

# 论网络犯罪刑事管辖权的国际冲突与规制

虞文梁

**内容提要:**刑事管辖权是国家发动刑罚权的前提,网络刑事管辖的积极冲突已成为当前网络犯罪国际治理的重要瓶颈。传统刑事管辖权在网络空间“水土不服”引发管辖的消极实现;网络空间政治化、扩张化和阵营化等“三化现象”进一步加剧了管辖的冲突。在冲突归因上,存在网络无国界化、犯罪行为难溯化、刑事立法滞后化、犯罪治理“巴尔干化”等多维度因素。在发展现状上,国内外学界的研究尚未形成统一认识,联合国力推全球性公约但阻碍重重,中国积极探索与“网络空间命运共同体”相匹配的管辖权制度,美欧等西方国家意欲不断扩张管辖主张。在冲突焦点上,存在扩张性与谦抑性的原则性摇摆,霸权主义与主权主义的体系性博弈,“硬法不硬”与“软法不软”相向而行等内、外源性冲突。对此,要平衡扩张性与谦抑性的关系,“求同存异”地寻求最大公约数,为推动建立公正、合理和有序的全球网络治理秩序提供中国方案。

**关键词:**网络犯罪 刑事管辖权 管辖冲突 刑法规制

虞文梁,中国法学会法治研究所助理研究员。

## 一 问题的提出

当前网络空间正处在类似于“西部拓荒”的野蛮生长期,各类网络犯罪大量迸发。根据“世界经济论坛”(WEF)2022年1月发布的《2022年全球风险报告》,2020年恶意软件和勒索病毒的网络威胁分别增加了358%和435%,已超出国际社会能够应对的范围。<sup>[1]</sup>而该组织发布的《2020年全球风险报告》<sup>[2]</sup>将网络犯罪列为全球治理未来十年的第二大风险,认为2021年全球6万亿美元损失额足以比肩全球第三大经济体,而美国对网络犯

[1] See *The Global Risks Report 2022*, World Economic Forum (January 15, 2022), [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2022.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf), 最近访问时间[2022-03-18]。

[2] See *The Global Risks Report 2020*, World Economic Forum (January 15, 2020), [https://www3.weforum.org/docs/WEF\\_Global\\_Risk\\_Report\\_2020.pdf](https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf), 最近访问时间[2022-03-18]。

罪的起诉率却不足 0.05%。国际刑警组织 2020 年报告显示,新冠肺炎疫情期间全球针对医院、诊所和医疗公司的网络攻击暴增。<sup>[3]</sup> 高威胁风险、低效能治理的对比足以说明,网络犯罪治理已成为全球治理中不可忽视的重大难题。

作为“应对‘首要威胁’的起点”,<sup>[4]</sup> 刑事管辖权是国家行使国家主权的重要形式,也是国家发动刑罚权的重要前提。刑事管辖权问题是数字时代极为严重的挑战,因为它关系到国际和国家管辖权间的相互关系、跨界活动和域外后果。<sup>[5]</sup> 由于传统犯罪的行为、主体和结果等要素均与现实空间的相应物理坐标相关联,但在网络数字化时代,网络犯罪行为产生了溢出效应,各种新问题、新情况和新挑战让传统刑事管辖权在网络空间遇到诸多不适应,例如国际云服务商的基础设施分散于不同国家、不同法律和不同管辖权下,<sup>[6]</sup> 很容易出现不同国家国内法同时扩张适用的冲突情形。同时,刑法适用必须受到国际法的限制,任何国家不能恣意地无限扩大本国刑法的适用范围,忽视他国在国际法上的权利而任意地主张界定刑罚权限的权力,以彰显本国绝对主权。<sup>[7]</sup> 但出于最大程度维护本国利益的需要,很多国家功利性地积极主张或者有选择性地积极主张本国刑事管辖权。一方面,采取“合则管、不合则弃”的选择性扩张管辖,即对不在本国管辖范围内但符合本国利益的案件想方设法地予以管辖,而对在本国管辖范围内却没有直接利益关系的案件却置之不顾。另一方面,对于只要符合自身利益的,部分国家宽泛地主张“应管尽管、能管尽管”,实施扩张性保护管辖或长臂管辖,不遵循国际法中尊重他国主权的要求,漠视甚至抵制他国行使网络主权和刑事管辖权,严重背离了国际法“合理原则”和“礼让原则”,容易滋生“网络霸权主义”“网络欺凌主义”等倾向。<sup>[8]</sup> 这种行为进一步加剧网络犯罪治理的复杂性,客观上容易引发国家间刑事管辖权的积极冲突和消极实现。由此可见,当前国际网络空间治理的重心不仅在于网络治理本身,还在于网络治理的国家间主导权的博弈上,即网络犯罪刑事管辖权的政治化、扩张化和阵营化“三化现象”,对建立与数字化时代相匹配的网络犯罪刑事管辖权制度提出了新的迫切需求。

## 二 网络刑事管辖冲突的归因

随着人类活动深度融入“第五空间”,许多全新复杂的问题应运而生,致使现有国际法和国际机制已难以满足虚拟空间发展的客观需要。<sup>[9]</sup> 网络管辖权不仅是一个法律问

[3] See Justin Malzac, Leveraging Domestic Law against Cyberattacks, 11 *National Security Law Brief* 1, 1-2 (2021).

[4] 参见郭烁:《应对“首要威胁”的起点:网络犯罪管辖研究》,《求是学刊》2017年第5期,第104页。

[5] See Yulia Razmetaeva, Hanna Ponomarova & Iryna Bylya-Sabadash, Jurisdictional Issues in the Digital Age, 10 *Ius Humani, Revista de Derecho* 167, 166-169 (2021).

[6] See Divyraj Ray, Cloud Computing and Challenges Faced in Existing Legal Structure, 2 *Jus Corpus Law Journal* 257, 257-262 (2021).

[7] 参见刘艳红:《论刑法的网络空间效力》,《中国法学》2018年第3期,第90页。

[8] 参见吴海文、张鹏:《打击网络犯罪国际规则的现状、争议和未来》,《中国应用法学》2020年第2期,第197-200页。

[9] 参见《中国代表在中美互联网论坛上的发言》,载中国国际法学会主办《中国国际法年刊(2013年)》,法律出版社2014年版,第666页。

题,还是政治问题和全球治理问题。全球性网络国际规则制定面临着网络霸权、阵营分野、平台碎片化以及约束力不足等阻碍,<sup>[10]</sup> 属地管辖在网络空间不但延续了现实物理空间的难题,还受到了扩张新网络殖民地等冲击。<sup>[11]</sup>

