打击网络犯罪国际法机制的困境与前景

——以欧洲委员会《网络犯罪公约》为视角

胡健生[*]　黄志雄[**]

摘　要：2004 年生效的欧洲委员会《网络犯罪公约》，是迄今为止打击网络犯罪领域最具影响力的区域性法律文书。《公约》不仅是其成员国打击网络犯罪适用的首要法律依据，而且为中国在内的很多非成员国的国内立法所借鉴，还推动了其他区域性国际法机制的快速发展。但当前全球层面打击网络犯罪的国际法机制呈现“碎片化”状态，以《公约》为代表的区域性国际法机制，亦因其自身的局限性难以发展成为全球适用的法律标准。因此，制定新的综合性的全球法律文书势在必行。当前，美欧等西方国家与中国、俄罗斯、巴西等新兴国家和其他发展中国家正围绕推广欧洲委员会《公约》和制定新公约展开激烈博弈。本文将结合上述形势，对打击网络犯罪国际法机制的未来发展作出展望，并就中国参与构建相关机制提出建议。

关键词：网络犯罪　欧洲委员会《网络犯罪公约》　打击网络犯罪国际法机制　综合性全球法律文书

网络犯罪（cybercrime）通常被描述为以计算机或网络为工具、目标或地点的犯罪活动，其常见形式主要包括破坏计算机数据或系统的机密性、完整性与可用性的行为。除此之外，以谋取个人或经济利益，或是造成个人或经济损害为目的并与计算机有关的行为，包括与身份有关的犯罪行为（如在线窃取个人身份信息），及与计算机存储内容有关的犯罪行为（如窃取商业秘密）等亦属于广义上的“网络犯罪”。[①] 美国网络安全企业迈克菲（McAfee）2014 年有关网络犯罪造成的经济影响的研究报告显示，每年网络犯罪造成的经济损失保守估计约为 3750 亿至 5750 亿美元，至于间接的人力、物力损失更是难以估量。[②] 可以说，网络犯罪已成为当今危害性最为突出的网络安全威胁之一。

从二十世纪七十年代起，各国纷纷制定相应的法律和政策来规制网络犯罪。[③] 但互联网的跨

---

*　外交部条法司干部。

**　武汉大学国际法研究所珞珈特聘教授、《塔林手册》2.0 版国际专家组成员、亚非法律协商组织网络空间国际法工作组特别报告员。本文仅代表两名作者的个人观点，与任何机构无关。

① United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013, p. xvii, available at http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf (last visited October 17, 2016).

② McAfee, Net Losses: Estimating the Global Cost of Cybercrime, June 2014, p. 2, available at http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf (last visited October 17, 2016).

③ Stein Schjolberg, The history of Global Harmonization on Cybercrime Legislation—The Road to Geneva, p. 2, available at http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (last visited October 17, 2016).

国界性、互联性及脆弱性决定了仅靠各国自身的努力是远远不够的，在网络空间开展国际立法与合作是必然趋势。当前，国际上已形成了相当数量的打击网络犯罪的区域性国际法律机制，其中最具代表性的要数欧洲委员会（Council of Europe，简称“欧委会”）在 1997 年发起制定的《网络犯罪公约》（Convention on Cybercrime）。该公约是迄今为止网络犯罪领域最具影响力的区域性多边公约，不仅是欧委会成员国打击网络犯罪适用的首要法律依据，而且为中国在内的很多非成员国的国内立法所借鉴。但该公约自 2004 年生效至今，并未如欧委会预期地那样发展成为全球性公约。国际上至今也未能形成一份专门规定打击网络犯罪及相关国际合作问题的综合性的全球法律文书。那么，以欧委会《网络犯罪公约》为代表的现有国际法机制究竟存在哪些不足？国际社会为何至今仍未形成适用于全球范围的法律文书？打击网络犯罪国际法机制的未来发展方向会是怎样的？在这一过程中中国又可以采取怎样的主张？为回答上述问题，本文将以欧委会《网络犯罪公约》的历史和发展为视角，分析当前打击网络犯罪国际法机制面临的困境，进而展望机制未来的发展方向，并就中国参与构建这一机制提出相关工作建议。

一　欧委会《网络犯罪公约》的制定背景、主要内容和作用

（一）《网络犯罪公约》的制定背景

作为《网络犯罪公约》的发起方，欧委会在全球应对网络犯罪问题的区域性机构中发挥着引领者的作用。[①] 早在 1989 年，欧委会的决策机构部长委员会就通过了第 R（89）9 号决议，要求成员国在审议国内立法时考虑与计算机相关的犯罪行为，这也开启了欧委会在网络犯罪方面的立法进程。[②] 随着网络技术的成熟，电信和信息技术的走向融合，网络犯罪问题的日益严重，欧委会下设的欧洲犯罪问题委员会（European Committee on Crime Problems，CDPC）于 1996 年向部长委员会建议设立专家委员会来探讨应对网络犯罪的对策，并提出通过制定有约束力的国际法律文书来确保打击网络犯罪效率的建议。[③] 该建议为部长委员会所采纳，后者在 1997 年设立“网络犯罪专家委员会”来专门研讨网络犯罪问题并负责起草一份网络犯罪公约。

自开始工作起，专家委员会共进行了多达 10 次全会，15 次开放式的起草小组会议。欧委会成员国、欧委会的相关机构以及学界等各方就该公约草案开展了激烈讨论，具体条款多次修改。最终，该公约于 2001 年 11 月 8 日在欧委会第 109 次部长委员会会议上通过，并于 11 月 23 日在布达佩斯开放签署（该公约因此也称《布达佩斯公约》）。与该公约一同对外公布的，还包括专家委员会起草的《解释性报告》（Explanatory Report to the Convention on Cybercrime），该报告虽不具约束力，但一直以来被各方认为是公约最为权威的解释性文件。

---

① 成立于 1949 年 5 月的欧洲委员会，是一个致力于推动人权、民主和法治并在刑事司法、反恐、气候变化以及文化等领域协助成员国开展合作的区域性国际组织。随着 1989 年大部分中东欧国家的加入，欧委会的成员不断壮大，直至今日其共有 47 个成员国，成员范围几乎囊括了整个欧洲。同时，美国、加拿大、墨西哥、日本等国为其观察员国，也促使欧委会的影响范围扩展到全球。

② Council of Europe，Recommendation No. R.（89）9 of the Committee of Ministers to Member States on Computer-related Crime，1989.

③ Council of Europe，Explanatory Report to the Convention on Cybercrime，paras. 7 – 11.

