第 27 卷 第 11 期 太 平 洋 学 报 Vol. 27, No. 11
2019 年 11 月 PACIFIC JOURNAL November 2019

DOI: 10.14015/j.cnki.1004-8049.2019.11.007

鲁传颖 "试析中欧网络对话合作的现状与未来",《太平洋学报》,2019 年第 11 期,第 78-88 页。

LU Chuanying, "Current Situation and Prospect of China-EU Cyber Dialogue and Cooperation", *Pacific Journal*, Vol. 27, No. 11, 2019, pp.78-88.

试析中欧网络对话合作的现状与未来

鲁传颖[1]

(1.上海国际问题研究院,上海 200233)

摘要: 中欧网络对话合作是中欧关系的组成部分,对全球网络空间的安全、发展和治理有着重要意义。双方在网络领域业已开展了多领域、跨议题的对话合作,并取得了丰硕的对话成果,与此同时,战略定位有待进一步提升、信任缺失和机制设计不足等问题也逐步显现。从更深层次原因看,其中不仅有传统地缘政治的影响,更反映出双方在网络空间的战略认知、网络政策的决策体系方面存在一定的差异。未来中欧在网络领域的对话合作要克服客观存在的差异,建立互信,取得务实成果,就需要双方进一步确定网络合作的战略定位,完善机制设计,注重议程设置,以塑造一种建设性、面向未来的中欧对话合作图景,展现中欧网络对话合作在网络空间大国关系和全球治理中的示范、引领作用。

关键词: 中欧关系; 网络安全; 网络空间治理

中图分类号: D81 **文献标识码:** A **文章编号:** 1004-8049(2019)11-0078-11

大数据、人工智能、物联网和云计算(大智物云)等信息通信技术的发展使得各国在网络空间中的联系越来越紧密,国家间的物理疆界越来越模糊,由此带来了越来越多的网络安全和发展方面的挑战。[①]如"斯诺登事件"所揭示,网络安全已成为国际安全中风险危害程度和不确定性最高的领域之一,现有的国际安全体系难以应对该挑战。[②]各国政府为了应对网络安全挑战所采取的单边行动,如发展"网络部队"、进行"网络安全审查"、制定"数据本地化"政策等,在缺乏协调的情况下,不仅未能解决网络安全问题,还给现有国际经济和贸易体系带来了挑战,有可能进一步造成网络空间的"巴尔干化"。[③]

在这一大背景下,大国之间的双边对话合作成为影响网络空间和平、发展、稳定的重要因

收稿日期: 2019-05-08; **修订日期:** 2019-09-25。

基金项目: 本文系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"(19BGJ083)的阶段性成果。

作者简介: 鲁传颖(1983—),男,安徽芜湖人,上海国际问题研究院副研究员,法学博士,主要研究方向:网络安全、网络空间治理。

* 感谢《太平洋学报》编辑部和匿名审稿专家提出的建设性修改意见,文中错漏之处由笔者负责。中国国际问题研究院范郑杰对本文亦有贡献。

① Roger Hurwitz, "Depleted Trust in the Cyber Commons", *Strategic Studies Quarterly*, Vol.6, No.3, 2012, pp. 21-23.

② Panayotis Yannakogeorgos and Adam Lowther eds., *Conflict and Cooperation in Cyberspace*, Taylor & Francis Group, 2014, pp. 50-66.

③ Mar Negreiro, "ENISA and A New Cybersecurity Act", *ERPS Briefing*, February 26, 2019, http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

素。中国与欧盟作为网络空间的重要行为体，是构建网络空间全球治理体系的重要力量，前者是网络空间中发展最快的新兴力量，后者拥有最高的互联网普及率并在积极推进数字单一市场建设。加之中欧之间不存在直接地缘政治冲突，因此从整个网络空间全球治理格局来看，中欧在维护全球网络安全、推动网络空间发展、构建网络空间秩序方面有巨大的合作空间。中欧双方已在网络安全、发展、治理等多个领域、不同层面开展了内容丰富、议题专业的对话合作，在全球大国网络合作中堪称独树一帜。然而，相较两者自身的体量、地位和影响力，两者在其传统领域合作的层级、成果和影响力，以及双方与其他国家之间开展的网络合作，中欧之间的网络合作无论是在双边层面还是在全球治理层面都仍存在较大的提升空间。如果双方能够在内部网络政策制定加强沟通协调，将有助于中欧在技术、产业方面开展更加密切的合作; 双方若在国际战略层面进一步建立信任，缩小在基本原则、政策主张方面的差异，则会有助于推动网络空间全球治理“建章立制”的进程。研究中欧在网络领域的对话合作现状，分析对话合作背后存在的问题，探索如何克服这些障碍，不仅对中欧进一步提升网络领域的合作效率具有一定意义，对网络大国之间如何携手应对全球网络安全挑战、深化数字经济合作、探索构建全球网络空间治理体系也有参考价值。

一、中欧网络对话合作现状

目前，中欧网络对话合作领域主要建立了三个对话机制，分别为中欧信息技术、电信和信息化对话，中欧网络工作组，中欧网络安全与数字经济专家组。这三个对话机制分别定位为互联网技术发展与应用、网络空间国际治理和国内网络政策领域。