### (一) 网络犯罪行为具有复杂的时空性和无国界性

信息技术的发展推动形成了一个平行于现实物理世界的网络虚拟世界。传统的主权国家治理模式以国内犯罪为主,跨国犯罪的案发数量和频率远低于单纯的国内犯罪。由于全球网络信息产生、传播和流通等行为具有虚拟性、即时性、无边界性等特征,网络犯罪行为时空要素都以“数字化生存”<sup>[12]</sup> 的形式存在,网络“跨境”比现实世界“跨境”更加容易,网络犯罪活动主体、客体、对象、行为等要素可能跨越多国“网络边境”,从而打破了现实国家边界的藩篱,地域在网络空间中不再具有实质意义。<sup>[13]</sup> 基于全球信息交互所形成的新型社会关系,不仅让传统犯罪开始出现向网络化和数字化的整体转型,同时网络恐怖主义、供应链渗透、勒索病毒、数据泄露和非法跨境执法等新型犯罪威胁快速上升,传统刑事管辖权对此难以适应,给网络犯罪治理,特别是给网络犯罪管辖带来了很大的不确定性,国家在刑事侦查与刑事诉讼中的数据跨境获取受阻。<sup>[14]</sup> 确立网络犯罪管辖权成为一项复杂的系统工程。

### (二) 网络犯罪行为溯源具有较强的不确定性

由于网络空间具有开放性、匿名性和通信路径的不确定性等特征,网络犯罪的溯源与取证变得异常困难。首先,网络证据链的完整性要求和脆弱性现状形成鲜明的对比,成为国际网络刑事司法中的重大难题。为逃避司法机关的侦查与取证,网络犯罪主体往往采取多重隐匿身份和行为等措施,也会采取抹除、改变或伪造与犯罪行为相关电子痕迹的措施,导致司法机关在发现、侦查、取证、起诉等环节面临重重困难。2020 年国际刑警组织报告称,犯罪分子越来越多地利用执法管辖的地域限制,通过在全球范围内开展犯罪活动来躲避侦查。<sup>[15]</sup> 可以用于证明案件事实的电子数据也呈现出全球分散分布和高速传输的特征,进而使得跨境数据取证成为网络信息时代打击犯罪的新常态。<sup>[16]</sup> 其次,全球网络犯罪产业化正在形成。网络犯罪的高利润回报、低犯罪风险的特点直接催生了全球化的黑色、灰色产业链的成熟与发展,并有向全球完整产业化供应链的方向发展的趋势。专业性网络犯罪团伙的组织化、国际化、协作化的水平越来越高,并可以在全球范围内针对

[10] 参见方芳、杨剑:《网络空间国际规则:问题、态势与中国角色》,《厦门大学学报(哲学社会科学版)》2018 年第 1 期,第 23 页。

[11] 参见刘艳红:《论刑法的网络空间效力》,《中国法学》2018 年第 3 期,第 91 页。

[12] 参见齐爱民、祝高峰:《论国家数据主权制度的确立与完善》,《苏州大学学报(哲学社会科学版)》2016 年第 1 期,第 84 页。

[13] 参见李晓明、李文吉:《跨国网络犯罪刑事管辖权解析》,《苏州大学学报(哲学社会科学版)》2018 年第 1 期,第 91 页。

[14] 参见吴琦:《网络空间中的司法管辖权冲突与解决方案》,《西南政法大学学报》2021 年第 1 期,第 47 页。

[15] See Interpol, *Interpol's Comments - 6<sup>th</sup> Meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime* (22 July 2020), [https://www.unodc.org/documents/Cybercrime/IEG\\_cyber\\_comments/INTERPOL.pdf](https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/INTERPOL.pdf), 最近访问时间[2022-03-18]。

[16] 参见裴炜:《论网络犯罪跨境数据取证中的执法管辖权》,《比较法研究》2021 年第 6 期,第 30 页。

国家、组织和个人等发动协调一致的网络犯罪活动。最后,犯罪主体更加复杂多元,不再局限于传统犯罪中的小型犯罪组织、个人等非国家行为体,国家行为体和有国家背景的职业犯罪组织、国际性有组织犯罪组织等类国家行为体逐渐成为重要的行为主体,网络安全问题正成为国际社会的分歧点而不是合作点。<sup>[17]</sup> 当网络犯罪被当成国家博弈工具时,国家间就难以在跨国溯源、全球打击网络犯罪合作等问题上形成统一战线。

### (三) 刑事立法缺位和滞后引发网络空间治理真空

从网络刑事立法外部考察,网络刑事管辖权制度的缺位是造成网络空间治理规则真空的一大主因。网络犯罪是无国界的犯罪,在网络犯罪管辖国际条约尚未达成时,在网络犯罪中适用普遍管辖原则缺乏法律依据和现实基础。<sup>[18]</sup> 与传统刑法的管辖权已经形成共识并建立了相应的配套理论和立法支撑所不同,各国对网络犯罪的国际刑事管辖权尚未形成共识,在国际协同上存在各种不同的主张和意见,加之各国网络建设、管理和使用等方面的能力与水平参差不齐,全球化的网络犯罪预防和惩治合作机制尚未有效地建立,国际社会难以合力应对跨国网络犯罪中出现的各种新情况、新问题,客观上导致了网络犯罪刑事管辖的积极冲突和消极实现的结果。

从网络刑事立法内部来考察,传统刑事立法在网络空间水土不服,难以应对数字时代的新问题。与传统犯罪中的行为地、中间地、结果地等要素较为明确不同,网络犯罪行为的这些要素相对模糊化和游离化,对相关行为的认定难以形成完整的闭环。这种状态导致传统刑法中的管辖权规定难以适应网络犯罪的管辖问题,对传统刑法管辖权理论提出了挑战,也为国际管辖带来了很大的障碍。传统刑法中管辖权制度与网络发展脱节,难以适应与应对网络犯罪的新形态。实害或者影响关联性标准是解决方案之一,但该标准具有形式较模糊、内容不确定、借鉴不充分、根据不明确等缺陷。<sup>[19]</sup> 如果以实害结果而非危害行为来作为判断标准,不仅导致只能以结果犯而非行为犯来认定,从而让很多犯罪行为无法得到制裁,同时,由于对行为、主体和结果等内容的认定是一个十分抽象、复杂并操作困难的问题,必然进一步加剧网络犯罪行为认定的困难。特别是在一些案例中,网络犯罪“实害”结果并不是立即发生或立即被发现,难以评估网络犯罪行为危害结果的大小并据此追究主体的责任。

### (四) 国际网络空间治理“巴尔干化”进一步提升全球治理难度和复杂度

在国际关系领域,“巴尔干现象”意味着不同政治力量相互割据与对立,整个局势呈现“碎片化”特征。当前国际网络治理中也呈现出“巴尔干化”的态势,各国在网络治理上的博弈与纷争不断,各自为政、甚至相互对立,冲突与对立表现在网络治理的主张、政策、立法、司法、资源、模式等不同维度,特别是在治理立场、治理模式和治理道路等方面存在巨大的分歧与冲突,导致难以形成全球性网络犯罪刑事管辖权规则,较大降低了国际社会