值得一提的是，美国虽只是欧委会的观察员国，但其依托与欧洲盟友紧密的合作关系以及在网络犯罪领域丰富的国内立法经验，在该公约谈判和制定过程中积极发挥影响，力图使该公约尽可能地反映其主张，成为宣传其网络价值观的重要工具。这一点，在美国司法部名为《欧委会网络犯罪公约——经常提到的问题及回答》的文件中可得以证实："在公约起草过程中，美国务院、司法部、商务部以及利益相关的私营部门均积极参与到起草与全体会议中……（美）虽不能如成员国那样投票表决，但在起草过程中有着强有力的声音。"①

（二）《网络犯罪公约》的主要内容

该公约在结构上分4章，共48条，主要从实体刑法、程序法和国际合作3个方面对打击网络犯罪进行了规定。

第一，实体刑法（第2—13条）。该公约规定了参与谈判的国家共同认可的4大类共9种网络犯罪行为，分别是：（1）破坏计算机系统和数据机密性、完整性和可用性的犯罪行为，包括非法入侵、非法拦截、数据干扰、系统干扰、设备滥用等；（2）与计算机相关的犯罪行为，如与计算机相关的伪造和诈骗犯罪；（3）与内容相关的犯罪行为，如通过计算机实施的与儿童色情有关的犯罪；（4）与侵犯著作权及邻接权有关的，以计算机实施的犯罪行为。此外，公约还规定了上述各类犯罪的未遂、帮助和教唆形态，法人责任以及包括自由刑和罚金刑在内的刑罚措施。

第二，程序法（第14—22条）。该公约规定了专门的调查程序和特别措施，包括：公约的管辖权，计算机数据的快速保存，搜查、实时搜集和扣押计算机数据等规定。为防止计算机数据丢失，该公约还明确规定，缔约方可通过立法及其他必要措施要求相关责任人在必要时间内（最长可达90天）保持数据的完整性，以备查验之需。此外，公约还明确了程序法的相关规定不仅适用于实体刑法部分所列的网络犯罪行为，还可适用于其他通过计算机系统实施的犯罪和涉及电子证据的犯罪，极大地拓宽了该公约的适用范围。②

第三，国际合作（第23—35条）。该公约规定了较强的国际合作机制，内容涉及合作的一般原则，既包括引渡、主动提供信息等一般规定，也包括调查权方面的相互协作在内的特殊规定，如效仿八国集团建立的24/7全天候联络点、实时收集往来数据、跨境进入经同意的或者公开可获得的存储的计算机数据等。该公约亦规定，缔约国应依照该公约有关国际合作的规定并通过适用国际刑事合作的相关法律文书、在统一或互惠的立法基础上达成的安排以及国内法，最大限度地开展国际合作（第23条）。这意味着该公约在一定程度上是对现有各国刑事司法协助体系的补充，要服从于各国缔结的司法协助文书的安排。③

此外，该公约要求缔约国将该公约的实体刑法以及程序法的条款转化为相应的国内法，同时也允许缔约国对上述部分条款予以保留。而对于国际合作部分的条款，该公约虽未明确允许保留，但其第27条规定，允许缔约国可因政治犯罪或涉及国家主权、安全等重要利益拒绝开展司法协助，在尊重各缔约国主权的基础上对国际司法协助的开展作了灵活处理。

---

① U. S. Department of Justice, Council of Europe Convention on Cybercrime Frequently Asked Questions and Answers, available at https://www.justice.gov/criminal/cybercrime/newcoefaqs.html (last visited June 6, 2014).

② 公约第14条第2款规定："除第21条的特别规定外，缔约方应实行本条第1款规定的权力和程序：a. 本公约第2条至第11条规定的犯罪；b. 其他通过计算机系统实施的犯罪；c. 涉及电子证据收集的犯罪。"

③ 这一点也可从公约第39条得到佐证，该条规定："现行公约的目的是补充缔约方之间的多边和双边条约，包括……"。

（三）《网络犯罪公约》的主要发展

1. 缔约情况。该公约于2004 年7 月1 日正式生效。截至2016 年10 月19 日，共有49 个缔约国，另有6 国已签署但尚未批准公约。[①] 其中，俄罗斯、瑞典、希腊、爱尔兰、安道尔、摩纳哥、圣马力诺等7 个欧委会成员国尚未签署或批准该公约（欧委会共47 个成员国）。在非欧委会成员国中，美国、日本、加拿大、澳大利亚、以色列、多米尼加、毛里求斯、巴拿马和斯里兰卡等9 国已经先后加入该公约，南非已签署但未批准公约。而阿根廷、智利、墨西哥、秘鲁、菲律宾、加纳、摩洛哥等国已收到欧委会的邀请，正在加入谈判的过程之中。

2. 第一《附加议定书》。由于参与《网络犯罪公约》谈判的各方未能就种族主义和排外主义言论定罪的通用条款达成一致，因此，作为妥协，欧委会未在该公约中规定言论犯罪，而是将有关条款集成到了一个单独的《附加议定书》之中。[②] 该议定书于 2003 年 1 月开放签署，2006 年 3 月生效。但参与的国家数量明显少于《网络犯罪公约》，截至 2016 年 10 月 19 日，仅有 24 个国家批准或加入该议定书，美国、英国等主要国家尚未签署该议定书。

需要明确的是，对主公约的批准并不要求公约缔约国承担议定书下的任何义务，缔约国可自行决定是否加入该议定书。同时，欧委会近年来也形成共识，在不改变主公约内容的前提下将附加议定书作为修订主公约的主要方式固定下来。[③] 遗憾的是，至今未有第二个附加议定书问世。

3. 公约委员会（Cybercrime Convention Committee，T-CY）。委员会是依据该公约第46 条设立的供缔约国磋商、履约的机制。[④] 自 2006 年以来，委员会已经举行了 15 次全会，讨论通过了对计算机系统、僵尸网络（Botnet）、身份盗窃、关键信息基础设施等公约有关概念的定义与适用的指南，并建立了相关工作组对公约有关云证据（Cloud Evidence）、跨境获取电子数据、网络恐怖主义、公约的加入、管辖权以及委员会议事规则的修订等问题进行讨论并发布相关报告。可以说，委员会的工作对公约内容的研究发展以及缔约国的拓展起到了重要的推动作用。

（四）《网络犯罪公约》的积极作用

总体上看，该公约是国际上早期网络犯罪立法的有益尝试，起到了一定的示范作用。其由欧、美、日等网络技术相对发达、法律理念相对接近的西方国家共同制定，同时借鉴了欧委会、

---

① Council of Europe，Chart of signatures and ratifications of the Convention on Cybercrime，available at http：//www. coe. int/en/web/conventions/full-list/-/conventions/treaty/185/signatures? p_ auth = iyiWghKH（last visited October 18，2016）.

