《联合国打击网络犯罪公约》的制定问题研究

赵永琛*

内容摘要:联合国正在研究制定打击网络犯罪公约,这是联合国发展和编纂国际刑法的最新实践,具有重要意义。为更好开展全球网络治理,维护国际网络安全秩序,有必要在制定该公约过程中广泛吸收各国预防和打击网络犯罪的成功经验,将网络治理的实体法、程序法和特殊执法规则法定化、规范化,明确基本原则,调整核心要素设计;因应网络犯罪新态势,增设网络犯罪类别;突出程序规则针对性,强化惩治网络犯罪制度建设;创新国际司法与警务合作模式,提升打击网络犯罪效能;推进网络监管制度趋同化,夯实法治基础;统筹打防一体化关系,健全国际网络刑事法治。

关键词:打击网络犯罪　网络安全　网络治理

一、《联合国打击网络犯罪公约》的制定背景与意义

(一)制定背景

2022年2月28日至3月11日,《联合国打击网络犯罪公约》特设政府间委员会(以下称"特委会")第一次谈判会议在纽约举行,约140个国家、世界银行等14个国际组织和140个非政府组织代表与会。各方普遍认同应尽快制定《联合国打击网络犯罪公约》(以下称《公约》),并以协商一致方式通过《公约》框架和谈判安排。会议还围绕《公约》的目标、适用范围和核心要素等关键问题初步交换了意见,特委会主席将在综合各方意见基础上完善有关建议方案,并在第二次谈判会议前散发。

由于网络技术飞速发展,云计算、物联网、加密技术、人工智能等新技术突飞猛进,利用网络技术从事犯罪活动和针对网络系统的犯罪现象在世界各国越来越普遍,网络犯罪手段迭代更新越来越快,网络犯罪跨国化日趋突出,国际社会深感有必要运用国际立法对网络犯罪进行防范和惩治。2001年11月23日,欧洲委员会在匈牙利首都布达佩斯通过《网络犯罪公约》(又称《布达佩斯公约》),并向各成员国开放签字。由于该公约属于地区性条约,缺乏广泛代表性且准入条件不一,因而难以为

*　法学博士,海南大学法学院兼职教授,前中国驻格林纳达大使。

本文仅代表个人观点,不代表任何官方立场。

国际社会所普遍接受。[①]

有鉴于此，中国、俄罗斯以及其他新兴国家主张尽快在联合国框架下制定一部打击网络犯罪的国际公约，解决区域组织打击网络犯罪公约的碎片化和区域局限性问题，构建新的防范和惩治网络犯罪机制，满足国际社会打击网络犯罪的需要。美西方和中俄等国围绕制定联合国打击网络犯罪国际公约的主导权展开了多轮博弈。

2011年9月12日，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦驻联合国代表联名致函联合国秘书长潘基文，请他将上述国家共同起草的《信息安全国际行为准则》作为第66届联合国大会正式文件，散发给各会员国。这份文件就维护信息和网络安全提出一系列动议，包括各国不应利用包括网络在内的信息通信技术实施敌对行为、侵略行径和制造对国际和平与安全的威胁；各国有责任和权力保护本国信息安全和网络空间及关键基础设施免受威胁、干扰和攻击破坏；帮助发展中国家发展信息和网络技术，合作打击网络犯罪等。[②]

2013年，联合国毒品和犯罪问题办公室经过各国专家组的共同努力，发布长达300多页的《网络犯罪综合研究报告（草案）》。该报告综合分析全球范围内网络犯罪状况、趋势和防范对策，深入探讨各国开展网络犯罪立法的重要性，呼吁世界共同关注网络犯罪问题。

2015年1月9日，中俄和其他上海合作组织成员国向联合国提交《信息安全国际行为准则（更新草案）》。此更新草案吸纳了国际社会的合理意见，内容更趋全面平衡。此后，俄罗斯独立起草《联合国合作打击网络犯罪公约（草案）》，并提交给第72届联合国大会。

美西方在联合国讨论打击网络犯罪议题时，并不赞成中俄等国提案，鼓吹国际社会应以《布达佩斯公约》为蓝本，要求其他国家采取申请加入《布达佩斯公约》的方式来解决打击网络犯罪的国际法依据问题。[③]中俄和其他未参加该公约缔约谈判的国家不赞同美西方的意见。这些意见分歧直接影响到制定全球性打击网络犯罪公约的进程。我国于2017年发布《网络空间国际合作战略》，强调支持联合国开展打击网络犯罪工作，主张在联合国框架下制定打击网络犯罪全球性法律文书。

2019年12月27日，第14届联合国大会召开前，中国、俄罗斯等47国共同提出《打击为犯罪目的使用通信技术的决议草案》，提交联大投票表决，联大最终予以通

① 2011年联合国政府间网络犯罪专家组建立以后，在2017、2018、2019年的几次会议上，各国专家就此问题进行过充分讨论，并形成了相同或相似的看法。

② 2011年，在中国、俄罗斯和巴西等国倡议下，联合国经济和社会理事会（Economic and Social Council，ECOSOC）下的预防犯罪和刑事司法委员会（UN Commission on Crime Prevention and Criminal Justice，CCPCJ）根据联合国大会决议设立联合国网络犯罪政府专家组。

③ 参见胡健生、黄志雄：《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》，《国际法研究》2016年第6期，第27页。

过。该决议草案决定成立一个代表所有区域的特设政府间专家委员会,正式开启谈判制定《联合国打击网络犯罪公约》的进程。令人遗憾的是,美西方并不完全认同这份联合国决议草案,依然在多种场合质疑联合国制定打击网络犯罪公约的必要性和可行性。

(二)制定意义

笔者认为,联合国在制定打击贩毒、恐怖主义以及跨国有组织犯罪等领域的全球性法律文书方面拥有丰富的成功经验,这些经验可以适用于打击网络犯罪的国际条约的编纂工作,因此制定《联合国打击网络犯罪公约》不仅可行,而且具有重要的意义,具体而言:

1.有助于满足国际社会应对网络犯罪的迫切需要。网络犯罪严重威胁各国网络信息安全,对各国政治安全、经济安全、社会安全、金融交易安全、个人隐私安全都构成严重威胁,但是,单靠任何一个国家或区域组织都无法完成防范和惩治全球网络犯罪的任务,因此,需要国际社会共同努力,采取政治、经济、社会和法律措施加以治理。制定《公约》,有助于国际社会统一认识,共同采取法律手段惩治网络犯罪。

2.有助于弥补打击网络犯罪国内立法之不足。为了惩治网络犯罪,各国纷纷出台预防和打击网络犯罪的国内法,但是,这些国内法的适用范围只及于本国管辖范围内,无法作为国际法依据来调整国家间惩治国际网络犯罪的权利义务关系,因此,国际社会唯有统一立场,采取国际法编纂的方式,加强预防和打击网络犯罪的国际法治力度,方为上策。

3.有助于满足维护网络空间秩序的现实需要。网络社会是虚拟社会,海量网络数据编织起全球网络空间。在这个空间里,人类社会命运与共。由于网络空间固有的脆弱性,网络犯罪对网络空间秩序的破坏往往非常致命。依法维护网络空间秩序,是关乎人类经济社会发展的重大问题。国际社会唯有加强网络刑事法治建设,加强网络治理,从源头上堵截、清除网络各种有害信息,净化网络空间环境,才能让网络社会健康发展。联合国若能如期制定《公约》,必定能够促进以国际法为基础的网络空间秩序的良好运行,从而保障网络社会的有序健康发展。