[17] See *The Global Risks Report 2022*, World Economic Forum (January 15, 2022), [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2022.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf), 最近访问时间[2022-03-18]。

[18] 参见陈结森:《关于我国网络犯罪刑事管辖权立法的思考》,《现代法学》2008年第3期,第93页。

[19] 参见刘艳红:《论刑法的网络空间效力》,《中国法学》2018年第3期,第89页。

协同打击网络犯罪的效能。在网络治理模式上,部分西方国家主张实行“多利益攸关方”的治理模式。由于这种治理模式反对国家拥有网络主权和网络管辖权,相关规则模糊、不透明,其主导权和解释权仍然牢牢掌握在部分西方国家手中,仅代表了部分西方国家的诉求和主张,事实上无法解决现在网络治理中的各种困境和问题,因而遭到了广大发展中国家的强烈反对。这种根本性分歧为网络犯罪的国际管辖权发展带来了巨大的影响,并形成网络犯罪治理的“巴尔干化”的发展态势,在全球网络治理中起着负面的作用。

### 三 全球网络犯罪刑事管辖权的发展现状

#### (一) 相关理论研究发展现状

当前,国内外理论界对网络犯罪刑事管辖权的研究和认识尚未形成统一定论。综合各国对网络犯罪的国际管辖的不同理论主张,主要包括以下几种观点:一是新主权理论,认为在网络空间形成独立于各国政府的全球性,社会拥有独立的组织形式、价值标准和规则。<sup>[20]</sup> 该理论实质是“伪无政府主义”的主张,一定程度上迎合了网络霸权主义的需求。二是扩大属地管辖理论,主张对既有属地管辖规则的解释,只要符合一定的条件就可以将刑事案件的管辖由现实空间的属地管辖运用于网络空间。<sup>[21]</sup> 该主张有利于以较小的成本和代价对接现实空间和网络空间的管辖权问题,但也存在普遍管辖权被滥用等风险。<sup>[22]</sup> 三是网络自治理论,认为网络属于类似公海、南极洲一样的全球公域,各国均可以以本国法律对网络空间任何人和任何行为实施自治管辖。<sup>[23]</sup> 该理论由于过于理想化,缺乏可操作性,同时其主张与反对的内容也相互矛盾。四是网址管辖理论,主张网址是行为人在网络空间的虚拟地址,对与网址相关联的地理位置案件拥有管辖权的法院对该地的网络犯罪拥有管辖权,网址所对应的服务器位置所在地是产生管辖权的基础。<sup>[24]</sup> 该理论忽视了网址的相对不确定性、可变性、易伪造性等特征,难以实现确定网络管辖权的目的。五是有限管辖原则,包括属人管辖关联说、属地管辖关联说、侵害法益关联说等。其中属人管辖关联说主张以属人管辖为基础,从犯罪行为对本国国家或者公民的侵害或者影响关联性为标准来判断是否具有刑事管辖权。<sup>[25]</sup> 属地管辖关联说主张以属地管辖原则为基础来建立有限管辖原则,侵害法益关联说则主张以该网络行为对刑法所保护的法益造成的实际损害作为判断的标准。<sup>[26]</sup> 该原则可以较好地解决网络信号“抽象越境”的管辖问题,<sup>[27]</sup> 但也存在侵害对象非完整性、关联性标准不明确等缺陷。六是实害联系原

[20] 参见郑泽善:《网络犯罪与刑法的空间效力原则》,《法学研究》2006年第5期,第75页。

[21] 参见屈学武:《因特网上的犯罪及其遏制》,《法学研究》2000年第4期,第98页。

[22] 参见陈结森:《关于我国网络犯罪刑事管辖权立法的思考》,《现代法学》2008年第3期,第94页。

[23] 参见孟传香:《关于网络犯罪国际刑事管辖权的思考》,《重庆邮电大学学报(社会科学版)》2011年第5期,第37页。

[24] 参见罗艺方、赖紫宁:《网络空间司法管辖理论比较研究》,《中南民族大学学报(人文社会科学版)》2003年第6期,第57页。

[25] 参见郑泽善:《网络犯罪与刑法的空间效力原则》,《法学研究》2006年第5期,第76页。

[26] 参见陈结森:《关于我国网络犯罪刑事管辖权立法的思考》,《现代法学》2008年第3期,第94页。

[27] 参见吴华蓉:《浅论网络犯罪刑事司法管辖权的建构》,《犯罪研究》2006年第4期,第70页。

则,主张属地管辖中的结果要素基于危险到实害的程度不同亦具有独立意义,<sup>[28]</sup>即要以实害标准作为判断的前提性根据。该原则其实是在有限管辖原则的基础上进一步主张将侵害或者影响关联性作为管辖的前提,从将危险犯剥离惩治范围,仅仅惩治实害犯,这一主张值得斟酌。此外,德国刑法学界还存在结果地限制说、双重可罚说等学说,<sup>[29]</sup>日本学界则存在特别连接点说、放弃普遍管辖原则说、空间效力原则与犯罪论整合说,<sup>[30]</sup>这些学说也各有利弊。

## (二) 联合国主导的国际立法努力

2003年12月,联合国信息社会世界峰会在日内瓦通过《原则宣言》(Declaration of Principles),提出“与因特网有关的公共政策问题的决策权应为各国的主权”,<sup>[31]</sup>首次确认各国对本国网络空间拥有排他性的主权。2005年11月,联合国信息社会世界峰会发布《突尼斯承诺》(The Tunis Commitment),提出“承认各国政府在峰会进程中发挥关键作用和责任”,<sup>[32]</sup>再次确认国家网络主权。2013年6月,联合国通过《关于从国际安全的角度来看信息和电信领域的发展政府专家组的报告》(Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,第A/68/98号决议),认为“国家主权和源自主权的国际规范和原则适用于国家进行的信通技术活动,以及国家在其领土内对信通技术基础设施的管辖权”,<sup>[33]</sup>确认以属地管辖为主的网络管辖权。同年,首尔会议形成的《旨在维护网络空间开放与安全的首尔框架及承诺》(Seoul Framework for and Commitment to an Open and Secure Cyberspace),提出“国家对其领域内的信息基础设施享有管辖权”,<sup>[34]</sup>明确在网络空间适用传统管辖权规则。2015年7月,联合国再次发布了《关于从国际安全的角度看信息和电信领域的发展政府专家组的报告》(Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,第A/70/174号决议),强调“国际法、《联合国宪章》和主权原则的重要性”,<sup>[35]</sup>再次明确对网络管辖权的立场。虽然,联合国在官方文件中没有直接使用“网络主权”“网络管辖权”等术语,但对国家在网络空间享有排他性的主权与管辖权持肯定立场。但由于各国在网络主权和管辖权问题上的争议较大,联合国主导下的国际网络治理规则制定工作