② Council of Europe，Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems，January 28，2003.

③ Alexander Seger，“The Budapest Convention on Cybercrime 10 years on：Lessons Learnt or Web is a Web”，presented in the Session IV at the International Conference on Cybercrime in Courmayeur Mont Blanc，Italy，2 – 4 December 2011，p. 6，available at https：//rm. coe. int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId = 09000016802fa3e0（last visited October 18，2016）.

④ 公约委员会的《议事规则》规定，委员会的职能在于：对缔约国履约进行评价；通过对执行和解释公约的意见和建议，若成员一致同意，该建议便以指导说明的方式作为缔约国履行公约的指南；起草法律文件（公约、议定书、协议或建议等）呈部长委员会批准；采纳欧委会其他机构要求的意见；审查 24/7 联络点的设置状况；在相关国际场合推动缔约国形成共同立场；参与到与相关国际组织的对话机制中以加强国际合作；加强网络犯罪和电子证据方面的能力建设；建立工作组来研究或解决特定问题等。Cybercrime Convention Committee（T-CY），T-CY Rules of Procedure，art. 1，available at https：//rm. coe. int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId = 09000016802e7278（last visited October 18，2016）.

欧盟、经合组织、八国集团以及联合国在打击网络犯罪领域的工作成果，客观上具有一定的积极作用。

首先，公约技术中立性（technology-neutral）的语言，使得具体条款一定程度上适应了互联网技术快速发展所带来的挑战。[①] 譬如，公约虽然名为“网络犯罪公约”，但除了标题和序言以外，具体条款中均没有出现“网络”一词，而是从犯罪对象或犯罪工具的角度出发，以“利用或侵入计算机系统、拦截或获取计算机数据”等描述性条款来界定具体的网络犯罪行为。同时，在对计算机系统的定义中，将其规定为“任何设备，或是一组互联的或相关的设备……自动处理数据”，巧妙地反映了网络的互联性。由此，公约将“网络犯罪”的概念转化为“通过互联计算机系统及其内容实施的犯罪”，避开了对“网络”这一发展中的概念的定义，一定程度上消减了因技术发展可能带来的定义滞后等问题。

其次，公约有关程序法和国际合作的条款，针对性和可操作性较强，一定程度上适应了网络犯罪突发性、即时性的特点。网络犯罪的发起往往难以预测，具有较强的隐蔽性和即时性，传统的犯罪预防与调查机制已难以适应。而公约设定了要求互联网服务商快速保存计算机数据，授权执法部门搜查、实时搜集和扣押计算机数据在内的一系列实时响应式的规则，给缔约国应对网络犯罪提供了示范与引导，有力地增进了相关国家网络犯罪预防的能力建设。此外，这些程序法规则还适用于涉及电子证据的犯罪，体现了公约制定者全面的考量。

再次，公约部分条款否认双重犯罪原则是缔约国之间开展司法协助的前提条件，一定程度上克服了合作的障碍。传统的双多边司法协助文件，尤其是引渡协议，往往将双重犯罪原则作为启动双边司法协助的基础，此也被称为“相同原则”。[②] 虽然现今国际上呼吁刑事司法协助“去双重犯罪化”，但实践中各国还是从维护本国的司法主权出发，多数适用“双重犯罪原则”的传统做法。由于目前各国对网络犯罪的定罪存在较大差异，如果公约在国际合作机制上“因循守旧”，势必会给网络犯罪分子钻漏子、寻找“避罪天堂”提供便利。[③] 鉴于此，该公约制定者作出尝试，在其有关计算机数据快速保存的条款中规定，“在接到另一缔约方的请求后，被请求方应依照其国内法律，采取适当措施……为对请求作出回应，双重犯罪（原则）不应成为提供数据保存的条件”。[④]

由于该公约要求缔约国将其规定转化为国内法，因此，缔约国之间就公约实体刑法部分规定的罪行开展司法协助，原则上是要满足“双重犯罪”前提的。而上述计算机数据快速保存条款针对的罪行，则是公约实体刑法规定以外的、其他涉及电子证据的犯罪。公约为何选择在该问题上作出一定突破？本文认为，计算机数据的快速保存对一国司法主权的“侵入性”程度较低，且被请求方可在保存数据后再评判该行为是否属于其国内法规定的罪行，进而决定是否对请求方披露该数据。这样既不损害被请求方的司法主权，也适应了电子证据极难留存的特点。[⑤] 当然，除该条款以外，针对其他非公约规定的、涉及电子证据的犯罪所开展的双边司法协助仍要以“双重犯罪”或缔约国司法协助文件的安排为前提。

---

① Explanatory Report to the Convention on Cybercrime, para. 36.

② 梁西主编，曾令良修订主编：《国际法》，武汉大学出版社 2011 年第 3 版，第 255 页。

③ Amelia M. Weber, “the Council of Europe’s Convention on Cybercrime”, (2003) *Berkeley Technology Law Journal*, Vol. 18, p. 434.

④ 参见该公约第 29 条第 3 款的规定。

⑤ Explanatory Report to the Convention on Cybercrime, para. 285.

二　从《网络犯罪公约》看现有国际法机制的不足

除了欧委会的《网络犯罪公约》以外，当前其他区域性组织也制定了相关的国际法机制，如非洲联盟的《网络安全与个人数据保护公约》、阿拉伯国家联盟的《打击信息技术犯罪公约》等。但这些公约或多或少都借鉴乃至“照搬”了欧委会公约的相关内容。此外，上海合作组织框架下制定的《上合组织成员国保障国际信息安全政府间合作协定》（以下简称《上合组织信息安全协定》），其部分条款亦涉及网络犯罪问题。[①] 全球层面，在联合国和国际电信联盟等国际组织框架下，也有《联合国儿童权利公约关于买卖儿童、儿童卖淫和儿童色情制品问题的任择议定书》等涉及网络犯罪问题。表面上看，打击网络犯罪的国际法机制及相关实践似已有长足发展。实际上，这些机制大多只是各国从地缘政治或本国立场角度出发，在所处地区区域组织或与立场相近国家构成的“小圈子”的框架下开展相关国际合作构建而成的，地域性和政治性特点明显。不少机制也存在原则性强，缺少具体规制的问题。全球层面至今并未形成各国可统一适用的打击网络犯罪的国际法机制，“碎片化”“各自为战”现象严重。进一步而言，网络犯罪作为与核武器、化学武器等相类似的、公认的全球威胁，仅靠分散性的区域性机制很难有效应对，必须构建国际性的集中（Centralized）应对机制。[②] 因此，整合这些不同区域、不同立法背景且主旨不同的国际法机制，从中发展出一套全球适用的法律标准便成为亟需解决的焦点问题。