1.1　中欧信息技术、电信和信息化对话

中欧双方在互联网领域的合作历史悠久。中国在 1994 年正式全功能接入互联网之前，就是通过德国科研机构的网关与互联网进行连接，中国国家顶级域名服务器最初也是由德国卡尔斯鲁厄大学运营。1997 年，中国向世界发出的第一封电子邮件“越过长城，走向世界”，也是最先发给了卡尔斯鲁厄大学的维纳·错恩教授。① 中国与欧盟国家在互联网发展历史上的良好合作关系也延续到了双方政府层面。2009 年，在中国工业和信息化部与欧盟委员会通信网络、内容和技术总司等主管部门的推动下，第一次中欧信息技术、电信和信息化对话在北京举行，双方围绕信息通信基础设施建设、电子商务、电子政务，以及数字转型等内容进行了探讨。此后，这一年度对话机制轮流在中国和欧洲举办，至 2018 年底已举办了 9 次。

信息通信技术在过去十年蓬勃发展，信息通信的技术、产业和政策不断迭代更新，更加凸显了中欧双方合作对话的重要性。中欧信息技术、电信和信息化对话既包括一些长期性的议题，如信息通信技术政策与监管、数字转型、通信基础设施合作等，也包括一些时代意义很强的话题，如数字经济、5G 研发、工业数字化等。此外，双方在对话框架下还开展了联合研究项目，如 2016 年启动的“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分析、探索合作。② 通过该对话机制，双方加强了政策层面的协调，促进了产业界合作，为中欧在 5G、工业互联网、人工智能等战略新兴领域的合作奠定了良好基础。③ 同时，对话也反映出中欧在信息通信技术和产业领域拥有巨大的合作空间。

1.2　中欧网络工作组

2012 年《第 14 次中欧峰会联合宣言》宣布，

① 参见中国互联网协会《中国互联网发展史(大事记) 》，2013 年 06 月 27 日，中国互联网协会网站，http: //www.isc.org.cn/ihf/info.php? cid = 218。

② Khalil Rouhana, “8th EU - China ICT Dialogue”, 11 July 2017, https: //ec.europa.eu/digital - single - market/en/blog/8th - eu - china - ict - dialogue - 11 - july - 2017.

③ 工业和信息化部“第九次中欧信息技术、电信和信息化对话会议在京召开”，中华人民共和国中央人民政府网站，2018 年 9 月 28 日，http: //www. gov. cn/xinwen/2018 - 09/28/content _ 5326276.htm。

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

将由中国外交部与欧盟对外行动署联合建立“中欧网络工作组”(EU-China Cyber Task Force),这是一个由双方外交部门牵头的关于国际网络安全的跨部门沟通协商机制。① 自2012年以来,网络安全问题集中爆发,对国际安全、信息通信和数字经济等领域的全球合作产生了很大危害。② 因此,从国际安全角度探讨应对网络安全危机成为网络空间全球治理的重要议题。

在中欧网络工作组建立后不久,“斯诺登事件”爆发,网络安全一时成为全球最重要的国际政治、安全话题。中欧作为美国开展“大规模监听”的共同受害者,通过该机制,共同发声谴责“大规模监听”这一危害国际政治、安全秩序的恶意网络行为,一定程度上引领了网络安全国际治理的议程。此外,双方通过中欧网络工作组加强了在国际安全领域的合作,中欧外交部门之间就建立网络空间中的国家行为准则、国际法在网络空间中的适用、建立信任措施,以及加强关键基础设施保护、打击网络犯罪的国际合作等议题展开了讨论。通过对话,双方增加了政策透明度,增进了相互之间在网络领域的信任,为双方网络安全相关机构(如计算机应急响应机构)深化合作奠定了基础。

1.3 中欧网络安全与数字经济专家组

2016年,在全球网络空间安全形势不断恶化的背景下,中欧各自在网络空间实施了一系列新举措,从网络的安全、发展与治理入手,围绕网络空间的战略规划、政策制定、产业发展和人才培养等问题探索建立全方位的战略体系。③ 如何加强中欧在网络安全和数字经济领域的协调,对于双方网络战略和政策的实施具有重要作用。在该年7月第十八次中欧领导人会晤期间,由中国国家互联网信息办公室与欧盟委员会通信网络、内容和技术总司共同组织的“中欧网络安全与数字经济专家组”成立。④ 该机制主要任务是聚焦双方内部网络政策和监管模式,商讨如何加强政策协调沟通,增加政策透明度,减少各自国内的相关法律法规对双方商业和数字经济领域的影响,并为双方在战略层面建立互信、在产业层面加强合作提供建议。截至2018年底,中欧网络安全与数字经济专家组已举办了4次会议,并商定在未来继续开展对话。

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、制度建设对双方所产生的影响,以及如何进一步推动中欧在产业发展、人才培养和科学研究的合作开展对话。如在数据安全领域,欧盟制定了《一般数据保护规则》(GDPR),中国制定了《个人信息和重要数据出境安全评估办法(征求意见稿)》,这些管理政策不仅对双方互联网及相关企业的运营模式和个人信息安全带来重要影响,也会引起一定程度的司法管辖权争议。中欧双方的参会代表在该对话机制中曾多次就数据安全政策方面的问题进行及时沟通和协商,妥善回应了对方的关切,促进了双方互信。