4.有助于推进全球网络治理。预防和控制网络犯罪是全球治理的重要一环。联合国回应国际社会呼声,制定《公约》,调整国家间网络治理权利义务关系,解决网络治理过程中的矛盾和纷争,完善网络治理领域国际规则,是全球网络治理现代化、法治化的必由之路,必定有利于促进全球互联网治理实现共商共建共享。

5.有助于促进数字经济发展和繁荣。随着网络技术的飞速发展,大数据、数字货币、区块链、网上交易、网络金融支付结算发展迅猛,维护网络大数据、数字货币、区块链、网上交易、网络金融支付结算的运行秩序和安全,能有力地保障全球信息化健康发展,从而促进数字经济迈上更快更好的发展轨道。这是国际社会利用刑法手

段保护和促进数字经济发展的必由之路。

考虑到联合国特委会正在研究制定《公约》，本文围绕《公约》框架设计和核心要素以及相关的重大理论和实践问题，提出一些不成熟的个人意见和建议，以期能为我国参与《公约》谈判和相关研究提供一些参考。

二、《公约》指导原则和核心要素的确定

按照特委会初步协商的意见，《公约》草案分为八章，包括一般规定、刑事定罪、程序规定和执法、国际合作、技术援助、预防措施、实施机制、最后条款。这个设计框定了《公约》的大致结构。特委会下一步将按照这个框架起草《公约》文本。

作者认为，从《公约》的适用范围和核心要素的角度看，似应对《公约》框架及内容设计进行适当调整，并从刑事实体法和程序法以及网络执法规范等方面加以完善，以便更好地体现其全面性、针对性和实用性。

（一）明确指导原则

第一，应明确提出构建和平、安全、开放、合作、可持续的网络空间命运共同体的理念[①]，并落实到《公约》序言中。习近平主席指出："随着世界多极化、经济全球化、文化多样化、社会信息化深入发展，互联网对人类文明进步将发挥更大促进作用。同时，互联网领域发展不平衡、规则不健全、秩序不合理等问题日益凸显。不同国家和地区信息鸿沟不断拉大，现有网络空间治理规则难以反映大多数国家意愿和利益；世界范围内侵害个人隐私、侵犯知识产权、网络犯罪等时有发生，网络监听、网络攻击、网络恐怖主义活动等成为全球公害。面对这些问题和挑战，国际社会应该在相互尊重、相互信任的基础上，加强对话合作，推动互联网全球治理体系变革，共同构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的全球互联网治理体系。"[②]

第二，应申明《联合国宪章》确立的不使用武力、尊重国家主权和基本人权及自由、不干涉内政的国际法原则，同样适用于打击网络犯罪。《联合国宪章》确立的主权平等原则是当代国际关系的基本准则，覆盖国与国交往的各个领域，其精神实质也应成为打击网络犯罪的基本原则。"我们应该尊重各国自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利，不搞网络霸权，不

① 2020年9月8日，中国发起《全球数据安全倡议》，主张各国应在相互尊重基础上，加强沟通交流，深化对话与合作，共同构建和平、安全、开放、合作、有序的网络空间命运共同体。该倡议全文可参见www.gov.cn/xinwen/2020-09/08/content_5541579.htm。2020年10月11日，上海合作组织成员国元首在《上海合作组织成员国元首理事会关于保障国际信息安全领域合作的声明》中明确了共同构建和平、安全、开放、合作、有序的网络空间命运共同体的立场，http://www.rmzxb.com.cn/c/2020-11-112711457.shtml，2022年9月8日访问。

② 习近平：《在第二届世界互联网大会开幕式上的讲话》，《人民日报》2015年12月17日，第2版。

干涉他国内政,不从事、纵容或支持危害他国国家安全的网络活动。”[①]

第三,坚持以联合国为核心的国际网络安全秩序,注重发挥联合国在应对国际信息安全威胁领域的关键作用,支持联合国制定该领域新的负责任的国家行为准则。[②]

第四,坚持维护国家网络主权原则,使国家主权、安全和发展利益免受来自网络空间的侵害,维护网络社会秩序和法律秩序的正常运转。[③]明确打击网络犯罪必须在国际法框架内进行,而不能超出必要限度,从而避免网络空间活动损害国际法的基本原则,侵害和平、安全和国家主权,危害公共利益。

(二)统筹打击网络犯罪和保障网络安全的关系

建议《公约》增加统筹打击网络犯罪和保障网络安全关系的内容。[④]在这个问题上,无论是《布达佩斯公约》,还是阿盟公约和非盟公约都没有兼顾好打击网络犯罪和保障网络安全的关系,留下了较多的欠缺。中俄等国在其提交给联合国大会的相关文件中已提出一些原则性构想,希望国际社会通过《公约》的编纂,维持打击网络犯罪和保障网络安全关系的平衡性,促进网络社会的健康发展。

(三)兼顾网络安全和网络发展[⑤]

特委会应充分考虑发展中国家发展网络的需要,鼓励而不是限制发展中国家发展网络,尤其应鼓励发达国家对发展中国家给予网络硬件和软件技术开发支持,共同促进网络信息化技术的进一步发展。[⑥]要抵制和反对网络霸权主义和单边主义,防止某些国家利用网络技术优势,侵害发展中国家网络发展权。

(四)融合网络刑事法和网络安全管理法要素

作为一部全球性的打击网络犯罪条约,《公约》必须满足打击网络犯罪的实际需要。这就要求《公约》必须解决有关定罪量刑、网络安全监管等最核心的问题。这种核心要素设计思路和制定《联合国打击跨国有组织犯罪公约》和《联合国反腐败公

---

① 习近平:《在第二届世界互联网大会开幕式上的讲话》,《人民日报》2015年12月17日,第2版。

② 参见2022年《中华人民共和国和俄罗斯联邦关于新时代国际关系和全球可持续发展的联合声明》。

③ 《全球数据安全倡议》强调指出,各国应尊重他国主权、司法管辖权和对数据的安全管理权,未经他国法律允许不得直接向企业或个人调取位于他国的数据。俄罗斯和一些国家指出,美国自认为网络是美国发明的,经常肆无忌惮地侵犯别国网络主权和安全,对国际网络空间构成重大威胁。

④ 上海合作组织元首峰会近几年发布的声明和相关宣言中一直反复阐明这个基本精神,尤其是《上海合作组织关于国际信息安全的声明》更具体地阐述了该组织及其成员国的上述原则立场。

⑤ 中方明确提出了统筹全球发展和安全的新理念、新倡议和新思路,得到世界各国的广泛支持。在2022年9月上海合作组织国家元首峰会通过的会议声明中,各成员国对此给予充分肯定。

⑥ 联合国毒品和犯罪问题办公室自1997年成立以来,一直在防范和打击毒品非法贩卖、犯罪和恐怖主义方面给广大发展中国家提供技术援助和支持。这个成功经验可为今后开展打击网络犯罪技术援助提供借鉴。