那么，现有的国际法机制是否具有发展成为全球标准的可能？以下将以缔约国数量最多，内容最具综合性且影响力最大的欧委会《网络犯罪公约》为例，从其立法平台、具体内容、加入程序及其修订调整的频率等角度分析判定该机制能否实现“全球化”。

第一，公约制定平台“先天不足”。欧委会地域特点十分明显，其成员国局限于欧洲范围之内。因此，其起草并开放签署的公约一般仅在欧洲范围内适用。除个别观察员国，如美国、日本等积极参与相关公约谈判，并发挥实质性影响外，其他域外国家，特别是广大发展中国家对公约内容毫无话语权，自然也不易认同和接受该公约成为全球标准。相反，若公约在联合国框架下制定，则世界各国均可参与公约内容谈判，公约也自然而然可实现“全球化”。

第二，公约内容方面局限性明显。公约实体刑法部分规定的罪名难以适应网络犯罪的发展形势及其他国家的关切。公约规定的网络犯罪罪行侧重于技术性犯罪，即以网络为犯罪对象的犯罪（如非法入侵、非法拦截、数据干扰、系统干扰、设备滥用等），与当前“传统犯罪网络化”的形势不相适应。[③] 除上述技术性犯罪外，公约规定的其他罪行，包括网络儿童色情、侵犯知识产权犯罪等，多为美欧发达国家关切的罪行，而发展中国家重点关注的网络成人色情、网络赌博等罪行均未纳入公约。再有，公约对网络恐怖主义问题的态度值得商榷。公约委员会及欧委会研讨恐怖主义的专家委员会认为，网络恐怖主义一般指对国家信息基础设施发起恐怖主义性质的网络

① 我国于 2009 年 6 月 16 日在叶卡捷琳堡签署该协定，并于 2011 年 3 月 5 日批准该公约。公约的详细文本请参见澳门行政区第 28/2013 号行政长官公告：http：//bo. io. gov. mo/bo/ii/2013/30/aviso28_ cn. asp#cht（last visited October 18，2016）.

② Susanna Bagdasarova，“Brave New World：Challenges in International Cybersecurity Strategy and the Need for Centralized Governance”，（2015）119 *Pennsylvania State Law Review*，p. 1126.

③ 于志刚：《缔结和参加网络犯罪国际公约的中国立场》，载《政法论坛》2015 年第 5 期，第 91—108 页。

攻击，该公约与联合国反恐公约的规定足以规制这类行为，而当前迫切要解决的则是以恐怖主义为目的利用计算机系统的行为，如利用互联网谋划恐怖主义活动、进行军火交易等。[①] 本文认为，公约有关规定规制的是一般性质的网络攻击行为，而上述意见简单地以适用公约规定来规制具有网络恐怖主义性质的网络攻击行为，极易导致对相关行为的制裁难以达到罪责刑相适应的要求。

从该公约内容来看，公约规定的管辖权适用范围有限，很难满足缔约国打击网络犯罪的需求。公约第 22 条规定了属地管辖、航空器的管辖、船舶的管辖以及属人管辖 4 种情形，其局限性十分明显。由于航空器、船舶的管辖可以视同其登记国的“属地管辖”，故该公约实质上只有属人管辖的规定才能使缔约国尤其是受害国通过行使“域外管辖权”以应对网络犯罪的跨国性，并由此开展相关司法协助。同时，该公约还允许缔约国可对除属地管辖外的其他管辖作出保留。如果缔约国据此对属人管辖作出保留，则缔约国之间只能适用属地管辖。。

公约构建的国际合作机制也易受各国有关国家主权、安全以及公共秩序主张的影响，实际效果有限。公约第 27 条第 4 款规定，“被请求方除了可基于第 25 条第 4 款的情形（现有司法协助文书的安排）拒绝请求外，还可基于以下情形拒绝协作：a. 被请求方视请求中的罪行为政治犯罪或与政治相关的犯罪，或者；b. 被请求方认为请求的执行可能损害其主权、安全、公共秩序以及其他重要利益。”因此，一国完全可以上述规定的情形为借口，拒绝他国的司法协助请求。虽然公约要求被请求方在拒绝合作时告知原因，但被请求方在解释涉及国家政治、主权、安全的原因时通常只会模糊处理，请求方往往只能无奈地面对。在更为极端的情况下，一个可能承担网络犯罪国家责任的缔约国甚至会以此规定为挡箭牌，阻碍他国对其从事网络犯罪行为的调查。[②] 各缔约国进行国际合作的例外条款极易演变成缔约国寻求“司法保护主义”的庇护伞。

公约内容中有关未经缔约方同意即可跨境取证的条款（第 32 条 b 款）很可能会对缔约国的国家主权造成冲击。该条规定，“缔约方可不经另一方的授权允许，a. 获取公开的存储计算机数据；b. 或是从获得法律授权、有权披露数据的个人那里，在征得其自愿、合法的同意后获取位于另一缔约方境内的数据。”撇开获取公开数据不谈，该公约并未就该条 b 款中所提到的情形给出明确解释。公约制定者还认为条款中涉及的“获得法律授权的个人”是一个需要结合背景具体分析的概念。[③] 这就给缔约方实施该条款带来了极大的灵活性：首先，该条款赋予了缔约国在另一缔约国官方不知情的情况下访问或接收位于后者境内的非公开数据的可能性，无疑是对缔约国司法主权的冲击；其次，公约并未定义“计算机数据”的范围，故涉及一国国家安全、军事利益的数据也将包含在内，无形中是对网络间谍行为大开绿灯；再次，为表面上满足公约所规定的“合法而自愿的同意”的条件，不排除一些缔约国会对数据权利人采取贿赂、威胁、欺骗等非法手段。

---

① Cybercrime Convention Committee (T-CY), Information Document concerning the Opinion of the Committee of Experts on Terrorism (CODEXTER) on Cyberterrorism and Use of Internet for Terrorist Purposes, available at http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/T-CY% 20 (2008)% 20INF% 2002% 20E.pdf (last visited October 18, 2016).

