,不仅有助于缓解双方在意识形态、政治制度领域的分歧,更会深化双方在现有的战略、经济、安全和文化领域的合作。网络空间不仅是物理世界在网络中的映射,也代表了未来国际社会的发展方向,其重要意义不言而喻。2019年4月9日发布的《第21次中国-欧盟领导人会晤联合声明》再次将网络议题置于重要位置,提出要共同维护网络稳定,探讨国际法、国际规范在网络空间的适用,并在打击网络空间恶意活动和保护知识产权等领域加强合作。① 双方领导人对网络问题的重视程度不断上升,这将有助于双方实施更丰富的合作举措、构建良性的中欧网络关系。总体而言,加强中欧网络合作有助于国际体系的安全和网络空间的稳定繁荣,是建立面向未来的中欧关系的重要基础。

(**作者简介**:鲁传颖,上海国际问题研究院网络空间国际治理研究中心秘书长、副研究员;**责任编辑**:张海洋)

① 新华社:《第二十一次中国-欧盟领导人会晤联合声明》,2019年4月9日,http://www.xinhuanet.com/world/2019-04/09/c_1124345605.htm, 2019年4月10日访问。