[28] 参见刘艳红:《论刑法的网络空间效力》,《中国法学》2018年第3期,第105页。

[29] 参见[日]松本博之著:《因特网、信息社会与法——日德研讨会论文集》,信山社2002年版,第410页。

[30] 参见郑泽善:《网络犯罪与刑法的空间效力原则》,《法学研究》2006年第5期,第74-75页。

[31] 参见《原则宣言》,联合国官方网站, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/576/95/PDF/N0457695.pdf?OpenElement>,最近访问时间[2022-03-18]。

[32] 参见《突尼斯承诺》,联合国官方网站, <https://www.un.org/chinese/events/wsis/promises.htm>,最近访问时间[2021-12-15]。

[33] 《从国际安全的角度来看信息和电信领域发展的政府专家组的报告》,联合国官方网站, <https://undocs.org/ch/A/68/98>,最近访问时间[2021-12-15]。

[34] See *Seoul Framework for and Commitment to Open and Secure Cyberspace*, United Nations (October, 2019), <https://www.un.org/disarmament/wp-content/uploads/2019/10/ENCLOSED-Seoul-Framework-for-and-Commitment-to-an-Open-and-Secure-Cyberspace.pdf>,最近访问时间[2022-03-18]。

[35] 《关于从国际安全的角度看信息和电信领域的发展政府专家组的报告》,联合国官方网站, <https://undocs.org/ch/A/70/174>,最近访问时间[2021-12-15]。

遇到重重困难,难以在短期内取得重大突破。

### (三)中美欧的立场、主张及立法实践

#### 1. 中国

我国一直倡导构建包括网络主权、网络管辖权在内的网络治理主张,积极探索“网络命运共同体”下的网络管辖权制度。2010年《中国互联网状况白皮书》首次提出网络主权和网络管辖权的主张,强调“中华人民共和国境内的互联网属于中国主权管辖范围,中国的互联网主权应受到尊重和维护”。<sup>[36]</sup> 2014年11月,习近平总书记在致首届世界互联网大会的贺词中强调,建立互联网治理体系要“尊重网络主权,维护网络安全”。<sup>[37]</sup> 2015年12月,习近平总书记在第二届世界互联网大会上重申,推进全球互联网治理体系变革,应该坚持尊重网络主权原则。<sup>[38]</sup>

在刑事立法方面,2009年《刑法修正案(七)》规定了有关计算机网络犯罪的内容,但未涉及网络刑事案件的管辖权问题。2015年《国家安全法》规定了属地管辖、属人管辖和保护管辖等网络刑事管辖原则。2016年《网络安全法》中明确了“维护网络空间主权”的立法目的。2021年6月《数据安全法》也规定了数据管辖权的内容,主要包括属地管辖和保护性管辖。在司法解释方面,2012年11月最高人民法院出台了《关于适用〈中华人民共和国民事诉讼法〉的解释新刑事诉讼法司法解释》,规定网络犯罪行为5类“犯罪地”认定的规则。2014年,最高人民法院、最高人民检察院和公安部联合发布了《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》,规定了7种认定“犯罪地”的情形。相比较2012年最高人民法院的司法解释,2014年的司法解释则进一步扩充了管辖权的内容,增加了“被侵害的计算机信息系统或其管理者所在地”“使用的计算机信息系统所在地”和“被侵害时所在地”等情形。2021年1月最高人民法院出台的《关于适用〈中华人民共和国民事诉讼法〉的解释》列举了五种情形的犯罪行为地和犯罪结果地。2022年8月,最高人民法院、最高人民检察院、公安部联合发布《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》,基本重申了前述犯罪地的规定,但增加了“其他涉案人员使用的信息网络系统所在地”的情形。我国司法解释总体上采取了属地管辖的立场和做法。

#### 2. 美国

美国在网络犯罪刑事管辖权的立场发展遵循了由传统保守到国内扩张,甚至试图实现“全球扩张”的发展历程。在“9·11”事件之前,美国立法和司法总体上承认国家网络主权和刑事管辖权,主要采取扩大属地管辖的立场,即将与终端设备、服务器等相关行为地、犯罪地或结果地作为启动网络刑事管辖的条件,通过对传统属地管辖规则的解释,将刑事管辖延伸到网络空间来解决网络犯罪管辖问题。如1986年《计算机欺诈和滥用法》

[36] 参见国务院新闻办公室:《〈中国互联网状况〉白皮书(全文)》,国务院新闻办公室网站,[http://www.scio.gov.cn/ztk/dtzt/28/3/Document/661296/661296\\_5.htm](http://www.scio.gov.cn/ztk/dtzt/28/3/Document/661296/661296_5.htm),最近访问时间[2022-09-18]。

[37] 参见《习近平致首届世界互联网大会贺词(全文)》,共产党员网,<https://news.12371.cn/2014/11/19/ARTI1416366354829717.shtml?from=groupmessage&isappinstalled=0>,最近访问时间[2022-09-18]。

[38] 参见《习近平在第二届世界互联网大会开幕式上的讲话(全文)》,共产党员网,<https://news.12371.cn/2015/12/16/ARTI1450250340197792.shtml?from=groupmessage>,最近访问时间[2022-09-18]。

(*The Computer Fraud and Abuse Act*)规定,网络犯罪行为“犯罪地”包括行为实施地、受攻击计算机、软件及程序所在地、行为人所在地、涉案数据所在地和流经地等。<sup>[39]</sup> 1987年《计算机安全法》(*Computer Security Act*)提出,联邦机构对国内网络安全防护和敏感信息负有保护职责,继续延续了扩大属地管辖的立场。

从“9·11”事件开始,美国大幅提升了网络跨境管辖的立法和执法力度,转向采取侵害法益关联说的立场,即以网络行为对刑法所保护的法益造成的损害作为判断的标准。美国以反恐名义制定和修订《爱国者法案》(*USA PATRIOT Act*)和《外国情报监视法案》(*Foreign Intelligence Surveillance Act*)等国内立法,对网络空间进行严密监控,像维护现实空间的领土主权一样在网络空间内实施事实上的国家管辖权。从司法判例的角度来看,美国法院持有类似的属人管辖关联说主张,即主张以属人管辖为基础,从犯罪行为对本国国家或者公民的侵害或者影响关联性为标准来判断是否具有刑事管辖权。原先的有限管辖原则在法院判决被取而代之,长臂管辖规则被大量适用于网络案件中。

2010年至今,美国逐步转向新主权理论的立场,即站在网络资源和网络技术优势地位,排斥其他国家在网络空间主权和管辖权的主张,将全球都视为其网络主权和网络管辖权的适用范围。如在2011年的美国执法机关要求美国公司交出欧洲地区用户数据的案例。<sup>[40]</sup> 2016年美国设计了更便捷的直接跨境电子证据调取方式,包括向在国外运营的本国互联网企业直接调取数据以及允许执法机关直接跨境远程取证。2022年4月,美国联合60个国家及地区推出《互联网未来宣言》(*Declaration for the Future of the Internet*),提出“推动符合美西方价值观的信息自由流动”的主张,<sup>[41]</sup> 试图进一步强化其对全球网络空间和数据的管辖权。