② Shannon L. Hopkins, “Cybercrime Convention: A Positive Beginning to a Long Road Ahead”, (2003) 2 *Journal of High Technology Law*, p. 108.

③ Explanatory Report to the Convention on Cybercrime, para. 294.

虽然公约委员会已发布了指导说明来解释这一极具争议的条款，但该指导说明也承认，除了当前可预见的，个人或互联网服务提供者同意将其在他国服务器上所存储的数据提供给执法部门，或是网络犯罪嫌疑人同意将其电子邮箱中有关犯罪的证据提供给警方等情形外，公约对其他情形既未授权也未阻止。① 可见，公约制定者尚待澄清该条款的含义与适用，现实中缔约国如何“自圆其说”地适用该条款就更为模糊了。此外，该条款无法提出保留，一旦成为缔约国，就必然面临适用该条规定的风险。

第三，公约的加入程序复杂，缔约国数量迄今仍然有限。公约第 37 条规定，非欧委会成员国加入公约须由部长委员会征得缔约国的一致同意，然后在部长委员会的投票中获得 2/3 以上多数的支持，并取得列席委员会投票的缔约国代表的一致支持，方可获邀请加入公约。实践中，受邀程序还包括欧委会秘书长与成员国的非正式磋商以及法律合作特别小组（GR-J）的讨论等流程。可以说，上述程序的复杂性以及获得缔约国全体一致同意的不确定性使得许多非欧委会成员国在是否加入公约的问题上打了退堂鼓。考虑到复杂的加入程序已成为公约“全球化”的一大障碍，欧委会曾就简化加入程序提出相关方案。但该方案虽然取消了取得缔约国一致同意的要求，却又增加了公约委员会的审议或犯罪问题委员会审议的环节，依然未解决程序繁琐的问题。②

受制于繁琐的加入程序等因素，公约自 2003 年生效以来，拓展缔约国的进程十分缓慢。下图是《网络犯罪公约》历年加入国家统计表。从表上看，公约每年新增缔约国数量为 2—7 个不等，其中 2006 年和 2012 年分别达到了 7 个和 6 个。考虑到公约开放前期（2002—2011 年）新增缔约国数量主要为欧委会成员国，且近年来未加入公约的成员国数量日趋减少的因素，近 3 年（2013—2015 年）新增缔约国数量则明显暴露出“后劲不足”的态势，仅稳定在 3 个左右。由于今后公约将主要以争取非欧委会成员国加入为目标，其难度必然大于争取其成员国的加入。故可以预见的是，除非取得突破性的进展，公约在今后几年每年新增的缔约国数量不会多于 3—4 个，离实现 100 个缔约国都显得遥遥无期，更不用说发展成为全球性公约了。

《网络犯罪公约》新增缔约国数量年度统计表《网络犯罪公约》新增缔约国数量年度统计表③

年份	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
成员	2	2	4	3	6	3	2	3	4	2	4	1	2	1	1
非成员	0	0	0	0	1	0	0	0	0	0	2	2	1	2	1
合计	2	2	4	3	7	3	2	3	4	2	6	3	3	3	2

第四，公约的修订至今缺乏实质性进展，无法反映后加入公约的非欧委会成员国的利益。作为后加入公约的非欧委会成员国，其虽无须承担欧委会成员国及观察员国在条约谈判阶段付出的

① Cybercrime Convention Committee（T-CY），T-CY Guidance Note #3 Transborder Access to Data（Article 32），3 December 2014，available at https：//rm. coe. int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId = 09000016802e726a（last visited October 18，2016）.

② Cybercrime Convention Committee（T-CY），Criteria and Procedures for accession to the Budapest Convention on Cybercrime-Update，28 May 2012，available at http：//www. coe. int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_ 2012_ 12_ E_ accessprocedure. pdf（last visited October 18，2016）.

③ 由本文作者统计，其中 2016 年数据截止到当年 9 月为止，来源：http：//www. coe. int/en/web/conventions/full-list/-/conventions/treaty/185/signatures? p_ auth = iyiWghKH，最后访问时间：2016 年 10 月 18 日。

成本，却必然要承担公约内容难以反映其利益和关切的弊端。[①] 对此，虽然公约规定了可保留条款，但这仅减少了公约对这些国家可能产生的不利影响，后加入的缔约国依旧无法在公约中纳入其主张和关切。

虽然欧委会为打消这一顾虑，许诺后加入的缔约国可以参与到公约未来的发展与修订中。[②] 但实践表明这只是一张空头支票，原因于下。首先，公约设定了复杂程度堪比加入程序的修订程序。虽然新加入的缔约国有权提出公约修订的建议修正案，但该修正案需由欧委会成员国、参与公约起草的非成员国等各方在公约委员会的框架下讨论，形成文件提交犯罪问题委员会。部长委员会在参考犯罪问题委员会意见的基础上，提交各缔约国表决。其次，即使是顺利地走完上述程序，依照公约解释性报告的要求，建议修正案也只能对公约进行微调或小幅修改。若要进行重大调整，如对公约的加入程序等进行修订，则须通过附加议定书以实现。[③] 然而公约至今仅有 2003 年有关种族主义和排外主义言论定罪的唯一一份附加议定书，该议定书也只是因为各方争议太大才从公约中独立出来。故自公约生效以来，实质上并没有一份旨在修订公约内容的附加议定书出台。公约委员会虽然声称自 2012 年起已经在讨论起草有关云计算技术背景下跨境获取数据的第二附加议定书，但该议定书至今尚未成形；[④] 再次，考虑到通过修正案与附加议定书修订公约的可行性不高，公约委员会目前更倾向于通过发布指导说明（Guidance Note）实现对公约的修订与发展。具体而言，新加入的缔约国可向公约委员会提出修订公约的建议，供各方讨论后形成指导说明，作为缔约国履行公约的指导性文件。虽然这一方式极大地简化了程序，但其本身只是具有“软法”性质的文件，缺乏约束力，具体效果取决于缔约国的自觉履行，实际作用存疑。

由以上分析可知，无论是从制定平台、公约内容、加入程序以及修订程序来看，欧委会《网络犯罪公约》的局限性均十分明显。若非经历重大修订，实难为非缔约国接受，更不用说发展成为全球标准。《网络犯罪公约》尚且如此，其他如非洲盟、阿拉伯国家联盟、上海合作组织等创立的区域性机制就更无“全球化”的可能了。

三　打击网络犯罪国际法机制的前景及对中国的相关工作建议

（一）打击网络犯罪国际法机制的前景与评析

《网络犯罪公约》自 2001 年出台以来，已历经近 16 个年头。正如前文所述，虽然在其带动下，其他区域类似的国际法机制得到了长足发展，但全球层面始终缺乏具有普适性的打击网络犯罪的国际法机制，这与在网络犯罪领域国际社会面临的日益严峻的挑战根本上不相匹配。国际社

① Vincy Fon, Francesco Parisi, “the Formation of International Treaties”, (2007) 3 *Review of Law and Economics*, pp. 37 – 38.