1.4 小结

中欧在网络领域的三个对话合作机制正逐渐上升为中欧关系总体议事日程的重要组成部分。随着双方在对话中取得的成果越来越丰富,网络对话合作已成为中欧双边关系的重要支柱。2013年第十六次中欧领导人会晤共同发表的《中欧合作2020战略规划》中提到,“支持并推动构建和平、安全、有弹性和开放的网络空间。通过中欧网络工作小组等平台,推动双方

---

① “China's Policy Paper on the EU: Deepen the China-EU Comprehensive Strategic Partnership for Mutual Benefit and Win-win Cooperation”, Ministry of Foreign Affairs of PRC, 2 April 2014, http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/wjzcs/t1143406.shtml.

② 如《纽约时报》揭露,美国与以色列的情报机构共同在伊朗核设施的工业与控制系统中植入“震网病毒”,导致大量用于分离核原料的离心机受损。此后,震网病毒开始在网络中扩散,在全球范围内感染了大量的核电站和水电站,给国际社会带来了极大的安全隐患。

③ “Proposal for the 'Cybersecurity Act'”, European Commission, September 13, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN.

④ 中华人民共和国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”,中国网信网,2017年3月9日,http://www.cac.gov.cn/2017-03/09/c_1120599476.htm。

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

在网络领域的互信与合作。”[①]2014 年中国政府发布的《深化互利共赢的中欧全面战略伙伴关系——中国对欧盟政策文件》中提出，“加强网络安全对话与合作，推动构建和平、安全、开放、合作的网络空间。通过中欧网络工作小组等平台，促进中欧在打击网络犯罪、网络安全事件应急响应和网络能力建设等领域务实合作，共同推动在联合国框架下制订网络空间国家行为规范”。[②] 在建立中欧战略合作伙伴关系的政策指引下，上述机制围绕双边网络安全、信息化、国际治理等议题开展了多轮对话，取得了丰富成果，不仅加强了双边网络合作，也有利于维护全球网络空间的整体稳定。

二、现有中欧网络对话合作机制的不足

中欧在网络领域的对话合作机制虽然取得了大量的合作成果，但依旧存在一定的不足。特别是在网络空间战略性地位不断提升、国际网络安全威胁不断增加、全球网络空间秩序变革速度加快的背景下，中欧在网络领域的合作未能完全反映网络问题的战略性、重要性和全局性特点，离双方领导人提出的要求还存在一定差距。

2.1　现有的对话合作机制缺乏明确的战略定位，导致中欧网络合作的战略目标不清晰，影响力不足

目前三个对话合作机制的内容基本上聚焦于一些工作层面的信息交流和政策沟通，在战略协调和实质性合作等方面还有待进一步提高。[③]相比中美、欧美、中俄等双边层面的网络合作及其在国际上的影响力，中欧网络合作还有很大的提升空间。这种差距的存在并非因为双方没有共同的利益，而是中欧网络关系在双边和全球层面缺乏战略定位所导致。中欧分别都与美、俄等其他重要国家开展了一系列的双边网络对话合作，这些机制基本都有明确的战略目标。如中美之间的合作以解决网络商业窃密问题为导向，以维护中美在网络安全领域关系的稳定为战略目标，先后建立了“中美网络安全工作组”“中美打击网络犯罪及相关事项高级别联合对话”“执法与网络安全对话”等对话机制；中俄之间是战略协作，以建立互信、推广共同理念为目标，协调双方在国际网络治理中的原则理念、政策立场，如中俄在金砖国家和上海合作组织等框架下开展了网络安全对话机制，并共同制定了《信息安全国际行为准则》，作为正式文件在联合国大会上进行分发。[④]

与上述双边合作机制相比，尽管中欧现有的三个对话机制都各有自己的定位，但是中欧网络对话合作的总体目标和整体合作框架目前还不清晰，战略设定目标过于宽泛，缺乏明确导向。这不仅使现有的对话机制在面临结构性挑战时容易止步不前，也使得中欧网络对话合作无法围绕网络空间全球治理领域具有挑战性的议题开展工作。更为重要的是，这使得中欧网络对话在彼此网络外交中的优先级不够，容易受到中美、美欧网络对话的影响和冲击。缺乏战略定位限制了中欧对话合作在网络空间全球治理中发挥引领和示范作用。

2.2　现有中欧网络对话的层级限制了其对中欧网络政策协调的有效性

网络问题涉及议题大多具有高度的战略性和敏感性，所涉问题往往具有跨领域、跨部门特征，因此，双方高级别领导层面的统筹协调具有重要作用。以中美为例，网络议题一度是中美

---

① 中华人民共和国商务部欧洲司《中欧合作 2020 战略规划》，中华人民共和国商务部网站，2016 年 1 月 14 日，http://ozs.mofcom.gov.cn/article/hzcg/201601/20160101233963.shtml。

② “China's Policy Paper on the EU: Deepen the China-EU Comprehensive Strategic Partnership for Mutual Benefit and Win-win Cooperation”, Ministry of Foreign Affairs of PRC, 2 April 2014, http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/wjzcs/t1143406.shtml.