### 3. 欧洲

早在2001年11月,欧洲国家与美国等国家签署了全球首个打击网络犯罪的国际公约《网络犯罪公约》(*Convention on Cybercrime*),规定了“属地优越权”和“属人优越权”原则,同时规定“属地优越权”包含“拟制领土”,如第22条规定缔约国对本国领土内的犯罪具有管辖权。<sup>[42]</sup> 虽然《网络犯罪公约》规定了网络刑事管辖权,但仍然基于传统刑事管辖权,并未考虑网络犯罪的新特征,因此对确定网络犯罪刑事管辖权制度意义不大。2018年4月,欧盟提出《欧洲议会和理事会关于在刑事案件中欧洲电子证据提取令和留存令的条例(草案)》(*Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*),要求建立欧盟数据调取令和欧盟数据存留令,并规定了网络信息提供者的取证

[39] 参见吴海文、张鹏:《打击网络犯罪国际规则的现状、争议和未来》,《中国应用法学》2020年第2期,第199页。

[40] See Zack Whittaker, *Google Admits Patriot Act Requests; Handed over European Data to U. S. Authorities*. ZDNet (August 11, 2011), <https://www.zdnet.com/article/google-admits-patriot-act-requests-handed-over-european-data-to-us-authorities/>, 最近访问时间[2022-03-18]。

[41] See *Declaration for the Future of the Internet*, US Department of State (Apr. 28, 2022), <https://www.state.gov/declaration-for-the-future-of-the-internet>, 最近访问时间[2022-03-18]。

[42] See *Convention on Cybercrime*, European Parliament (Nov. 23, 2001), [https://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest/7\\_conv\\_budapest\\_en.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest/7_conv_budapest_en.pdf), 最近访问时间[2022-03-18]。



协助义务,<sup>[43]</sup>立场与美国新主权理论的立场趋近。总体而言,欧洲各国在网络主权和管辖权的立场相对矛盾并不断摇摆。一方面总体上认可网络主权,如 2003 年曾尝试推动由各国政府主导的合作模式来管理全球互联网,但另一方面往往受制于美国,在独立自主上显得力不从心。<sup>[44]</sup>

## 四 网络犯罪刑事管辖权冲突的焦点

网络刑事管辖扩张化的趋势存在于网络治理的几个重要方面,既存在管辖扩张性与刑法谦抑性的关系摇摆、“硬法不硬”与“软法不软”相向而行等内源性冲突,也存在霸权主义与主权主义的体系性博弈等外源性冲突。

### (一) 价值冲突:管辖扩张性与刑法谦抑性的原则性摇摆

刑法的谦抑性是刑事立法和司法等活动的重要原则,也是解决网络犯罪刑事管辖权冲突、维护网络空间法治秩序的一个重要原则。在对网络犯罪进行刑事管辖时,刑法谦抑性要求各国一方面应充分认识到刑法并不是万能的,不可能预防和惩治所有网络犯罪行为,更不可能消灭网络犯罪的社会根源,刑法管辖权应当在“必需”“必要”的情形下才可以发动。另一方面,刑法属于国内法,不能突破他国法和国际法。国内立法机关不能恣意地无限扩大本国刑法的适用范围,也不能忽视他国在国际法上的权利而任意地主张界定刑罚权限的权力,以彰显本国绝对主权,刑法适用必须受到国际法的限制。<sup>[45]</sup>也就是说,国内法中的刑事管辖权行使必须以他国法和国际法相关规定为界,不能突破这些限制。

现实空间与网络空间的相互交融为国家管辖的扩张带来了可能。如果网络犯罪被视作全球犯罪,普遍管辖就有可能代替属地管辖而升为原则。<sup>[46]</sup>各国网络犯罪刑事管辖权之间的界限很模糊,对同一类型犯罪行为的管辖很容易出现交叉和竞合的情形,从而导致包括主观属地管辖权和客观属地管辖权、效果原则主张的管辖权和依据保护原则主张的管辖权等之间的管辖权冲突。<sup>[47]</sup>同时,作为一个全新维度的域,网络空间衍生出的网络刑事管辖权成为各国试图扩大本国网络主权的抓手,甚至有些国家在与本国“属地”“属人”等要素均没有联系或联系很小的情形下,试图运用刑事管辖权来强行对其他国家的设施、人员和行为进行管辖。在网络犯罪与本国领土没有或只有很微弱联系的情况下主张属地管辖,实际是以属地管辖之名行过域外管辖之实。<sup>[48]</sup>在网络全球化导致国家间司法管辖权冲突频发的当下,法院对此越来越少地进行礼让分析。即使涉及别国主权利

[43] See *Proposal for a Regulation of The European Parliament and of The Council on European Production and Preservation Orders for Electronic evidence in Criminal Matters*, European Union (Jan. 1, 2018), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN>, 最近访问时间[2022-03-18]。

[44] 参见朱诗兵、张学波、王宇、刘韵洁:《世界范围内网络主权的主要观点综述》,《中国工程科学》2016年第6期,第91页。

[45] 参见刘艳红:《论刑法的网络空间效力》,《中国法学》2018年第3期,第90页。

[46] 参见刘艳红:《论刑法的网络空间效力》,《中国法学》2018年第3期,第92页。

[47] 参见甘勇:《〈塔林手册2.0版〉网络活动国际管辖权规则评析》,《武大国际法评论》2019年第4期,第119页。

[48] 参见吴海文、张鹏:《打击网络犯罪国际规则的现状、争议和未来》,《中国应用法学》2020年第2期,第200页。

益,法院更多地被要求将其视为“国内事务”并依照本国法律作出裁判,国际法“礼让原则”的适用充满挑战。<sup>[49]</sup>这不仅严重违背了刑法的谦抑主义,也会危及国与国之间的司法信任与合作,对加强全球合作、打击网络犯罪而言是灾难之举,更有可能引发网络冲突、甚至是网络战争。