② Brian Harley, “A Global Convention on Cybercrime”, *Columbia Science and Technology Law Review*, March 23 2010, available at http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (last visited October 18, 2016).

③ Explanatory Report to the Convention on Cybercrime, para. 323.

④ T-CY Work Plan for the Period 1 January 2014 – 31 December 2015, available at http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680473d79 (last visited October 18, 2016).

会已经认识到问题的症结所在，联合国预防犯罪与刑事司法委员会（United Nations Commission on Crime Prevention and Criminal Justice，简称 CCPCJ）下设的网络犯罪政府专家组在其发布的《网络犯罪问题综合研究报告》（Comprehensive Study on Cybercrime）中，便提出包括制定打击网络犯罪国际示范条款及综合性的多边法律文书等举措来加强现有的国家以及国际社会应对网络犯罪的法律措施，这也为未来打击网络犯罪国际法机制的发展点明了方向。[①] 事实上，由于相关国际示范条款并不具备约束力，其本身是旨在指导各国国内立法以及国际立法，因此，未来国际法机制发展的关键还是制定综合性的全球法律文书。当前，围绕构建这一国际法机制，各国主要有下列两种思路。

一是推动现有区域性法律文书全球化。在现有的区域性法律文书中，《网络犯罪公约》作为一项综合性的公约，最具可能发展成全球性公约的立法基础。[②] 事实上，美欧等公约缔约国近年来也的确在联合国、“伦敦进程”、七国集团首脑会议（G－7 Summit，简称 G7）等多个场合倡议该公约的“全球化”：如在 2016 年 5 月举行的七国领导人伊势志摩峰会通过的网络领域成果文件《G7 网络共同原则与行动》中，就明确提出要鼓励更多国家加入公约；[③] 在 2015 年第十三届联合国预防犯罪与刑事司法大会上，美欧等发达国家普遍认为公约是全球合作的适当框架，足以有效应对网络犯罪构成的挑战。[④] 英国外交大臣黑格（William Hague）在 2011 年“伦敦进程”网络空间大会的闭幕演讲中也强调各方对《网络犯罪公约》的普遍支持，认为当前无须制定新的公约。[⑤]《网络犯罪公约》委员会秘书长亚力山大（Alexander Seger）在国际网络犯罪大会的发言中也声称最大限度地适用现有标准，如《网络犯罪公约》，是应对网络犯罪最有效的对策，实质上也是希望该公约能发展为全球标准。[⑥] 此外，美国国务院网络事务协调员佩因特（Christopher Painter）近期在参议院网络政策听证会上阐述美国网络战略执行情况时，亦强调美国通过推广欧委会《网络犯罪公约》来促进网络犯罪实体和程序法律的国际协调。[⑦]

不过，美欧等公约缔约国的上述努力并未被包括中俄在内的新兴国家及广大发展中国家接

---

① United Nations Office on Drugs and Crime, supra note 1, p. xii－xv.

② 从涉及的内容范围来看，阿拉伯国家联盟的《打击信息技术犯罪公约》与《网络犯罪公约》一样，都属于综合性的网络犯罪公约，涉及了定罪、管辖权、程序规则以及国际合作等多个领域，但其条款……从缔约国数量来看，《网络犯罪公约》的缔约国数量最多，且涵盖了欧、亚、美洲等多个国家；其他如《打击信息技术犯罪公约》不仅缔约国数量较少，而且仅限于特定区域。

③ G7 Ise-Shima Summit, G7 Principles and Actions on Cyber, May 26－27, 2016, available at http://www.mofa.go.jp/files/000160279.pdf (last visited October 18, 2016).

④ Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, Report of Committee I － Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation (Item 5) (Agenda item 5 Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime), April 12－19, 2015, p. 4, available at http://www.unodc.org/documents/congress//Documentation/IN_SESSION/ACONF222_L3ADD1_e_V1502497.pdf (last visited October 18, 2016).

⑤ Foreign Secretary William Hague spoke at the end of the London Conference on Cyberspace on 2 November, available at https://www.gov.uk/government/speeches/foreign-secretarys-closing-remarks-at-the-london-conference-on-cyberspace (last visited October 18, 2016).

⑥ Alexander Seger, “the Budapest Convention on Cybercrime 10 years on: Lessons learnt or Web is a Web”, p. 5.

⑦ Christopher Painter, Statement before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, May 25, 2016, available at http://www.state.gov/s/cyberissues/releasesandremarks/257719.htm (last visited October 18, 2016).

受。笔者认为，这固然与网络国际法领域各国意识形态和立场主张分歧有关，比如以中俄为代表的新兴国家和发展中国家主张以联合国为框架制定新的国际法律文件，强调加强网络信息内容监管和打击网络恐怖主义，主张互联网服务商及用户应当配合执法机关开展网络犯罪调查；而美欧等发达国家则主张现有国际法在网络空间的阐释适用足以应对网络安全威胁，互联网信息传播自由与隐私保护，反对执法机关开展网络犯罪调查时侵犯互联网服务商和用户的隐私。① 但根本原因还是在于公约自身的局限性明显，这一点已在本文第二部分作详细分析，在此不作赘述。

二是在联合国框架内制定新的全球性网络犯罪公约。以中国、俄罗斯为代表的新兴国家和发展中国家则倡议在联合国框架内谈判制定新公约，认为新公约的制定可参考欧委会《网络犯罪公约》等区域性法律文书的规则，同时补充反映发展中国家关切和主张的内容。② 为此，中俄等国在联合国大会第三委员会、联合国预防犯罪与刑事司法委员会以及联合国预防犯罪与刑事司法大会（United Nations Crime Congress）等国际组织平台积极呼吁各国支持制定新公约的倡议。2010 年，在中俄等新兴国家和其他发展中国家推动下，联合国预防犯罪与刑事司法大会在成果文件《萨尔瓦多宣言》中提请预防犯罪和刑事司法委员会设立一个不限成员名额的政府间专家组，全面研究网络犯罪问题以及各成员国、国际社会和私营部门就此采取的对策，包括国家立法、最佳做法、技术援助和国际合作交流等，以期审查各种备选方案，完善现有的并提出新的具体对策。③ 该专家组至今已举行两次会议，并在 2013 年举行的第二次会上发布了《网络犯罪问题综合研究报告》，提出制定打击网络犯罪国际示范条款及综合性的多边法律文书，以及加强对发展中国家预防和打击网络犯罪的技术援助等对策。