约》的整体思路是一致的。[①]近年来,联合国编纂的《联合国打击跨国有组织犯罪公约》《联合国反腐败公约》以及一系列反恐怖主义公约,无一例外都明确规定了这些核心要素。《公约》本质上属于国际刑法公约,自然也要遵循上述联合国刑法公约的模式来设定其核心要素。

1.网络犯罪类型及其构成要件。特委会已经注意到这个问题的实质意义,并把它列入《公约》总体框架中进行研究。毕竟制定《公约》的目的是在全球范围内防范和惩治网络犯罪,自然应把各种网络犯罪类型纳入《公约》中,以刑法手段来实现《公约》的宗旨。各缔约国亦应承诺反对利用网络技术从事危害他国国家安全和社会公共利益的行为,反对利用网络技术从事针对他国的大规模监控、非法采集他国公民个人信息,反对以网络为目标攻击、破坏网络系统。从立法技术层面来讲,作为网络犯罪和刑罚的国际刑法公约,它完全有必要按照国内刑法范式分为总则和分则来规范定罪、刑罚原则以及各类网络犯罪的罚则。在《公约》刑事定罪总则部分,可规定刑法一般规范;而在分则部分,应以列举网络犯罪类型的方式尽可能将该类罪的构成要件规定清楚。

2.惩治网络犯罪的诉讼和证据规则。《公约》在设计网络犯罪诉讼程序部分时,不仅要把相应的刑事诉讼原则、刑事管辖权、证据规则、审判制度一并规定清楚,而且还要对打击新形态网络犯罪的特殊执法规则做出规定,比如,电子数据的收集、存储、调取、处理规则,电子数据证据的效力、电子数据链的完整性、可靠性、云电子证据保全措施等,以便各缔约国按照条约义务将其纳入本国法加以适用。这种刑事制度设计是完善打击网络犯罪程序和证据规则必不可少的举措。[②]

3.惩治网络犯罪的国际合作规范。网络犯罪大多具有跨国性,惩治网络犯罪极易牵涉他国司法主权和管辖权问题。如果因打击网络犯罪的需要,不得不在他国执法或司法,就涉及司法协助和警务执法合作。所以,《公约》应尽可能细化网络执法和刑事司法合作程序规则。考虑到国际刑法公约大多有司法协助和引渡的安排,这些国际刑事司法协助与引渡规则可直接引入《公约》。同时,要积极总结各国网络管理经验,强化缔约国协助取证、存储、移交电子证据等合作义务。[③]

---

① 实际上,在任何一部国际条约中,一般都要围绕条约主题设定一些核心要素进行规范。比如,国际刑法公约的核心要素主要关涉公约所指向的国际犯罪界定及其构成要件、刑罚原则等实体法内容、各缔约国在预防和惩处国际犯罪的权利义务关系、惩处各类国际犯罪的程序规则等。

② 《中华人民共和国网络安全法》(以下称《网络安全法》)和《中华人民共和国数据安全法》(以下称《数据安全法》)对此都有所规范,为中国依法打击网络犯罪提供了重要的刑事司法和执法依据。

③ 《数据安全法》第36条规定:"中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定,或者按照平等互惠原则,处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准,境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。"

4.网络安全防控的强制规范。网络安全防控不可或缺,这是网络健康运转的基本保证。《公约》应纳入网络安全防控规则,把网络安全与预防和打击网络犯罪挂钩,将安全责任接驳到网络运营者、服务者、网络技术开发者、网络终端使用者所在的各环节,设定明确的义务和法律责任,以提高网络安全系数和可控性。[①]毕竟通过刑法手段来进行网络安全防控是一种特殊预防措施,值得加以尝试。

5.惩治网络犯罪的技术援助规范。由于大多数发展中国家经济社会发展相对落后,网络技术和设施建设能力薄弱,如果发达国家能给予发展中国家网络技术系统建设援助、网络犯罪侦查技术培训、网络监控技术援助、网络安全技术援助,那么对惩治网络犯罪、保障网络安全无疑是有所助益的。所以,建议在《公约》中加入要求发达国家承担国际发展援助责任的条款,对发展中国家网络犯罪防范技术和网络基础设施建设给予发展援助,帮助发展中国家提高网络安全能力和水平,进一步填补发达国家和发展中国家数字鸿沟,使其与世界各国一道共同担负起预防和打击网络犯罪的重任。[②]

三、因应网络犯罪新态势,增设网络犯罪类别

如果特委会循着联合国国际刑法编纂路径来研究制定《公约》,我们应鼓励借鉴联合国新近制定的其他刑法公约,在《公约》"定罪部分"将网络犯罪及其刑事责任作为重要内容加以规范。

《布达佩斯公约》第2~12条对九类对网络犯罪做过界定,主要包括:(1)非法进入(illegal access);(2)非法截取(illegal interception);(3)资料干扰(data interception);(4)系统干扰(system interference);(5)设备滥用(misuse device);(6)伪造电脑资料(computer-related forgery);(7)电脑欺诈(computer-related fraud);(8)儿童色情犯罪(offenses related to child pornography);(9)侵犯著作权及相关权利的行为(offenses related to infringements of copyright and related rights)。[③]从网络技术发展态势和网络犯罪状况来看,这些界定没有将当代和未来可能发生的网络犯罪新类型纳入打击范围,无法满足国际社会打击网络犯罪的现实需要。联合国特委会必须正视《布达佩斯公约》对网络犯罪类型划分的缺陷,研究吸收各国最新的关于网络犯罪立法的发展动态,重新划分网络犯罪类别。

---

① 《网络安全法》和《数据安全法》都辟有专章对此类规则进行规定。

② 2014年,联合国毒品和犯罪问题办公室授权撰写的《网络犯罪问题综合研究报告(草案)》以对会员国、国际社会和私营部门进行广泛的调查为基础,阐述网络犯罪在全球的趋势、特点、危害、当前国际社会应对的状况和局限,提出制定综合性全球文书、国际示范条款、加强对发展中国家的技术援助等应对方案。在联合国政府间网络犯罪专家组历次会议上,许多发展中国家代表反复提出了发展援助的诉求。

③ 参见曾磊:《惩治网络犯罪攻击合作问题研究》,法律出版社2021年版,第195-207页。

笔者认为,《公约》有必要借鉴《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》的模式[①],采用刑法总则和分则模式对网络犯罪构成要件及其刑事责任和处罚原则做出明确而具体的规定。这就要求,不仅在规范网络犯罪定义和犯罪构成要件上给出明确的界定,而且还应就网络犯罪类型及刑罚原则做出明确规定。具体构想是,在吸收《布达佩斯公约》合理成分的基础上,结合网络犯罪智能性、隐蔽性、匿名性和跨国性的新特点,对网络犯罪及其类别进行定义,明确惩治网络犯罪的对象和范围,拟定网络犯罪刑事责任和刑罚标准。

建议增加《公约》"刑事定罪"部分的篇幅,充分考虑网络犯罪主体日趋多样化、犯罪行为日趋专业化、犯罪活动日趋有组织化和跨国化的现实情况,把网络犯罪主体利用网络技术从事传统犯罪与新型犯罪、以网络为破坏目标的犯罪、网络有组织犯罪、跨国网络犯罪等列入《公约》定罪类型中。考虑到有关非法网络战的定义一时难以形成统一共识,可暂不列入。