## (二)立场冲突:霸权主义与主权主义之间的博弈

当前国际网络格局的最基本现实是“五个没有变”,即不同区域之间广泛存在的信息鸿沟没有变,不同国家在国际互联网关键信息资源分配上的失衡没有变,国际互联网治理“去中心化”表象掩盖下的权力集中与垄断没有变,网络霸权国家对他国的监听监控与资源掠夺没有变,各国共同面临的网络安全挑战也没有变。<sup>[50]</sup>围绕是否制定全球性公约的争议,实质上是各方围绕国际规则的主导权之争。<sup>[51]</sup>出于地缘政治和国家利益等方面的考虑,各国在全球性网络犯罪公约的内容和形式上迟迟难以形成共识,特别是在网络主权和网络管辖权问题上的对立与博弈日渐胶着,形成了“网络霸权主义”与“网络主权主义”的根本性对立。当前在联合国平台形成了相互对立的双轨立法机制,即由美国主导的联合国信息安全政府专家组(UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNGGE)和由俄罗斯主导的开放工作组(Open-Ended Working Group, OEWG),都难以在短期内产生实质性结果。<sup>[52]</sup>其中,发展中国家往往对网络主权和管辖权作宽泛解释,坚持“网络主权主义”的立场,强调各国公平、公正地享有网络发展权、网络自主权、网络合作权等内容。<sup>[53]</sup>部分西方国家在网络话语权、网络技术和网络能力等方面占有绝对的主导权,则主张对网络主权和管辖权做限制解释,试图利用国际刑法规则固定和维护自身在网络体系中的压倒性优势,特别是在国际议程设置、治理规则制定和网络资源分配等方面进一步拉开与其他国家的差距,将现实空间的主导权投射在网络空间,复制和延续现实空间的霸权主义。

## (三)模式冲突:“硬法不硬”与“软法不软”的相向而行

当前主要存在三类网络空间立法模式,即“软硬法模式”“软法模式”和“硬法模式”。其中,“软硬法模式”是指推动既有立法在网络空间的适用。在理论上,“软硬法模式”具有良好的法律适用成本和效益,可以使用最小的法律成本、最短的时间推动既有网络犯罪立法与网络空间治理的对接,如可以将现有国际战争法和使用武力的国际法、国家责任法等国际法直接运用于网络空间,构建网络主权、网络不干涉主义、网络空间禁止适用武力等规则。这种模式具有良好的经济性,并可在短期内就发挥重要作用。但由于既有国际法在网络空间适用上存在诸多不适应性,如在规则类推、解释和适用等方面的存在较大困

[49] 参见吴琦:《网络空间中的司法管辖权冲突与解决方案》,《西南政法大学学报》2021年第1期,第59页。

[50] 参见支振锋:《将网络主权切实融入网络强国战略》,《中国信息安全》2017年第5期,第34页。

[51] 参见吴海文、张鹏:《打击网络犯罪国际规则的现状、争议和未来》,《中国应用法学》2020年第2期,第190页。

[52] See See Elaine Korzak, *What's Ahead in the Cyber Norms Debate?*, LAWFARE (Dec. 15, 2021), <https://www.lawfareblog.com/whats-ahead-cyber-norms-debate>, 最近访问时间[2022-03-18]。

[53] 参见《信息安全国际行为准则》,联合国官方网站, <https://undocs.org/zh/A/69/723>, 最近访问时间[2021-12-15]。

难,这种模式具有天然的缺陷。“软法模式”是指推动负责任国家行为规范的发展,当前受到各国的热捧。虽然软法不具有硬法的法律效力,但对网络空间国际立法“软硬法”适应性较差、“硬法”缺失的情况下,“软法模式”下的规则并不软。软法虽然不具有硬法的性质,但对各国的立法和司法起着重要的指导和示范作用。这种模式将在当前乃至未来相当长一段时间内发挥主导性作用,并对未来“硬法模式”的立法发展提供指引。“硬法模式”是指推动网络空间的新国际公约的制定。这种模式是未来全球网络空间立法的趋势,是协调与解决网络刑事管辖冲突与扩张的最有效途径。但由于各国在主导权和关键问题上的对立与分歧,在可预见的情况下难以在短期内取得重大突破。

## 五 网络犯罪刑事管辖权冲突的全球规制

随着网络空间逐步演变成国家间角力的新主战场,网络地缘政治将成为影响网络空间治理越来越重要的因素。对此,我国在探讨是否需要建立网络主权和网络管辖权制度,以及需要什么样的网络主权和管辖权制度时,不仅需要从法律内部来考虑推动理论研究、建章立制和规则实施等内容,还需要从全球网络刑事管辖冲突规制的中立立场出发,讨论国际社会的接受度或可行性。

### (一) 法律价值:平衡好网络犯罪刑事管辖权扩张性与谦抑性关系

在构建网络犯罪刑事管辖权的过程中,各国要在管辖扩张性和刑法谦抑性、应然和实然、政治与法律等相对对立的关系中,通过建立具有国际公认性的“合理原则”“礼让原则”等标准,形成一种动态的相对平衡机制,既推动发展公平合理的网络主权和刑事管辖权制度,也能压制部分国家试图扩张本国刑事管辖权的冲动。对此,应当从维护大多数国家利益的角度,在全球范围内推进能够平衡管辖扩张性和刑法谦抑性的网络刑事法律制定。一方面在国内立法中,各国要在治理理论、模式选择和管辖规则等方面坚持“合理原则”和“礼让原则”,在不违反本国主权的基础上充分尊重其他国家的刑事管辖权,克制国内立法出现网络犯罪刑事管辖权问题“三化现象”,不能为了达到特定的政治目的而滥用刑事管辖权并实施不合理的域外管辖、甚至是全球管辖。另一方面,各国在参与国际立法中,要从不同层面、不同形式系统地阐述对网络主权和刑事管辖权的主张,推动网络空间犯罪治理的“正和博弈、共赢发展、增量发展”<sup>[54]</sup>的新型国际治理范式,摒弃“此消彼长、非此即彼的传统零和博弈”<sup>[55]</sup>的冷战思维。因此,在全球网络治理的价值选择上,绝不能放弃刑法谦抑性和国际法“合理原则”和“礼让原则”等要求,应根据犯罪行为来主张管辖,避免因过分宽泛地界定“犯罪地”扩张管辖并引发管辖冲突。

### (二) 在国际立法上寻找网络空间法治化的最大公约数

全球当前无法在短期内就网络主权、刑事管辖权等问题形成统一的认识,但这并不意

[54] 参见吴雨欣:《阿里 CEO 张勇:数字化时代的大趋势是正和博弈、增量发展》,澎湃新闻, [https://www.thepaper.cn/newsDetail\\_forward\\_4727400](https://www.thepaper.cn/newsDetail_forward_4727400),最近访问时间[2022-09-18]。

[55] 参见潘旭涛:《携手共建网络空间命运共同体》,人民网, <http://ydl.people.com.cn/n1/2019/1021/c411837-31411041.html>,最近访问时间[2022-09-18]。

味着网络主权和刑事管辖权问题的发展前景一片黯淡。刚好相反,各国围绕网络刑事管辖权开展的激烈博弈会助推其发展。

首先,坚持在联合国主导下推动建立全球统一的网络犯罪公约。各国强烈需要一个多国法律的世界,同时也需要压低规制成本。<sup>[56]</sup> 各国在积极修改或制定网络犯罪的管辖权规则的同时,也考虑到网络犯罪跨国性追诉的困难和效能,并认识到只有国际合作方能对网络犯罪行为有实质性的规制。同时,也只有全球一致的立法,才能为网络使用者提供明确具体的规范,认识到网络犯罪的构成和基本内涵,从而不致因跨越国界而受到两种内容迥异的法律系统的规制。<sup>[57]</sup> 作为全球最具有代表性和权威性的国际性组织,联合国是未来全球制定网络空间规则并推进网络犯罪治理的最佳平台。任何将网络空间视为国家博弈的新战场,并把网络犯罪治理政治化、阵营化和扩张化的行为都无益于国际网络犯罪的治理,也不利于破除“网络霸权主义”“网络干涉主义”等危害。对此,各国可以网络主权、网络管辖权、网络犯罪的跨境取证、数据跨境流通、双边或多边引渡等重大争议问题不断寻找公约数,不断凝聚国际共识推动联合国启动相关国际公约的起草和后续议程。