但该专家组自成立以来，由于欧委会《网络犯罪公约》的缔约国反对制定全球性法律文书，讨论进程一度因此陷入停顿。④ 笔者认为，上述情形反映了美欧发达国家与发展中国家关于网络犯罪国际立法主导权的博弈。但美欧反对制定新公约的主张缺乏应有的说服力：一方面，根据前文分析，《网络犯罪公约》目前并不具有发展成为全球性法律文书的基础；另一方面，无论是从打击跨国犯罪还是其他领域的国际和地区实践看，以已有区域性公约为由反对制定全球性公约极

---

① 但近来美欧迫于网络反恐的严峻形势，在保护互联网信息传播自由问题的态度上似有一定程度转变：2016 年 5 月 31 日，欧盟委员会和微软、脸书、推特、油管等互联网巨头共同发布“反在线非法仇恨言论行为准则”（Code of Conduct on Countering Illegal Hate Speech Online），要求互联网企业根据欧盟成员国执法机关的通报或公民社会组织等的举报，及时审查相关在线不法内容，并对其予以删除。无独有偶，2016 年 1 月，美国务院、司法部及其他相关情报部门高级官员与苹果、脸书、推特等互联网巨头举行峰会，研究探讨如何辨别过滤网络恐怖主义信息。相关内容可参见：http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.；http://money.cnn.com/2016/01/08/technology/white-house-isis-silicon-valley?iid=EL（last visited October 18，2016）.

② 参见《中国代表团出席“联合国网络犯罪问题政府间专家组”会议》，中国驻维也纳和其他国际组织代表团新闻，2013 年 3 月 14 日，http://www.fmprc.gov.cn/ce/cgvienna/chn/drugandcrime/crime/t1018227.htm，最后访问时间：2016 年 10 月 18 日。

③ The Twelfth UN Crime Congress，Salvador Declaration on Comprehensive Strategies for Global Challenges：Crime Prevention and Criminal Justice Systems and Their Development in a Changing World，A/RES/65/230，December 21，2010，available at http://www.un.org/ga/search/view_doc.asp?symbol=a%2Fres%2F65%2F230&Submit=Search&Lang=E（last visited October 18，2016）.

④ 事实上，自 2013 年专家组发布《网络犯罪问题综合研究报告》并召开第二次会议后至今，专家组并未召开后续会议。2016 年 2 月，专家组秘书处联合国毒品和犯罪问题公办室发布了《报告》除英文版以外的其他联合国官方语言的版本，并照会 CCPCJ 成员国，要求于 8 月 31 日前就报告提交政府评论，具体可参见：http://www.unodc.org/documents/organized-crime/Cybercrime_Comments/CU_2016_50_English_sample.pdf.；http://www.unodc.org/documents/organized-crime/Cybercrime_Comments/CU_2016_133_English_sample.pdf（last visited October 18，2016）.

为罕见。以国际反腐败领域为例，《联合国反腐败公约》就是在《美洲反腐败公约》、欧盟《打击涉及欧洲共同体官员或欧洲联盟成员国官员的腐败行为公约》、欧委会部长《反腐败刑法公约》、《反腐败民法公约》等已有的区域性法律文书的基础上发展而来。[①] 因而区域性公约和全球性公约本身并不相互矛盾和冲突。因此，参照其他领域已有的国际实践，在借鉴已有的区域性法律文书的基础上，以联合国为平台谈判制定全球性公约，既具有广泛代表性，又可加强和补充区域性公约的作用，是当前构建全球层面打击网络犯罪国际法机制，弥补空白的不二选择。

总体来看，美欧等西方国家与中国、俄罗斯、巴西等新兴国家和发展中国家围绕推广欧委会《网络犯罪公约》和制定新公约展开的博弈，实质是各方在网络犯罪领域的国际标准主导权之争。由于网络国际立法关乎各国的政治、经济和安全利益，相互间不会轻易让步，因此本文预计各国围绕这一“国际法律标准之争”的博弈还将继续持续下去。

（二）对中国参与网络犯罪国际法机制构建的相关建议

中国已经在联合国大会等多个国际场合阐明了支持在联合国框架下谈判制定一份全面均衡的打击网络犯罪的国际公约的观点，并强调支持联合国网络犯罪政府专家组就此继续开展相关研究工作。但这仅仅是立场宣示，要实现制定全球性公约的目标，还需要有明确可行的实现路径和方式，包括：通过哪些步骤、路径推动制定一份全球性公约，该全球性公约的内容如何构建，对美欧力推《网络犯罪公约》的举措应如何统筹应对，等等。针对上述相关问题，本文初步提出以下建议。

近年来，中国已通过建立中美打击网络犯罪及相关事项高级别联合对话、中欧网络工作小组、中俄信息安全政府磋商、东盟地区论坛等双多边对口磋商渠道，同美国、俄罗斯、欧盟、东盟等网络技术发达的国家和重要的地区性国际组织建立了密切的合作关系，是否加入公约对中国目前开展网络犯罪国际合作没有实质性影响。在美欧推动公约“全球化”、争取更多域外国家加入的情况下，中国可以考虑加入公约，同时争取美欧等发达国家支持在联合国框架下制定网络犯罪公约或中国倡导的其他网络安全法律文书如“信息安全国际行为准则”[②]，以实现中国参与主导网络安全国际规则制定的目标。

同时，中国可通过多双边等渠道，以与新兴国家和发展中国家合作为依托，通过制定网络犯罪示范条款等方式推动全球性公约的制定。一方面，中国应通过现有的中美、中欧等双边网络犯罪、网络安全磋商机制，与美欧等发达国家加强对话，通过交流立场与观点，促使这些国家理解并支持中国推动制定全球性公约的倡议。另一方面，中国应加强与俄罗斯、巴西、印度等新兴国家及其他发展中国家在打击网络犯罪领域的合作。一是通过现有的金砖国家信息安全工作组、上海合作组织信息安全专家组等平台，研究和提出打击网络犯罪全球性公约的草案，进而提交联大

① 参见《联合国反腐败公约》序言，来源：http：//www. un. org/zh/events/anticorruptionday/convention. shtml，最后访问时间：2016 年 10 月 18 日。