从完善网络犯罪罪名体系的角度讲,《公约》可优先就各国国内法普遍认可的网络犯罪类型做出规范,突出体现《公约》案文刑事实体化的总体思路。

(一)规定利用网络技术危害国家安全犯罪

这是《公约》必须重点解决的核心问题之一,也是打击网络犯罪主体利用网络技术从事非传统安全领域犯罪的重要举措。[②]具体而言,(1)规定利用网络技术窃取国家安全情报信息罪。[③]任何个人和组织无视国际法原则,公然利用网络大规模窃取缔约国国家安全情报信息,危害他国国家安全,损害他国重大利益的行为,都要予以刑事归罪。(2)规定非法传播恐怖主义和极端主义罪[④]。随着恐怖主义的演变,恐怖主义分子和极端主义分子利用网络进行恐怖主义和极端主义宣传已成为常态,国际社会必须对此做出反应,对利用网络技术宣扬、传播恐怖主义、极端主义,挑动民族仇恨的活动予以刑事惩治。[⑤](3)规定非法传播暴力信息罪。要对利用网络制作、传播暴力犯罪信息或视频的行为予以严处。(4)规定大规模针对网络进行恐怖主义攻

① 《联合国反腐败公约》是到目前为止采用国内刑法分则模式对各种腐败犯罪行为进行列举的公约,其编纂和发展国际刑法条约的方式得到国际社会的广泛认同。这为联合国制定打击网络犯罪公约提供了范例。

② 在特委会讨论中,各国代表对此意见比较一致。

③ 西方国家对此高度重视,纷纷在其国内国家安全立法中予以规范,甚至不惜泛化国家安全概念,把一些与国家安全相关性不大的问题与之挂钩,对其他国家横加制裁。这在美国司法部滥诉若干华人教授网络窃密案件中反映得淋漓尽致。

④ 上海合作组织2019年缔结了世界上第一部区域反极端主义公约,将有关利用网络进行极端主义、恐怖主义宣传列为犯罪,进行防范和打击。

⑤ 2017年6月9日,上海合作组织成员国元首在第十五次峰会上签署的《上海合作组织成员国元首关于共同打击国际恐怖主义的声明》认为,应采取综合措施打击恐怖主义和极端主义思想传播,包括预防和阻止利用互联网等宣传、煽动恐怖主义和极端主义以及开展招募活动。

击和破坏的犯罪及法律责任。对于恐怖主义组织通过网络技术对有关国家网络系统、网络基础设施进行大规模破坏,制造社会恐慌,胁迫政府改变政策,实现其非法政治目的的行为,必须严惩不贷,唯有通过这样预设惩处网络恐怖主义条款,才能既有效打击恐怖主义组织和恐怖分子对信息关键基础设施的大规模攻击或者作为传播恐怖主义、极端主义和分裂主义的平台实施恐怖主义,也可有效防范某些西方国家情报机构假手网络运营者,把信息和通信技术作为施压工具或者作为破坏他国政治安全的手段,对其他国家进行攻击破坏,严惩其实施国家恐怖主义活动,维护他国网络主权和国家安全。

(二)规定利用网络危害公民权益犯罪

这类犯罪本质上属于国内刑法范畴,大多数国家刑法都有规制,但考虑到它也是世界各国最常见、最猖獗的网络犯罪之一,从净化网络空间环境、维护网络秩序的角度来讲,《公约》有必要将其上升为国际社会打击的网络犯罪类型。这类犯罪至少应包括如下罪名:(1)非法侵犯他人名誉罪;(2)非法侵犯他人知识产权罪;(3)泄露网络个人信息罪;(4)非法侵入他人网络罪。[①]

(三)规定编造、传播虚假信息扰乱经济秩序和社会秩序犯罪

这类网络犯罪最为常见,但《布达佩斯公约》忽视了此类犯罪。《公约》对此应有所反应。故意在网络上编造、发布关涉他国公司虚假财经、会计或信用报告,发布虚假广告,侵害他国公司名誉和形象,破坏他国营商环境,开展不正当竞争,扰乱他国正常经济活动,导致他国经济社会秩序混乱,造成严重危害后果的行为,应追究其法律责任。这是维护国际经济秩序之所需,也是促进国际经济发展和繁荣之所需。

(四)规定法人网络犯罪

由于大多数网络犯罪或多或少有网络公司参与或卷入,网络公司作为网络犯罪主体颇为常见,因此,遏制法人网络犯罪就成为必然的选择。《布达佩斯公约》将法人纳入网络犯罪主体范围,但只把代表法人权力实施、为法人利益做出决定而实施、法人控制下实施三种行为方式列为应予刑事处罚的行为。这种规定有一定局限性,不利于追究法人出于其他目的而实施的网络犯罪。故此,《公约》应适当扩大法人网络犯罪的归罪范围,具体而言,应增加以下规定:(1)规定非法网络经营和服务罪。将网络运营者不遵守法律、行政法规,不尊重社会公德,不遵守商业道德,不履行网络安全保护义务,故意违法从事经营和服务活动,造成破坏

① 2015年《中华人民共和国刑法》(以下称《刑法》)修正案(九)第28~30条对若干网络信息犯罪做出明确的界定,为我国打击此类犯罪提供了新的法律依据。

网络的犯罪行为，列入刑事处罚范畴。[①](2)规定网络数据安全渎职罪。即网络运营者不采取技术措施和其他必要措施，保障网络安全、稳定运行；不采取有效措施应对网络安全事件，防范网络违法犯罪活动，导致网络数据的完整性、保密性和可用性遭到严重破坏而构成犯罪的行为。(3)规定网络管理渎职罪。建议对网络安全管理部门严重失职渎职，导致国家信息关键基础设施遭受破坏，国家网络信息严重泄密，经济社会运转受阻的行为，追究刑事责任。[②]

(五)规定违法提供网络安全程序和工具犯罪[③]

网络犯罪的一个重要前提是熟练掌握和使用网络安全程序和工具，因此对提供网络安全程序和工具的上游行为应设限，把非法提供网络安全程序和工具的犯罪列入惩治范围，是非常必要的。《公约》应对非法制作或提供用于侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序和软件工具的行为，以及明知他人从事危害网络安全的活动而故意为其提供技术支持、广告推广、支付结算等帮助的行为，予以归罪处理。。

(六)规定破坏信息关键基础设施犯罪[④]

信息关键基础设施是国家重要资产，关系国计民生，一旦信息关键基础设施受到破坏，其影响和损失往往难以估量，故而必须对故意攻击、破坏公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域网络关键基础设施，造成严重危害国家安全、国计民生、公共利益的行为，予以刑事处罚，以遏制网络攻击活动，维护网络基础设施安全。这是制定《公约》的一个重要使命。在当前国际格局复杂多变的大背景下，一些国家利用网络技术开展网络战，破坏其他主权国家的网络空间安全，甚至破坏别国信息关键基础设施正常运行，已引起国际社会的高度警惕。联合国在编纂和发展打击网络犯罪国际刑法过程中不能无视这些新挑战和新威胁，否则，不仅对网络空间安全不利，而且对维护世界和平与安全也是有害的。