③ 中欧网络工作组会议在 2015 年第四次会议之后再未公开发布相关信息。

④ *International Code of Conduct for Information Security*, *Annex to the Letter Dated* 12 *September* 2011 *from the Permanent Representatives of China*, *the Russian Federation*, *Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General*, UN General Assembly Document A/66/359/, September 14, 2011.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

元首对话的核心议题，对中美关系产生了持续性的影响。2013年6月，中美元首庄园会晤，习近平主席与奥巴马总统直接就网络安全问题进行对话，在随后的多次元首会晤中，两国领导人都继续对网络安全问题直接表达了关切。① 双方领导人的重视对于提升网络议题在双边关系中的重要性无疑具有强劲的推动作用。相比而言，网络安全问题尚未成为中欧最高领导人对话中的核心议题。

如果将中欧网络合作纵向上与双方在战略、经贸及其他全球治理领域的对话合作比较，横向上与中美、欧美在网络领域的对话合作比较，会发现中欧网络对话的层级要低很多。目前，中欧间的三个网络对话合作机制基本上处于副部级或司局级层面。② 这使得中欧网络对话被纳为其他更高层级对话合作中的一个子议题，从而影响了网络对话的效率和效果。③ 在当前网络问题在国际、国内政治议程中地位如此突出情况下，中欧之间在网络领域的对话层级远远不能反映出问题的紧迫性和重要性，使得中欧网络问题在双边关系中得到的重视程度不够。

2.3 对话机制之间缺乏统筹协调，制约了对话成果的落实

现有的网络对话机制，除了中欧网络工作组之外，都是单一部门间的直接对话。而网络议题往往跨领域，网络安全、发展和治理等多个领域之间深度交融。因此，建立跨部门协调机制应是网络对话的重要形式。参照中美、欧美网络对话可知，跨部门协作在提升网络对话成果方面具有重要作用。如中美网络对话，中方是由中央政法委书记牵头，公安部作为主要的落实部门，成员包括中央网信办、外交部、工信部等部委的副部级领导，美方也是有国土安全部、司法部、联邦调查局等机构的部长级官员参加。欧美之间建立的网络安全与网络犯罪工作组和高级别网络对话合作也都是跨部门的对话合作，不仅欧美双方的多个政府机构参与对话，19个欧盟成员国的代表也作为观察员参与对话。④

跨部门协调机制是应对网络议题跨领域特性的重要方式。以中欧在5G议题上的对话为例，它既是技术和产业问题，也涉及网络安全与国家安全问题。现有的对话模式下，促进和制约中欧在5G领域开展对话合作的部门之间缺乏有效平衡，使得双方容易采取“最坏的打算”，增加了解决问题的难度。⑤ 中欧需要从技术、产业、网络安全和国家安全综合性角度来权衡双方在5G领域合作面临的成本与收益。这一综合评估任务，只有通过跨部门协调才有可能完成。随着中欧在网络领域对话的不断深入，现有机制的不足之处将会进一步制约对话合作的有效性。从现有的三个对话机制设计来看，还需要有经济、安全等更多部门参与其中才能推动对话走向深入，如中方可以将公安部、商务部、发改委、司法部等部委纳入中欧网络对话框架中，欧盟也可以将欧洲刑警组织(EUROPOL)、欧盟网络信息安全署(ENISA)、欧盟贸易总司(DG-Trade)等执法、商业、经济、法律主管部门纳入对话中来。

缺乏清晰的战略定位和足够高的对话层级，以及制度设计上缺乏跨部门协调等不足使中欧网络对话一定程度上陷入困境，主要体现为双方之间信任赤字扩大、主要政策立场差异未能弥合、务实合作成果有限等方面。中欧网络合作存在的深层次分歧和矛盾值得探究。

---

① The White House, “FACT SHEET: President Xi Jinping's State Visit to the United States,” September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

② 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。

③ “第十九次中国—欧盟领导人会晤成果清单”，新华网，2017年6月4日，http://www.xinhuanet.com/world/2017-06/04/c_1121081995.htm。

④ The White House, “FACT SHEET: U.S.-EU Cyber Cooperation”, March 26, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation.

⑤ Charles Rollet, “Huawei Ban Means the End of Global Tech”, *Foreign Policy*, May 17, 2019, https://foreignpolicy.com/2019/05/17/huawei-ban-means-the-end-of-global-tech/.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

三、困境背后的深层原因

中欧网络对话一定程度上的困境有多方面的因素,既包括前述技术性因素,也有以下深层次的因素。

3.1　中欧对网络空间基本属性存在认知差异,不利于双方在具体政策上达成共识

网络空间是人类基于信息通信技术建立的虚拟空间。中欧不同的政治体制、社会结构以及互联网发展模式使得双方对网络空间基本属性的认知存在较大差异。欧盟更多将网络空间看成是物理空间的延伸,因此主张将物理空间的秩序和规则体系延伸到网络空间之中。中方认为网络空间不仅是物理空间的延伸,也是物理空间的映射,映射强调虚拟空间与现实空间之间的互动会带来一系列新现象和新特点,物理空间中的秩序和规则难以简单地应用在网络空间,因此需要站在一个新的角度来看待网络空间以及相应的秩序构建和规则建立。