其次,全球在网络空间治理上存在加强合作的必然性与可能性。其一,各国对网络犯罪治理都存在巨大的客观需求。预防和惩治全球性网络犯罪已经超出了任何单个国家司法体系的能力范围,大国、强国对互联网的依赖程度可能更大,脆弱性也更大,对国际合作的需求也就更大。<sup>[58]</sup> 在这种背景下,网络犯罪的全球性给传统网络犯罪管辖制度造成了巨大的冲击,任何国家都难以独善其身或凭借本国的司法和执法体系实现对全球性网络犯罪的预防与惩治。其二,前期探索为全球犯罪公约发展打下了较好的基础。很多国家都积极推动网络空间的国际立法,说明各国已经认识到只有推动建立全球性统一的规则体系,才能真正有效遏制网络犯罪并提供国际协调行动规范,不至于因为国家法律体系的差异而束手无策。当前已经出现的一些国内立法和国际性软法,可以为未来出台国际网络硬法规则奠定良好的基础。其三,全球治理的力量对比正在悄然发生变化。当前正值塑造网络犯罪刑事管辖权的“窗口期”,以联合国为首的国际组织在网络空间规则制定中的主导性越来越强,发展中国家参与国际网络规则的意识 and 能力不断提升,包括欧洲国家在内的部分西方国家的自主性和独立性也在不断上升,这些都为未来制定具有全球代表性的公约提供了客观可能。对此,各国可以在网络恐怖主义、网络诈骗、知识产权保护、网络儿童色情以及利用暗网等途径从事国际贩毒、贩卖人口、大规模杀伤性武器流通等领域开展跨国合作,共同打击网络刑事犯罪。

最后,推动硬法和软法并行双轨制立法模式,并重视司法判例对国际刑事司法规则的塑造。在全球公认的国际网络公约缺位的情况下,网络犯罪刑事管辖权处于一个快速裂变的状态。国际会议、国际组织所通过的宣言、行动计划等文件都具有发展为特定软法规则的潜力,并产生较大的影响。<sup>[59]</sup> “软法模式”显现出“专家造法”的作用,成为欧美国家

[56] 参见[美]劳伦斯·莱斯格著:《代码2.0:网络空间中的法律(修订版)》,李旭、沈伟伟译,清华大学出版社2018年版,第331-333页。

[57] 参见田胜斌:《互联网刑事案件管辖制度研究》,《政法论坛》2021年第3期,第45页。

[58] 参见徐龙第、郎平:《论网络空间国际治理的基本原则》,《国际观察》2018年第3期,第42页。

[59] 参见王孔祥:《网络安全的国际合作机制探析》,《国际论坛》2013年第5期,第4页。

处理网络问题的参考指南,<sup>[60]</sup>软法虽然不像国际公约那样正式,但非常灵活并更容易为多边利益攸关方所接纳,在一定程度上发挥着硬法所应发挥的作用,并可能在未来实现“软法硬化”式的“华丽转身”,成为全球性网络犯罪公约等硬法的模版。我国要推动硬法和软法并行双轨制立法,尤其重视“软法硬化”的趋势与潜力,注重发挥软法“影子立法”的价值。《塔林手册 2.0》(The Tallinn Manual 2.0)作为迄今为止这一领域最为详尽的大型集体研究成果,它所涵盖的网络空间国际规则有可能成为未来相关实践中不可回避的“标杆”,甚至作为“影子立法”来填补现有规则空白并发挥事实上的规则指引作用。<sup>[61]</sup>在当前一些跨国网络刑事案件中,“软法硬化”的效果已通过一些司法判例予以实现。例如,在 2014 年“索尼影业案”和 2016 年美国“邮件门案”中,美国参考《塔林手册 2.0》的有关内容,对其声称的攻击来源国朝鲜和俄罗斯采取反制措施。<sup>[62]</sup>美国推广其主导制定的软法塔林系列,不在于运用软法行为本身,而在于其客观上形成一种判例和习惯,并可能对本国、国际乃至全球其他国家后续的司法都有一定的示范和引导作用。

### (三) 网络犯罪刑事管辖权冲突规制的中国方案

制定和运用网络国际法准则要考虑到政治、技术和法律等不同方面的问题。<sup>[63]</sup>我国应当充分认识当前阶段立法现状与需求,做好近期、中期和长期推进网络空间规则制定的规划,整合各种资源优势打造网络空间的规则优势,为推动建立公正、合理和有序的网络国际治理秩序贡献中国方案。

首先,提升我国刑法对国际网络空间治理的制度供给能力。我国当前相关的规定主要散见于刑法、附属刑法、刑事诉讼法、相关司法解释和国际公约中,对真正建立起与数字化时代相匹配的网络犯罪刑事管辖权制度的支撑严重不足。其中一个原因在于,我国当前刑事立法的重心立足于国内预防和打击犯罪的立场。一方面,在观念上忽视了我国刑事立法在国际治理中的价值与功能,缺乏在国际视野下如何推动中国刑法域外适用的意识;另一方面,在实践中能与国际刑法相衔接的制度供给能力不足,对全球网络空间治理缺乏总体性、系统性和完整性的刑事立法规则作为支撑。例如,我国《刑事诉讼法》第 18 条就跨境网络犯罪的立案管辖仅以“法律另有规定除外”一言蔽之,但至今未见相关规定出台。导致我国刑事管辖缺乏上位法依据,无法落实侦查取证的主体,还致使我国在实施《国际刑事司法协助法》和推进跨国网络犯罪治理中的能量无法充分释放,<sup>[64]</sup>从而造成国内法难以与国际法、他国法有效衔接。

其次,在相互尊重网络主权的基础上不断明确和实践我国的网络犯罪刑事管辖权制度。在宏观方面,应当讲求对等主义,充分相互尊重各国法律法规、司法制度和公共政策,坚决反对以维护本国网络利益为名,从事侵犯他国网络主权、干涉他国内政、大搞网络欺

[60] 参见黄志雄:《网络空间国际规则制定的新趋向——基于〈塔林手册 2.0 版〉的考察》,《厦门大学学报(哲学社会科学版)》2018 年第 1 期,第 7 页。

[61] 参见黄志雄:《〈塔林手册 2.0 版〉:影响与启示》,《中国信息安全》2018 年第 3 期,第 85 页。

[62] 参见黄志雄:《〈塔林手册 2.0 版〉:影响与启示》,《中国信息安全》2018 年第 3 期,第 85 页。

[63] See K. Pipyros, L. Mitrou, D. Gritzalis & T. Apostolopoulos Cyberoperations and International Humanitarian Law: A review of Obstacles in Applying International Law Rules in Cyber Warfare, 1 *Information & Computer Security* 24, 38-52 (2016).