(七)规定跨国网络诈骗犯罪

《布达佩斯公约》第8条对网络诈骗犯罪做了规定，但归罪范围较窄，且对跨国网络诈骗未做规定。《联合国打击跨国有组织犯罪公约》对打击跨国有组织犯罪有诸

---

① 《网络安全法》有相关规定，可供联合国特委会参考。我国特委会专家组代表团似可据此与各国展开磋商讨论。

② 《网络安全法》和《数据安全法》对上述犯罪都有相应规定。联合国特委会似可参考中国的立法成例，在相关条文设计中予以采纳。

③ 《网络安全法》第48条和第60条对此类犯罪做出了规定。

④ 参见《网络安全法》第31~39条。

多规范,但没有对跨国网络诈骗犯罪做出明确规定,尽管其法律原则可延伸适用,但从“法无明文规定不为罪”的原则来讲,还是需要《公约》明确规定。故此,《公约》应把打击新形态跨国网络诈骗犯罪列入其中,即不仅要将利用网络从事传统诈骗活动予以刑事归罪,还要把跨国有组织网络犯罪集团利用网络新技术实施新形态诈骗犯罪,包括通过非法获取口令代码、模拟仿生声频音频谱、恶意代码等方式,实施跨国电信诈骗、跨国金融网络诈骗、国际互联网诈骗、建立跨国销售假冒伪劣商品网络平台、制作发布虚假广告信息促销违禁物品和管制物品等行为,规定为犯罪行为,予以刑事处罚。这也是拓展《联合国打击跨国有组织犯罪公约》适用范围,完善网络国际法治的一个有益补充。

(八)增设投放网络病毒罪

随着网络技术的飞速发展,世界各国网络黑客经常利用自己掌握的网络技术编写病毒程序,故意违法向社会发布计算机系统漏洞、计算机病毒、网络攻击方法、网络侵入方法等,导致各种网络病毒大规模爆发,造成被攻击的网络系统甚至一个地区网络系统终端大面积瘫痪,严重影响网络系统正常运行,各国国内网络安全法对此行为一般都会做归罪处理,所以,联合国有必要将各国的成熟做法纳入国际犯罪罪名体系,进一步鼓励各缔约国强化刑事处罚机制,遏制黑客故意危害网络安全。

除了设定上述罪名之外,《公约》还应把网络犯罪的共犯、从犯、胁从犯、教唆犯、上下游犯罪、犯罪既遂和未遂规定清楚,尤其在设定刑事责任方面尽可能引入刑罚量刑原则,以此鼓励各缔约国朝着网络安全保护刑事政策趋同化的方向迈进。这样规制,不仅可以为缔约国打击网络犯罪的国际合作奠定新的国际法基础,而且也为今后国际刑法公约朝着刑事实体规范趋同化的方向发展树立新标杆。

四、突出程序规则针对性,强化惩治网络犯罪程序机制建设

联合国在制定《公约》过程中应尽可能把刑事诉讼程序和行政执法规则实用性和可操作性问题摆到重要位置上进行考量,做出合理的机制建构。唯有如此,才能更好地奠定打击网络犯罪的诉讼法制基础,提高网络执法和司法的效能。

(一)兼收并蓄不同法系刑事诉讼规则

《公约》设计有关缔约国追究网络犯罪刑事诉讼的条约义务时,应统筹考虑各法系诉讼和证据规则所存在的重大差异,尽可能寻找几大法系共通的诉讼原则和制度加以融会贯通,尤其要将侦查、起诉、审判网络犯罪案件程序规则和证据规则规范化,以便各缔约国将其转化为国内法并纳入国内诉讼体系中加以适用。因此,《公约》要适当做好各法系诉讼规则之间的平衡。这种刑事诉讼制度设计理念在联合国制定《国际刑事法院规约》中已得到完整体现。《公约》也应遵循《国际刑事法院规约》

制定的思路，借鉴其成功经验。

第一，在刑事调查方面，鉴于网络技术公司掌握网络技术、网络资源和用户资料，可为执法和调查网络犯罪提供配合，《公约》应对网络运营服务公司包括电信、金融、互联网公司设定配合执法机关保护、维持、存储、调取网络数据，禁止非法删除重要数据，禁止伪造网络信息的法律义务。中俄等国刑事诉讼法和网络安全法对此有强制性的法定义务，英美法有控辩交易制度，但大多数国家国内法中缺少公私合作开展网络刑事调查的制度安排。联合国打击网络犯罪政府间专家组自2011年成立以来，多次讨论公私合作预防和打击网络犯罪的问题，尽管各方对此争议较大，但正在逐步朝着达成共识的方向迈进。《公约》如能做出公私合作开展网络犯罪刑事调查的安排，将会有效弥合不同法系在此问题上的制度差异。这必将有助于打击网络犯罪刑事调查合作机制的进一步健全和完善。

第二，在电子证据调取方面，鉴于此类问题往往涉及国家网络主权问题，具有敏感性，如果没有国际法依据，有关国家很难越过法律障碍开展此类司法或执法活动，《公约》应授权缔约国执法机关依法跨境调取网络电子数据，收集网络犯罪证据，查封扣押网络设备和终端，查封、冻结、扣押、没收网络犯罪财产及其收益等，以便侦查人员对跨境网络犯罪案件开展刑事调查，收集犯罪证据。《布达佩斯公约》对此已有规制，而且为美西方各国执法机关所认可。[①]制定《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》，就是遵循这个基本路径推进的，即先有区域公约，再由联合国制定统一公约。

第三，在电子证据采信方面，《公约》应通过规定电子证据采信制度，促使各缔约国接受和认可电子证据的效力，改变传统刑事诉讼法不认可电子证据的有效性、客观性和可靠性的做法。截至目前，各国刑事诉讼法在这个问题上尚未完全趋同。[②]为了推动这项刑事诉讼制度改革，联合国网络犯罪政府间专家组在其撰写的《网络犯罪问题综合研究报告（草案）》中，呼吁国际社会制定与电子证据调取相关的国际示范条款、电子证据国际合作文书、有约束力的全球性法律文书等。如果联合国在制定《公约》时做出相应的安排，将合法收集的电子证据视为法庭可采信的证据，就可为各缔约国修改国内法提供示范，从而促使各国更顺畅地接受电子证据采信制度。

第四，在刑事强制措施方面，鉴于网络犯罪侦查的特殊性和网络数据易更改、删除、毁灭的特点，《公约》应设计相关条款，允许执法人员采取特殊手段，对危险的网络犯罪嫌疑人尤其是恐怖组织成员予以临时拘留逮捕，防止其逃避法律追究或者利

① 该区域公约在此问题上做出了相关规定。

② 我国司法实践中已将区块链技术引入电子证据的存证，初步建立了关于区块链存证的临时性规范体系。参见张中、赵航：《建立区块链证据采信新规则》，《检察日报》2021年6月25日，第3版。