中国以一种综合性、战略性的视角来看待网络空间,更加主动地接受网络空间,认为"网络空间越来越成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域。"[①]相比而言,欧盟对网络空间概念、内涵缺乏明确界定,其唯一一份全面阐述网络空间战略的文件——《欧盟网络安全战略》,主要从安全视角出发,强调欧盟的价值观、人权、接入权、多利益攸关方、共同责任等五大基本原则。[②] 其核心思想是将欧盟在物理世界的伦理、规范和规则体系移植到网络空间。

对于网络空间基本属性的不同认知影响了双方对于网络空间秩序构建的基本理念。中方认为网络空间作为一种新空间、新疆域,产生了新的生产方式、生活方式和思考方式,由此产生的治理问题是一种新现象、新挑战,提出了网络空间全球治理的"四项原则、五点主张"。[③] 欧方认为网络空间与现实空间是在线(online)和离线(offline)的区别,更多强调网络的工具属性,只需要将物理世界的规则体系延伸到网络空间,即可以实现对网络空间的治理。[④]

3.2　双方对网络空间治理原则存在不同理解,不利于双方在战略层面取得互信

在构建网络空间秩序的基本原则上,中方认为主权国家在网络空间治理中拥有权威性与合法性,认为应当基于网络主权来构建网络空间的秩序,支持《联合国宪章》在内的国际法在网络空间的适用。欧方强调《欧盟基本权利宪章》(Charter of Fundamental Rights of the European Union)所规定的基本权利、自由表达权、隐私权等价值观是网络空间治理中的基本原则。[⑤] 对于治理原则的不同理解,容易引发双方在政策层面的误解。如欧盟认为,中国对网络主权的强调,将会分裂互联网,中国的网络安全政策也是服务于政府权力在网络空间的扩张。从中方角度来看,欧盟在网络政策领域过度强调所谓的"隐私和自由"问题,实际上有双重标准之嫌,如欧盟在批评中方网络内容管理政策的同时,也在加大对"假新闻"的打击力度,实际上也是在践行"网络主权"。

当然,双方在治理原则领域的分歧是非本质的,只是在优先顺序以及现实政策面临取舍时有所差异。中方强调的网络主权是一种旨在奠定新空间、新疆域中基本秩序和权力的理念,其内涵与现实社会的主权存在较大的差异,应

---

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.html。

② European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", July 2 2013, Brussels.

③ Lu Chuanying, "China's Emerging Cyberspace Strategy", *The Diplomat*, May 24, 2016, https://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy.

④ "The EU Gets Serious about Cyber: The EU Cybersecurity Act and Other Elements of the 'Cyber Package'", *Convington Report*, September 18, 2017, https://www.cov.com/-/media/files/corporate/publications/2017/09/the_eu_gets_serious_about_cyber.pdf.

⑤ Alina Kaczorowska-Ireland, *European Union Law*, 4th Edition, Routledge-Cavendish, 2016, p. 176.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

结合网络空间属性进行重新定义。欧方强调有限主权,以国家责任的视角来看待国家在网络空间中的主权范畴。[①] 两者之间有一定的重叠之处,也存在较大的差异。如果不能理解对方的治理原则,就会进一步加大对对方政策的误解,将双方在传统国际关系领域的"主权、人权、发展、平等、自由"的理解分歧带入网络空间全球治理中,不利于建立双方在网络领域的互信。

3.3 中欧对于网络空间全球治理模式有不同的选择,限制了双方合作的成果

在网络空间全球治理领域,欧盟推崇"多利益攸关方"(multi-stakeholder)模式,中方更倾向于多边(multilateral)与多方(multi-parties)共存的治理模式。"多利益攸关方"模式强调国家、市民社会和私营部门共同参与治理,采取自下而上、公开透明的基本原则,主要为互联网名称与数字地址分配机构(ICANN)等互联网技术社群所采用,背后一定程度上暗含了突出社群主导地位、限制国家作用的意味。[②] 欧方理解的"多利益攸关方"模式主要应用在互联网关键资源治理领域,是一种较为理想化的治理模式。中方不反对"多利益攸关方"模式,但认为这一概念运用领域过于广泛、内涵较为繁杂,因此不提倡在双边和国际场合使用这一概念。[③] 特别是在国家在网络安全、网络空间治理等领域的作用和地位愈发重要的趋势下,中方认为不应回避国家的主导作用。因此,中方采取的是一种更加符合实际的态度,认为应当根据不同的治理议题来分别采取多边治理和多方治理模式。