[64] 参见安柯颖:《跨国网络犯罪国际治理的中国参与》,《云南民族大学学报(哲学社会科学版)》2019 年第 3 期,第 158 页。

凌主义和网络霸权主义等行为。在具体执行层面,考虑建立属地关联管辖原则、属人关联管辖、侵害法益关联说相结合为主,辅之以普遍关联管辖、保护关联管辖与实害管辖原则相结合的网络刑事管辖制度。一方面,在我国境内针对相关设施、人员、数据等造成或可能造成实质损害的实害犯与危险犯,我国可以依据以属地关联为基础的有限管辖原则进行管辖。其中,实质损害要达到造成严重危害计算机系统和计算机数据的机密性、完整性和可用性以及滥用计算机系统、网络和数据的一种客观存在的损害状态。<sup>[65]</sup> 另一方面,针对其他国家、组织和个人或我国组织与个人在境外针对我国境内网络法益的损害行为,我国应依据侵害法益关联和属人关联的有限管辖原则进行管辖。同时,我国还应当考虑建立普遍关联管辖、保护关联管辖与实害管辖原则相结合的辅助性管辖制度,对特定重大危害国际安全和人类发展的网络犯罪行为行使普遍管辖权,如针对他国民用航空器、空间站、核电站等设施进行攻击足以引发设施和人员等发生重大损失的行为实施管辖。

最后,强化可执行和可操作的国际刑事立法。法律话语权和主导权以国家实力和政治影响力为后盾,但在国家利益的实现必须借助于细化并可落地执行的法律规则运行。例如,《塔林手册 2.0》全文涉及 14 个领域的 154 条规则,基本覆盖了网络行为各个方面的规制内容。但《信息安全国际行为准则》(*International Code of Conduct for Information Security*) 仅有 13 条局限于政策性、原则性和框架性的行为准则,其国际影响力难以与《塔林手册 2.0》相比,对国际刑事立法、司法等活动缺乏有益指导。这充分说明了我国在网络犯罪国际规则制定上仍缺乏必要的张力,立法技术和水平仍有待于进一步提升,特别是细化对网络犯罪刑事管辖权基本概念、网络攻击和网络战争边界等法律问题研究,提升我国立法技术。因此,我国未来在主导国际规则制定时,要更多地打破法律问题政治化的习惯,更多地采取政治问题法律化的积极立场,通过构建中国刑法话语和中国刑法叙事体系,打造融通中外网络犯罪领域的新概念、新范畴、新表述,善于将政治诉求和主张通过涉外刑事立法、司法和执法等活动来展示。同时,我国未来要更加重视国家层面的“软法模式”,可以考虑参照各国专家参与《塔林手册 2.0 版》编写的方式,积极地依托网络空间领域的专家群体参与和主导国际网络规则的制定,为未来国际规则提供引导和示范,并在国际和国内司法平台上探索有重大国际影响力的司法运用场景。具体而言,可以分三步走:一是在国内汇聚不同部门、不同机构和组织的相关专家,围绕包括网络管辖权在内的网络空间治理的重大问题形成相应的全国性学术性法律文件(有专家建议称为《珞珈手册》<sup>[66]</sup>)。二是依托世界互联网大会等以国内为基础的国际性平台,汇聚相应的专家学者群体对前述产生的法律文件进行修订、审核与推广,逐步形成具有区域性的软法文件。三是在联合国、二十国集团、亚太经合组织、上合组织等国际平台推出能代表相应发展中国家群体的软法文件,吸收更多的国家和地区专家学者群体的认同并参与其中。

[本文为作者参与的 2021 年度国家社会科学基金重大课题“网络信息安全监管法治体系构建研究”(21&ZD193)的研究成果。]

[65] 参见陈结森:《关于我国网络犯罪刑事管辖权立法的思考》,《现代法学》2008 年第 3 期,第 98 页。

[66] 参见龙坤、朱启超:《网络空间国际规则制定:共识与分歧》,《国际展望》2019 年第 3 期,第 51 页。

[ **Abstract** ] Positive conflict of current cybercriminal jurisdiction has become an important bottleneck in the international governance of cybercrimes. The traditional criminal jurisdiction has not acclimatized itself to cyberspace, resulting in the negative realization of criminal jurisdiction over cybercrime. The politicization, expansion, and alignment of cyberspace have further aggravated the conflict of jurisdiction over cybercrimes. With respect to the conflict attribution of criminal jurisdiction over cybercrime, the space and time elements of cybercrimes all “exist in the digital form” and the complex space-time and borderless nature has brought great uncertainty to the global criminal jurisdiction over cybercrime. The sharp contrast between the integrity requirements of the cyberspace evidence chain and the vulnerability status quo makes it extremely difficult to trace sources, collect evidence and carry out international cooperation in the fight against cybercrimes. The absence of international legislation on cybercrime jurisdiction leads to the lack of legal and practical bases for the application of universal jurisdiction to cybercrimes. The “Balkanization” of international cyberspace governance has further increased the difficulty and complexity of global governance and played a negative role in global cyberspace governance. China is actively exploring the criminal jurisdiction over cybercrime system that matches the vision of “building a community with a shared future in cyberspace”, whereas the United States, European countries and some other western countries are constantly expanding the criminal jurisdiction over cybercrime, and regard the whole world as the scope of application of the cyberspace jurisdiction. There are many endogenous and exogenous conflicts of criminal jurisdiction, showing an oscillation between the principle of expansion and the principle of modesty. The conflict of positions is reflected in the systematic game between hegemonism and sovereignty, with “hard law being not hard” and “soft law being not soft” going in the opposite direction. While the “soft-hard law mode” and the “hard law mode” are faced with many problems of inadaptability, the “soft law mode” is rising rapidly. In the global regulation of criminal jurisdiction over cybercrime, China should balance the relationship between the expansion and modesty of criminal jurisdiction over cybercrime, adhere to the principle of modesty of criminal law, and the principles of reasonableness and comity in international law, and promote the new international governance paradigm of cybercriminal governance. It should work together with countries all over the world to find a common divisor in promoting the development of rule of law in cyberspace, and “seek common ground while reserving differences” in the stance and response to major issues, so as to provide support for the formation of global common cognition and practice, constantly improve its capacity for institutional supply to the creation of cyberspace rules, and contribute its own solutions for the problems in establishing a fair, reasonable and orderly international cyberspace governance order.

---

---

(责任编辑:贾元)