用有关国家的法律漏洞而逃之夭夭。[①]对特别危险的网络运营人可执行刑事强制措施,禁止其从事网络开发、运营服务和其他活动,查封其利用网络进行犯罪的网络系统,查抄收缴网络设施和计算机及其他电子终端,防止其破坏、销毁电子数据,消灭犯罪证据,防止其继续从事更加危险的网络犯罪;对网络利益链条,采取执法措施予以斩断,防止网络犯罪分子或犯罪集团从中谋取利益。[②]尽管这些制度安排在各国国内法中不是特别普遍,但也存在先例。"9·11"事件后,美国颁布的《爱国者法案》有类似的制度安排,该法赋予联邦警察监控恐怖组织和恐怖分子网络通信信息的特殊权力,一旦发现恐怖组织或恐怖分子策划网络恐怖活动,执法人员有权采取超常规的强制手段加以处置。我国《刑法》《网络安全法》《数据安全法》等有相关条款专门就此刑事调查制度做出了安排。《公约》如能引入这些制度,对遏制网络犯罪的泛滥无疑是有益的。

(二)适当扩大网络行政执法权

在国内网络管理过程中,网络执法机关往往要不间断地对可疑网络信息进行严密的技术监控,一旦发现违法犯罪信息,就会采取措施加以调查、处置,比如,对一些违法网络公众号、交友平台,网络执法部门可能会采取屏蔽公号、删除有害信息、禁止登录网络账号、限制浏览等措施或者采取责令网络公司或交友平台删除有害信息、直接限制或注销交友账号等方式予以处理。由于有些公众对网络监管所造成的不便大多不明就里,担心这类网络监管容易造成网络管理部门滥权,侵蚀公民自由权利,因而往往不愿支持此类立法。这就需要联合国先行一步,在《公约》中适当设置特殊执法条款,对网络风险管理、信息关键基础设施应急处置、网络信息安全破防应对、网络社会危机应对等,设置相应的网络监管执法条件和执法权限,明确要求各国网络监管部门依法采取适度的执法手段和措施,尽可能有效地保障网络监管和执法的公正与公平,防止肆意侵犯公民自由与权利。

五、创新国际司法与警务合作模式,提升打击网络犯罪效能

在《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》中,有关司法协助、引渡和警务合作的条款占了很大的篇幅。后者用一个专章专门规定若干司法协助、引渡和警务合作的特殊制度,诸如,对腐败分子的国际追捕,对腐败资产的国际追缴、冻结、扣押和没收,对腐败资产的分享等。《联合国打击跨国有组织犯罪公约》创设了联合侦查跨国有组织犯罪案件制度。这类司法协助与执法合作规则,与传统的国际刑事司法协助和国际警务合作相比,有若干重大突破。这为各国开展司法合

① 2018年最高人民法院、最高人民检察院、公安部、司法部《关于办理恐怖活动和极端主义犯罪案件适用法律若干问题的意见》对此有专门规定。

② 参见中国《刑法》修正案(九)。

作奠定了新的国际法基础。

鉴于上述国际刑法条约，联合国特委会在制定《公约》过程中很可能会参照这些条约的体例，对相关国际刑事司法协助与国际警务合作制度、体例和结构进行规划。基于此，笔者认为，根据网络犯罪的规律特点以及预防和打击网络犯罪的特殊要求，有必要在《公约》"国际合作"部分就有关打击网络犯罪司法协助、警务执法合作进行更有针对性的制度创新，以提升网络犯罪执法和司法的效能，具体而言：

1.构筑打击网络犯罪国际刑事司法协助新体系。《公约》应设立专章，对文书送达、调查取证协助、联合侦查跨国犯罪案件、协助追捕逃亡犯罪嫌疑人、协助临时拘留逮捕、协助追缴没收赃款赃物、引渡、刑事诉讼移转管辖、承认和执行外国刑事判决等做出规定。

2.创新网络执法国际合作机制。各国执法部门在预防和惩治来自外国的网络犯罪时，无不需要借助他国网络技术力量的介入、网络公司的配合、他国执法机构的合作，包括协助检测查找网络安全漏洞、查找网络后门、追踪网络犯罪信息源、查找恶意插入网络木马、破解网络病毒、抓捕网络黑客、截断恐怖主义。因此，《公约》应就网络执法国际合作做出详细规定，将发布国际通缉、协助遣返非法移民、大型活动安保警务合作、非法移民管控、难民管理合作等当代国际警务合作形式一并引入网络执法合作中。此外，为了提高各国执法部门网络监管水平和网络治理能力，《公约》应设定相应条款，推动各国加强网络管理部门之间和执法机关之间的网络空间治理合作、网络技术研发和标准制定合作、网络技术培训合作等。

3.遵循国际执法合作的基本原则。《公约》应明确要求，各缔约国必须承诺尊重他国司法主权、司法管辖权和对电子数据的安全管理权，未经他国法律允许不得直接跨境向有关网络企业或个人调取位于他国的数据。[①]如因打击网络犯罪需要跨境调取数据，应通过司法协助渠道或其他相关合法渠道解决，不得擅自侵害他国司法主权和数据安全，也不得随意侵犯他国公民个人隐私，妨碍公民自由和人权。

4.鼓励区域网络执法合作。《公约》应要求缔约国加强区域网络执法合作，充分发挥区域组织职能，建立健全专业区域组织执法网络体系，发挥多边合作不受外界第三方干预的优势，高效开展网络执法合作。

六、推进网络监管制度趋同化，夯实网络法治基础

网络监管是预防和打击网络犯罪的前提条件和基础。《公约》鼓励缔约国建立网

① 在联合国政府间网络犯罪专家组第四次会议上，各国专家就此进行了深入探讨，对跨境调取电子数据证据持有不同的立场。大多数专家认为应尊重各国对网络管理的司法主权。

络监管制度,明确网络监管主体责任,设定网络监管措施,强化网络安全保障体系建设,可考虑在《公约》"预防措施""实施机制"部分适当增加这方面的条款,将网络监管制度法定化。

(一)化解网络监管认知分歧,凝聚网络监管趋同化共识

第一,美西方应抛弃对网络监管制度的双重标准。美西方国家在网络监管上一贯采取双重标准,对国际社会网络监管制度建设造成巨大的冲击。长期以来,美西方一方面严密监管本国网络,无底线进行全网络信息情报收集,甚至对他国领导人和社会精英通信和网络交流实施全方位监控与窃听窃密①。另一方面,它们经常利用所谓的网络自由,恶意操纵舆论,对其他国家网络监管制度污蔑抹黑,指责别国进行网络攻击和窃密,对别国网络监管污名化,造成网络监管不公正,给这些国家的主权、安全和社会稳定带来巨大的隐患和挑战,造成广大发展中国家网络监管的巨大困惑,受到各国的强烈抵制和反对。

第二,美西方国家应加快网络监管法治化的步伐。美西方以《布达佩斯公约》为依据,开展打击网络犯罪国际合作,但该公约并没有规定网络监管的内容,因而很难依据该公约开展网络监管国际合作。国际社会难以将《布达佩斯公约》作为打击网络犯罪的"国际标准",就不足为奇了。②除非美国等西方国家改变原有立场,向网络监管法治化的方向迈进,否则,这种监管制度缺失会给网络刑事法治留下越来越大的漏洞。