不同的治理模式选择,客观上对中欧对话合作造成了一定程度的干扰。例如在中欧网络安全与数字经济工作组中,中方希望能够发挥政府的指导作用,与欧方在网络安全与数字经济战略和政策层面加强统筹协调。欧方更加倾向"多利益攸关方"模式,主张让私营部门发挥主要作用,并邀请了诸多私营部门代表参与甚至主导对话,而一些欧洲企业则把对话视为解决其在华运营中面临的具体问题的渠道。中方强调在战略和政策领域的协调,欧方希望在具体务实的问题上取得进展,这与双方在网络领域采取的治理模式不同有很大关系,客观上使对话的安排不对等,对对话的效果产生了负面影响。[④]

3.4 中欧之间的网络政策体系存在结构性差异,阻碍了双方沟通交流

网络是一个新的议题,中欧双方的网络决策体系还处于不断完善过程中。决策体系内部不完善和双方传统的决策体系之间的不对称,增加了建立有效沟通机制的难度,而欧盟内部的双层治理结构更是加大了其内部形成共识、进而对外进行有效对话的难度。

网络空间属于国内政治和国际政治中的新兴议题,中欧双方的统筹协调治理机制都在建立和完善的过程中,这也会影响双方在网络合作上的有效性。很多专家都曾用"九龙治水"形容各国对网络议题的治理结构。欧盟网络领域存在多层次的复杂协调机制,各机构间缺乏明确的权责分配,加之资金有限、人员不足,机制间缺乏有效的协调实践。同时,不同机构的网络治理目标不同,多头治理现象突出。如欧盟负责网络安全政策制定、实施的机构有欧盟委员会通信网络、内容和技术总司、欧洲网络信息安全署(ENISA)、欧洲网络犯罪中心;负责网络领域国际合作的机构有欧盟对外行动署(EEAS)、欧洲防务局(EDA);负责打击网络犯罪的机构有欧洲刑警组织(Europol)、欧洲警察

---

① European Parliamentary Research Service, "Cybersecurity in the EU Common Security and Defence Policy(CSDP): Challenges and Risks for the EU", European Parliament, May 2017, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf.

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 参见鲁传颖"网络空间大国关系面临的安全困境、错误知觉和路径选择",《欧洲研究》,2019年第2期,第115-120页。

④ Laura DeNardis, *The Global War for Internet Governance*, New Haven: Yale University Press, 2014, pp.20-25.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

学院(*European Policy College*)等。[①] 多头治理造成欧盟网络空间管理机制碎片化问题突出,难以形成行动凝聚力。[②] 具体到微观层面,则是多机构之间难以就具体问题达成及时、高效的合作。中国方面,虽成立了中央网络安全与信息化委员会以加强网络议题的统筹协调,改善不同部门之间的权力与职责划分问题,但随着社会信息化程度的增加,各个部门涉及网络的工作比重不断增加,统筹协调的难度和成本也不断增加,特别是在统筹国内和国际两个层面的网络问题上,还需要进一步完善机制。由此可见,中欧之间面临的沟通不顺畅,落实合作困难等现象都与双方的内部统筹治理机制存在的问题有关系。

欧盟双层治理机制也增加了中欧对话的难度。作为超国家行为体,欧盟与第三方国家进行网络空间合作时存在特殊性。一方面,欧盟在涉及共同安全和防务政策领域享有法定权力,但网络安全与国家安全密切相关,网络治理的权力主要掌握在成员国手中,欧盟在该领域的治理能力赤字明显。另一方面,主权国家和超国家机构尚未就网络安全领域的权能划分形成有效共识,欧盟整体缺乏清晰的治理结构。成员国之间网络实力的差异,使得各方在网络空间治理与合作上的政策立场存在较大差异,各成员国间的网络合作需要欧盟统一协调,由此产生了成员国与欧盟双层次的治理结构。欧盟通过《网络与信息系统安全指令》(简称 NISD)规范网络安全治理的主要方向,通过欧洲网络信息安全署的机制性建设协调相关工作。但欧盟指令对成员国不具有强制性,成员国国内的网络安全法律仍起主导作用;加之欧盟机构的复杂授权机制,导致运转效率较低,难以形成快速、有效的对外共同政策。[③] 中方与欧方进行合作时既需要与成员国进行政策沟通,也需要把握欧盟整体的网络政策,这增加了中欧合作的复杂性和沟通成本。同时,成员国和欧盟机构的相互龃龉导致政策相对低效,也加大了中欧共同制度设计的机制性困难。

3.5　美国等地缘政治因素对中欧网络对话合作形成制约

传统地缘政治因素,特别是美国因素,对中欧网络领域合作具有很大影响。美欧盟友关系决定了欧盟在安全领域对美国有很大依赖,其网络空间战略深受美方影响,双方在网络战略协调、政策对接和务实合作方面具有广泛基础。[④] 这无疑会影响中欧网络合作的优先性。在中美欧三角关系中,欧盟本能地会将欧美关系置于优先地位。欧盟尚未形成自主的网络安全战略和网络威慑能力,在网络技术和网络能力领域倚重美国,“追随美国”的政策倾向明显。[⑤] 无论是网络安全战略思维,还是网络空间国际治理理念,欧洲基本上认可美国提出的主张,其对美国的安全依赖及欧美固有的理念共识,导致欧盟在多边和双边领域都保持了与美国的政策协调,双方在网络军事互动和共同舆论发声上保持了高度一致。[⑥] 欧盟往往配合美国的网络政策,争取西方网络安全话语权,实现西方国家集团利益的最大化。而欧美集团所欲实现的目标与中国在国际网络领域的目标相悖,美欧密切协调也不利于新型互联网治理模式的推广和实现。[⑦] 美国因素成为中欧网络关系中重要的第三方因素,使既有的中欧合作机

---

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

③ European Court of Auditors, “Challenges to Effective EU Cybersecurity Policy”, European Union, March 2019, https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.