② 《信息安全国际行为准则》（A/66/359）系 2011 年中国、俄罗斯、塔吉克斯坦和乌兹别克斯坦共同向第六十六届联大提交的倡议文件，希藉此推动国际上关于信息安全国际准则的辩论，并帮助及早就此问题达成共识。吉尔吉斯斯坦和哈萨克斯坦于不久后加入成为共同提案国。2015 年 1 月，上述 6 国向联合国大会共同提交了新版“信息安全国际行为准则”（A/69/723）。具体可参见外交部网站，《信息安全国际行为准则》，http：//infogate. fmprc. gov. cn/web/ziliao_ 674904/tytj_ 674911/zcwj_ 674915/t858317. shtml，最后访问时间：2016 年 10 月 18 日。

开展相关讨论。二是尽可能地推动专家组尽快召开后续会议，继续探讨全球和国家层面应对网络犯罪的具体举措。三是注重通过专门的国际法平台如亚洲—非洲法律协商组织（简称“法协”）等，研究和提出打击网络犯罪国际文书草案，为中国在联合国框架下推动相关倡议提供有力的智力支持。法协是根据万隆会议的决定于1956年成立的亚非两大洲在国际法领域唯一的政府间国际组织，中国、印度、南非、日本、韩国等均为其成员国。[①] 在2015年4月举行的第54届亚非法协年会上，经中方倡议，会议通过相关决议，设立不限名额的“网络空间国际法”工作组，讨论网络空间国家主权、和平利用网络空间、打击网络犯罪国际合作法律规则等网络空间国际法问题。[②] 2016年5月，该工作组在亚非法协第55届年会期间举行首次会议并通过决议，授权工作组下一步通过举行会间会等方式继续研讨54届年会决议中所列的网络空间国际法问题，尤其是要考虑到亚非国家打击网络犯罪的需求。[③] 本文认为，既然工作组有明确授权，中国可以借助工作组平台，推动研究和制定专门针对亚非国家需求的网络犯罪示范条款，既服务于亚非国家打击网络犯罪的需要，也为今后制定全球性公约“投石问路”。

构建未来的全球性公约，除借鉴《网络犯罪公约》等现有的国际法机制及其包含的实体法、程序法、国际合作条款外，还应在公约中明确网络主权等根本性问题，并力争纳入网络反恐等内容。具体来说，现有的国际法机制往往并未回答网络的性质以及网络主权等问题，只是简单地列举需要打击的网络犯罪罪行及国际合作条款，这适合立场主张相近的国家来适用，却并不易被其他国家所认同。而未来的期望得到广泛认同的全球性公约，在谈判过程中各方首先就要就网络的属性、网络主权等根本性问题达成共识，进而探讨具体的罪行。而在未来的全球性公约中明确网络主权概念，就是明确国家作为主权主体，享有依法对网络空间行使管理、打击网络犯罪的权力，这也是全球性公约具有执行力的重要保障。另一方面，还应在未来的全球性公约中纳入相应的新内容，如就网络恐怖主义活动定罪等。作为严重的网络犯罪形式，网络恐怖主义活动近年来愈演愈烈。但美欧国家以保护网络自由为由，长期消极看待网络恐怖主义问题。近两年来，随着美欧国家逐渐成为网络恐怖主义危害的主要对象，其在网络恐怖主义问题上的立场亦有所转变。鉴于此，在未来谈判制定网络犯罪公约时，应力争将网络反恐纳入公约，以实现对网络恐怖主义的罪责刑相适应。

四　结语

打击网络犯罪全球性国际法机制的“道路选择”问题，即是制定新公约还是立足欧委会《网络犯罪公约》等现有国际法律文书，是当前国际上打击网络犯罪领域争论的核心焦点问题。现阶段发展中国家和发达国家两大阵营在该问题上立场相异，取得的进展有限。本文认为，从整

① 外交部新闻，《亚非法协第54届年会在京成功举行》，2015年4月29日，来源：http://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/tyfls_674667/xwlb_674669/t1259018.shtml，最后访问时间：2016年10月19日。。

② AALCO, Resolution of 54th Annual Session on International Law in Cyberspace, available at http://www.aalco.int/54thsession/resolutions2015/RESOLUTION%20ON%20_INTERNATIONAL%20LAW%20IN%20CYBERSPACE_%20as%20on%2015%20April.pdf (last visited October 19, 2016).

③ AALCO, Resolution of 55th Annual Session on International Law in Cyberspace, available at http://www.aalco.int/Final%20Resolutions%202016.pdf (last visited October 19, 2016).

个网络空间国际规则博弈和发展形势看，打击网络犯罪问题与网络领域的其他问题，如国际法适用、互联网治理问题相比，已具备较好的国际立法基础，各国在该领域也有着较迫切的合作需求与较成熟的司法实践，极有可能成为网络空间全球性国际法规则制定取得进展的首要突破口。因此，中国应把握住这一形势，迎难而上，主动参与并推动开展相关谈判，有力推动打击网络犯罪全球性法律文书的谈判和制定，积极争取网络空间国际规则制定的主导权。

The Problems and Prospects of the International Legal Regimes in Combating Cybercrimes ——From the Perspective of Council of Europe's Convention on Cybercrime

Hu Jiansheng and Huang Zhixiong

Abstract: The Council of Europe's Convention on Cybercrime ("the Convention"), which entered into force in 2004, is the most influential regional legal instrument in the field of combating cybercrimes. The Convention not only provides the primary legal basis for the member states of the Council of Europe in fighting cybercrimes, but also influenced the domestic legislation of many non-member states including China. Meantime, it contributed to the quick development of other regional international legal regimes. However, at the global level, the international legal regimes in combating cybercrimes are featured by fragmentation, and it is difficult for existing regional regimes including the Convention to evolve into global legal standards due to their own limitations. Thus, it is time for the international community to consider the draft of a new comprehensive global legal instrument. Currently, there is a confrontation between the United States and other western countries' attempt to globalize the Council of Europe's Convention on Cybercrime on the one hand, and the desire of emerging economies and developing countries such as China, Russia and Brazil to make a new convention on the other hand. Against this background, this article offers some insights into the future development of international legal regimes for combating cybercrimes, and suggests the strategies for China's participation in constructing the relevant regimes.

Keywords: Cybercrime, Council of Europe's Convention on Cybercrime, International Legal Regimes for Combating Cybercrimes, Comprehensive Global Legal Instrument

（责任编辑：曲相霏）