第三,美西方不应再继续利用本国秘密网络监管手段干涉别国内政。美西方经常打着"民主、自由、人权"的旗号,在社交媒体上搭建针对他国的巨大宣传网,通过设立虚假账户、传播相似内容、制造话题热度等手段发动政治宣传和造谣行动,③干涉别国内部事务,策动"颜色革命",支持这些国家内部反政府势力游行示威,制造骚乱,给这些国家带来严重的政治安全问题。这种网络政治工具化的做法极大地损害了网络国际合作环境。联合国特委会在制定《公约》过程中,应充分评估这些潜在的政治安全隐患,鼓励各国加强网络监管,避免网络监管和打击网络犯罪政治工具化、武器化,还原打击网络犯罪的法治本质,从而更好地预防和惩治网络犯罪。

---

① 2022年9月5日,国家计算机病毒应急处理中心和360公司分别发布了关于西北工业大学遭受美国国家安全局网络攻击的调查报告,美国国家安全局下属的特定入侵行动办公室使用了40多种不同的专属网络攻击武器,持续对西北工业大学进行攻击窃密,窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。参见《西北工业大学遭美网络攻击 揭开"黑客帝国"虚伪面纱》,《中国纪检监察报》2022年9月6日。

② 许多发展中国家在联合国政府间网络犯罪专家组讨论会上经常就此做出阐述,属于老生常谈的话题。

③ 参见《2022年9月26日外交部发言人汪文斌主持例行记者会》,https://www.fmprc.gov.cn/web/fyrbt_673021/jzhsl_673025/202209/t20220926_10771881.shtml,2022年10月11日访问。

（二）客观认知网络安全的脆弱性，强化网络安全风险监测制度建设

众所周知，网络本身存在着许多安全隐患。（1）Internet是一个开放的、无控制机构的网络，黑客经常会侵入网络中的计算机系统，或窃取机密数据和盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。（2）Internet的数据传输是基于TCP/IP通信协议进行的，这些协议缺乏传输过程中的信息安全措施。（3）Internet上的通信业务多数使用Unix操作系统来支持，Unix操作系统中明显存在的安全脆弱性问题会直接影响安全服务。（4）在计算机上存储、传输和处理的电子信息，没有传统邮件通信那样的信封保护和签字盖章。信息的来源和去向是否真实，内容是否被改动，以及是否泄露等，在应用层支持的服务协议中是凭着“君子协定”来维系的。（5）电子邮件存在着被拆看、误投和伪造的可能性。使用电子邮件来传输重要机密信息存在着很大的风险。（6）计算机病毒通过Internet的传播给上网用户带来极大的危害，病毒可以使计算机和计算机网络系统瘫痪、数据和文件丢失。在网络上传播病毒既可以通过公共匿名FTP文件传送，也可以通过邮件和邮件的附加文件传播。[①]基于此，联合国制定《公约》时，不能无视网络自身存在的脆弱性，必须通过创制网络监管法律制度，防患于未然，防止网络犯罪分子实施网络犯罪。

（三）充分认知网络监管的极端重要性，提高网络监管法治化水平

首先，网络监管是预防网络犯罪的重要举措。一般来说，在网络犯罪方式上，犯罪分子往往通过破坏网络物理安全、结构安全、系统安全、应用系统安全和管理制度，或者采用中断、截获、修改和伪造等方式针对网络进行攻击，从而瘫痪网络系统，使之无法继续工作，破坏网络安全。如果执法部门能通过强有力的网络监管，及时发现网络隐患以及网络犯罪动向和线索，就可以将网络犯罪扼杀在预谋阶段，从而有效地预防和制止网络犯罪危害后果的发生，从而保障网络安全。[②]

其次，加强网络监管是打击网络犯罪的重要手段。由于网络犯罪具有跨国性、匿名性、智能性，而电子证据不稳定、易灭失，各国执法机关在打击网络犯罪方面经常面临诸多现实难题和挑战。许多国家的实践充分证明，唯有通过网络监管，才能及时发现网络犯罪活动轨迹，截获电子信息和犯罪证据，斩断网络犯罪链条，有效打击网络违法分子活动。

联合国应正本清源，反对网络监管的双重标准，吸收中国和其他国家网络安全风险管理经验，通过制定《公约》，授权缔约国加强互联网安全风险管理，鼓励各国建立健全网络监管体制机制，将网络监管政策规范化、趋同化、法治化，鼓励各国依法监测、防御、处置网络安全风险和威胁，保护信息关键基础设施免受攻击、侵入、干扰和

① 参见甘利杰、孔令信、马亚军：《大学计算机基础教程》，重庆大学出版社2017年版，第152页。

② 我国《网络安全法》对此做了许多相关规定。

破坏,维护网络空间秩序,维护网络信息安全。

七、统筹打防一体化关系,健全国际网络刑事法治

《公约》草案专门设置预防措施和实施机制一章,在磋商谈判这两部分条款过程中,有以下几个法律关系需要理顺。

(一)正确处理预防和打击网络犯罪一体化的关系

在惩治犯罪方面,“打防一体化”是世界各国普遍认同的基本刑事政策。《公约》草案设置“预防措施”一章,目的就是贯彻这一国际公认的基本刑事政策。为了落实这个构想,《公约》应妥善处理好以下法律问题:

第一,在预防方面,《公约》应从以下几个方面进行规制。一是政策层面。联合国应通过订立相关条款,规定缔约国建立和完善国家网络安全体系和数据安全治理体系的条约义务,要求各国积极采取措施,监测、防御来自国内外的网络安全风险和威胁,保护关键基础设施免受攻击、侵入、干扰和破坏,开展网络治理、网络技术研发和标准制定,推进网络安全社会化服务体系建设,支持企业、研究机构、高等学校、网络和相关组织参与网络安全标准和行业标准制定,推动网络保护技术创新,更好地从政策上给予网络安全保障,提高网络犯罪预防能力。[①]二是网络管理层面。《公约》应设定相关条款,要求各国加强网络硬件管理,加强网络运行安全管理,强化信息关键基础设施运行安全管理,倡导建立健全网络安全等级管理、风险管理、预警管理、应急管理制度,建立健全用户信息保护制度,全方位保护网络安全。三是法律层面。《公约》应设定缔约国加强网络安全立法的条约义务,敦促各缔约国制定预防网络犯罪法律法规和行政执法规章,要求网络运营者、网络技术开发者、网络使用者遵守法律,积极采取防范措施,实现网络犯罪预防前置法的特殊功能。

第二,在惩治方面,有几个方面须引起重视:一是要贯彻预防为主、打击为辅的刑事政策。这个刑事政策是世界各国公认的基本刑事政策。《公约》有关预防网络犯罪的国际法规范,如同国内法一样,属于前置法,是为了防范、控制、制止网络犯罪而设定的;而有关制裁网络犯罪的国际法规范属于后置法,是为了制裁、处罚网络犯罪而设定的。通过“打防结合”,相互配合,实现预防和惩治网络犯罪、维护网络安全的目标。二是要通过特殊预防来达到一般预防的目的。特委会在制定《公约》草案过程中,应积极贯彻这种理念,将特殊预防网络犯罪的精神融入《公约》之中。