④ John B. Sheldon, “Geopolitics and Cyber Power: Why Geography Still Matters”, *American Foreign Policy Interests*, Vol.36, No.5, 2014, pp. 286-293.

⑤ Iva Tasheva, “European Cybersecurity Policy--Trends and Prospects”, European Policy Centre, June 8, 2017, http://www.epc.eu/documents/uploads/pub_7739_europeancybersecuritypolicy.pdf.

⑥ George Christou, *Cybersecurity in the European Union*, Palgrave Macmillan, 2016, pp. 146-149.

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

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

制更为复杂，给推进中欧网络安全合作带来困难。

四、中欧在网络领域合作的未来提升路径

由前述分析可知，影响中欧网络对话合作的，既有对话机制本身存在的问题，也有深层次的结构性因素。要推动未来中欧网络对话深入开展，一方面应完善机制建设，建立符合网络议题特点的战略性、高层级、跨部门的对话机制；另一方面，双方政府应加强议程设置，围绕双方共同利益开展务实合作。

4.1 完善和丰富现有对话合作机制，建立战略定位更清晰、对话层级更高、跨部门协调机制更完善的中欧网络对话合作机制

现有的中欧网络对话合作更多反映了工业化时代的对话机制设计，已经无法反映新的数字时代背景下网络空间所具有的战略性、全局性和颠覆性意义。要适应新时代要求，一是要双方从战略高度来重新审视网络空间对物理世界双边关系所带来的深刻变化。网络空间一方面让双方的交往更频繁、联系更紧密、合作更多元，另一方面也导致网络政策的外部性更加明显、冲突更加高频、矛盾来源更加广泛。因此，双方应在战略层面意识到网络议题在中欧关系中的优先位置；二是要通过提升对话的级别来增加对话的效率。从现行的体制来看，最有效的方式就是让更高层级的官员来担任网络对话的牵头人。无论是参考中欧在其他重要领域的对话层级，还是比照双方与其他国家之间的对话层级，都需要将现有的司局级对话合作提升到更高层级；三是要建立跨领域、跨部门的统筹协调机制来推动中欧网络对话，并尽力克服欧盟双层治理结构所带来的影响。一直以来，双方对于如何找到自己对应的合作伙伴存在一定的困难，到底是与欧盟合作还是与成员国开展合作才能有效解决问题是中方部门困惑的来源，这需要欧盟内部进一步加强政策协调，形成欧盟层面网络国际事务的相对一致性[①]。同时，中方的相关部门也需完善对欧盟双层治理机制的了解，厘清网络事务中欧盟的不同部门及其与成员国之间的权责分配，在合作时能够找准对象，有的放矢。

双方应将平等互信作为对话合作基础，克服双方在意识形态和政治制度方面的分歧。欧洲一直以来处于国际关系的中心地位，在国际规则制定上有很大的影响力与话语权，这一影响同样体现在网络领域，如欧盟在网络犯罪、网络战，以及传统国际法在网络空间适用性等方面的研究和实践走在全球前列。中国则是国际治理领域的新兴参与者，在网络领域的实力发展较快，涌现了腾讯、阿里、百度等一批在全球有重要影响的互联网企业，网络实力不断增强。一方是传统国际关系主角，一方是有潜力的未来大国，双方在对话中心态微妙，不易展开坦诚、深入的交流合作，特别是在面对分歧时无法真正从内心理解、认可对方的主张。客观而言，双方在网络领域的很多理念、政策分歧是双方国情的客观反映，并没有对错或高下之分。欧洲注重从人权角度看待网络领域出现的问题，反映的是欧洲社会对于隐私问题、言论自由问题的高度重视。中方注重从发展的角度来看网络问题，是因为中国社会更加注重在发展过程中解决存在的问题。[②] 中欧双方如果能够以更加平等、协商的姿态来开展网络对话，将会有利于提升对话的成效和影响力。

4.2 加强中欧对话合作的议程设置，围绕共同利益来设置对话的重点

中欧网络对话合作的阶段性目标主要包括增信释疑、管控分歧和促进合作。现有对话机制在前两个阶段的目标上已取得进展，双方对于现有对话机制存在的问题，以及问题背后的深层次因素也基本有了共识。下一阶段，中欧

① 周秋君“欧洲网络安全战略解析”，《欧洲研究》，2015年第3期，第77页。

② Joseph Nye, “The Regime Complex for Managing Global Cyber Activities”, *Global Commission on Internet Governance Paper Series*, No. 1, 2014, pp. 5-13.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

应将目标放在如何促进双方在网络领域的合作上,这就需要从政府层面完善对话的议程设置,围绕促进双方共同利益来开展合作。在当前国际网络安全陷入结构性困境、全球网络治理机制构建停滞不前、网络空间秩序与繁荣面临严重威胁的背景下,中欧的共同利益主要体现在共同应对网络攻击挑战、维护网络空间稳定,以及携手构建数字贸易规则等方面。

中欧在双边层面可以承诺互不开展网络攻击,加强在网络攻击的溯源、信息共享等领域的合作,并签署具有约束力的国际协定。① 双方可以将关键基础设施保护为突破点,在联合国信息安全政府专家组(UNGGE)制定的网络规范基础之上制定更加有操作性的中欧关键基础设施保护计划。② 2015 年,联合国信息安全政府专家组发布重要的共识文件,呼吁各国加强在关键基础设施保护领域的合作,认为"各国均不得从事或者在知情情况下支持违反国际法规定的义务的信息通信技术活动,这些活动有意破坏关键基础设施或损害其使用和运行,导致其不能为公众提供服务。"③中欧可以在这一规范基础上探讨双方对关键基础设施的定义、范围;双方承诺互不攻击对方关键基础设施;在对方提出请求的情况下,协助调查、取证等。相比其他领域,这一方面的合作存在一定的敏感性,但是有利于双方建立互信,因此,需要双方加强对话议题和机制的设计,确保在互信的基础上开展实质性合作。

中欧应共同在全球层面积极维护网络空间稳定。以中国、美国、欧盟、俄罗斯为代表的网络空间大国关系已经进入新的力量重整阶段,正在重塑网络空间秩序,并且对物理世界的国际安全、政治、经济体系产生巨大冲击。特别是在中美网络关系进入新一轮博弈的情况下,中欧网络关系面临新的不确定性。美国对中国的网络科技和信息通信领域产业极力打压,遏制中国的同时,也对全球的供应链安全、创新生态体系造成了极大破坏。中欧都是网络空间发展、繁荣的受益者,也是全球信息通信技术供应链和创新体系中的不可或缺的部分,强行将中国剥离出去,将严重影响国际经济、技术的安全与发展,欧洲也无法独善其身。在这一特殊的转折时期,中欧应当共同维护网络科技的全球供应链安全和创新体系,遏制住美国的破坏性举措。

中欧应携手探索构建全球数字规则体系,共同防止网络空间的"巴尔干化"(balkanization)。网络空间有很多属性,其中最重要的一个属性就是互联互通性(connectivity),"巴尔干化"是指其打破全球网络空间互联互通的趋势,从技术、数据和商业层次建立国家化的网络空间。"巴尔干化"具体包括互联网基础架构、数据和应用三个层面的分裂,当前主要表现为"数据国家化"导致在数据层面的"巴尔干化"。2018 年以来,欧盟出台了《一般数据保护规则》(GDPR),中国制定了《个人信息出境安全评估办法(征求意见稿)》。未来全球网络空间有可能形成中国、欧盟和美国三种数据监管模式,这会给基于数据开展创新的人工智能、大数据和云计算等产业及相关商业模式带来极大的挑战。为避免"巴尔干化"对全球经济造成的损害,中欧双方可以着手开展建立数字经济国际规则的对话合作,包括如何在确保安全的前提下降低企业合规门槛,引导企业合法进行数据跨境流动;双方的数据保护部门可以为对方涉及数据跨境业务的企业提供定期培训;推动邮政、物流、电子商务等重点行业的数据互通;加强涉恐、涉刑事犯罪的个人数据跨境协作等。双方应通过务实合作,为探索建立全球数字规则体系建立样本,从而防止网络空间的"巴尔干化"趋势的加剧。

---

① Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies*, Vol.38, No,1-2,2015, pp.4-37.

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 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.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

五、结 语

综上所述，中欧现有的对话合作机制覆盖了战略、政策、技术和产业等方面，在取得了很大的合作成果的同时，也面临网络议题本身的复杂性和双方对于网络空间、治理原则、治理方式上认知差异等方面的挑战。未来中欧在网络领域的对话合作需要进一步完善机制设计，加强议程设置，克服中欧之间客观存在的各种差异，通过对话合作不断建立互信，增加合作成果，展现中欧网络对话合作在网络空间大国关系和全球治理中的示范、引领作用。

编辑 邓文科

Current Situation and Prospect of China-EU Cyber Dialogue and Cooperation

LU Chuanying[1]

(1. *Shanghai Institutes for International Studies*, *Shanghai* 200233, *China*)

Abstract: The China-EU cyber dialogue and cooperation makes an essential part of China-EU relations, which plays a significant role in the security, development, and governance of the global cyberspace. China and the EU have had a series of comprehensive and in-depth dialogues on cyber issues, but there are also problems such as inaccurate strategic positioning, lack of mutual trust, and insufficient institutional design. The problem reflects differences in their strategic cognition and decision-making systems, as well as the influence of traditional geopolitical factors. In the future, China and the EU are supposed to further define the strategic positioning of cyber cooperation, strengthen the dialogue institutional design, and focus on agenda-setting to jointly shape the future of China-EU cyber cooperation.

Key words: China-EU relations; cybersecurity; cyberspace governance

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net