(二)稳妥处理打击与保护的关系

国际社会制定《公约》的目不是仅为打击网络犯罪,更多的考虑是如何通过打击

① 《网络安全法》第二章至第四章和《数据安全法》第二章至第五章从不同侧面对这些问题进行了规定。

网络犯罪，保护网络赖以生存和发展的社会经济基础，保护国家网络主权、安全和发展利益，保护人权和自由，维护公平正义。所以，《公约》要稳妥处理打击与保护的关系。

第一，在打击方面，一是明确打击的对象是网络犯罪人，包括自然人和法人。而国家不能被列为打击对象，除非国家实施网络恐怖主义，构成国家恐怖主义罪行。二是明确打击手段是国际法许可范围内的行政、执法、司法和科技手段。《公约》应明确禁止以违反国际法的手段包括非法战争、恐怖袭击、毁灭性武器攻击等手段对信息关键基础设施的攻击、破坏和损毁。三是明确打击不超过必要限度。对网络犯罪的打击、制裁、惩罚，只要在合法框架内，都是可以接受的正当防卫。《公约》设定打击措施时，适当加入国家自卫权、自保权条款，不仅符合国际法原则，也符合防范和打击网络犯罪的实践逻辑。

第二，在保护方面，鉴于《公约》的要务是维护网络安全，有必要在《公约》中将保护对象和范围加以明确。一是保护国家网络主权。除了在《公约》“一般规定”中申明这一原则之外，应在“预防措施”和“实施机制”中具体予以规范，重点要禁止缔约国情报机构、军方采取非法手段窃取别国政治、经济和军事重要信息或者肆意编造谣言，散布虚假信息，扰乱别国政治、经济、金融和社会秩序，也要禁止非法跨境搜集、调取、截获电子信息，侵犯别国司法主权和刑事管辖权，等等。二是保护网络安全。这打击网络犯罪本身也是保护网络安全的重要手段，在这一点上不必特别设定更多的条约义务，只须在“一般规定”和“预防措施”部分申明相关原则立场即可。三是保护国家利益发展。随着网络信息技术的高速发展，区块链、数字经济、数字货币等新经济给世界各国带来巨大的财富效应和发展机会，任何国家都可从中获取相应的利益。但是，任何新生事物总有正反两面性，有的国家在财富分配中获得巨大利益，有的国家所得无几；一些网络发达国家利用网络技术和资源优势，从全球各地获取巨额财富，一些国家却被剥夺了相应的利益。数字鸿沟日益加剧世界贫富差距，带来许多经济社会问题。所以，在制定《公约》时，不能忽视网络犯罪对数字经济发展的破坏作用，要尽可能兼顾各国经济发展可持续性、均衡性、包容性，以便更好地保护地区和世界经济的发展繁荣。四是保护人权。在网络时代，保护人权是捍卫人类共同价值观和精神要求的必要之举。《公约》要在“定罪”部分设定相应的惩罚条款来打击网络社会形形色色侵犯人权的行为。同时，在“防御措施”部分设定相应的防范措施，防止侵犯人权。五是保护公平正义。打击网络犯罪同样需要打击网络虚拟社会中侵害公平正义的行为，为此，《公约》不仅要在“一般规定”中加以明确，也应在其他实体部分有所体现，以便敦促缔约国通过执法和司法机制来保护公平正义。

（三）统筹兼顾国内治理与国际治理的关系

从世界范围来看，网络犯罪主要是国内刑法规制的犯罪。但是，由于互联网

是全球互联互通的,任何一个国家的网络系统只要连接到互联网上,就成为全球网络的一个组成部分或一个子系统,所以,网络犯罪极易成为全球性问题。为了治理网络问题,遏制网络犯罪,就要从全球视角看问题,统筹兼顾国内治理和国际治理的关系。

第一,从国内治理来看,至少应着力解决如下问题:一是加强网络治理立法。《公约》应敦促各缔约国将网络犯罪纳入本国刑法,将网络国内治理刑事法治化。二是加强国内网络安全制度建设。要将网络安全实施机制落实到本国网络管理过程中。三是加强网络司法能力建设,创新刑事诉讼制度,将网络技术运用到司法过程中,促进电子证据制度的发展和完善,依法惩治各类新型网络犯罪。

第二,从国际治理来看,涉及全球治理和全球秩序的问题更多,需要统筹协调处理。[①]一是坚持以联合国为核心的网络治理国际体系。《公约》应旗帜鲜明地阐明这个基本原则,将国际网络治理纳入正轨。二是坚持网络治理多边主义,反对单边主义。《公约》应反对网络武器化、政治工具化,明确反对任何国家借助网络治理干涉别国内政,侵害别国利益,反对借助网络治理搞小圈子,以区域治理代替全球治理。三是坚持以国际法为基础的国际网络治理秩序。《公约》出台生效后,其中有关打击网络犯罪的刑事规范就可成为国际网络刑事法的重要组成部分,有关预防网络犯罪的规范就可构成国际网络安全法的组成部分。由国际网络刑事法和国际网络安全法共同组成网络空间国际法,成为调整国家间有关国际网络安全的权利义务关系的准绳。故此,在制定《公约》时,不仅要把刑事法规范阐述清楚,也要把国际网络安全法的原则和精神贯彻其中,为国际网络治理夯实法律基础。

为了推动各国构建和平、安全、开放、合作的网络命运共同体,建立多边、民主、透明的网络治理体系,联合国在制定《公约》过程中,应给国际网络刑事法预留出发展空间。联合国应围绕网络安全问题制定出更多的全球性文件,包括国际网络安全公约、协定、战略和指南,不断扩充国际网络刑事法治范畴,以此构建起国际网络刑事法体系。

结语

《公约》是联合国正在草创中的一部国际刑法公约,受到国际社会的广泛关注。为让《公约》顺利出台,国际社会应本着良法善治精神,积极借鉴当代国际刑法的发展经验,结合网络技术的发展状况,及时跟踪分析网络犯罪的动态和趋势,制定出包含国际刑事实体法、国际刑事程序法、国际网络执法合作法和网络监管规则的综合性公约,为各国提供打击网络犯罪的国际法依据,以适应国际社会预防和打击网络

① See UN, A-RES/70/174.

犯罪的需要。一旦《公约》如期诞生，必将对国际社会预防和打击网络犯罪，维护网络安全和秩序，促进数字经济发展，促进网络技术为人类发展与进步发挥不可估量的作用。我国应积极主动参与和推动《公约》的制定工作，贡献中国智慧和中国方案，为在全球网络治理中发挥负责任大国的作用而不懈努力。

On the Codification of the United Nations Convention against Cybercrimes

Abstract: The United Nations is studying the formulation of a convention against cybercrimes, which is of great significance to the latest practice of the United Nations in developing and codifying international criminal law. In order to better carry out global network governance and maintain the international network security order, it is necessary for the United Nations to widely absorb the successful experience and practices of various countries in preventing and combating cybercrimes in the process of formulating the convention. Furthermore, it is suggested to legalize and standardize the substantive laws, procedural laws and special enforcement rules, and to clarify the basic norms and core elements of the convention. In response to the new trend of cybercrimes, the Convention shall stipulate new categories of cybercrimes and consequential legal responsibilities, highlight the pertinence of procedural rules and strengthen the construction of a procedural system for punishing cybercrimes, innovate international judicial cooperation models to enhance the effectiveness of combating cybercrimes, promote the convergence of the network supervision system and consolidate the foundation of the cyberspace rule of law, coordinate the internal and external relations of the integration of combat and prevention, and improve the international network criminal rule of law in the field of cyberspace.

Key words: combating cybercrimes; network governance;network security

（责任编辑：彭芩萱　钱静）