暗网犯罪国际法规制的问题与进路

李　彦

摘要：暗网的匿名性、加密性和跨国性特征，使暗网犯罪较一般网络犯罪更具特殊性。一般性国际刑事规则和网络犯罪国际刑事规则存在的局限性，国际软法法律拘束力的缺失，影响暗网犯罪国际法规制的效能。解决暗网犯罪国际法规制问题对技术治理、顶层设计和执法合作提出了更高要求。应确立技术和法治相结合的原则，以法律促进和保障技术发展，以技术拓展法律的规制范式；并建构和完善暗网犯罪国际治理的顶层设计，推动网络犯罪国际刑事规则中增加规定“暗网犯罪”条款和暗网犯罪国内法规制的具体化；且继续强化打击暗网犯罪国际执法合作，并将发展中国家纳入其中。

关键词：暗网犯罪；匿名性；加密性；《联合国打击网络犯罪公约》

中图分类号：D990　　**文献标识码**：A　　**文章编号**：1000—8691（2023）06—0105—09

暗网犯罪已成网络治理的重灾区和国际社会普遍关注的罪行。暗网犯罪较一般网络犯罪更难追踪，暗网用户信息被加密地传送到计算机中，越多人使用加密层越厚；而加密货币支付进一步保障了暗网犯罪的隐蔽性。目前，相关研究多集中于暗网犯罪的国内刑事规制上，鲜有综合考量暗网犯罪国际法规制的问题和进路。本文在分析暗网犯罪国际法规制存在的问题基础上，从多个层面提出应对方案。

一、暗网犯罪的特殊性

互联网由表网、深网和暗网三层结构组成。表网（Surface We）是常用的以 .com 或 .org 或 .net 为域名的普通网站，可直接通过常规搜索引擎访问，是一般网络犯罪发生的空间。深网（Deep Web）是因访问限制而使搜索引擎无法检索，需特定密码和加密浏览器才能访问的网站，如大学和研究机构的数据库、保险公司、银行的数据库等。[①] 由于储存了特定主体的保密信息，在深网中易滋生网络诈骗、侵犯个人信息等犯罪。暗网（Dark net）是深网的特殊加密子集，是通过点对点的链接、采用多层次加密、多节点存取等技术形成的具有匿名性、加密性和跨国性的信息交流平台。首个可用于进入暗网的软件“自由网”（Freenet）是由伊恩 • 克拉克（Ian Clark）开发并于 2000 年 3 月公开发布，以使用户匿名共享文件、浏览和发布自由网站。同年，美国海军研究实验室（US Naval Research Laboratory）开发了旨在保护美国军事人员、特工和持不同政见者身份的匿名软件“洋葱路由”（The Onion Router，Tor），为用户伪装互联

基金项目：本文是国家社会科学基金重大项目“网络空间国际规则博弈的中国主张与话语权研究”（项目号：20&ZD204）、国家社会科学基金青年项目“全球网络犯罪法律规则制定与中国方案研究”（项目号：20CGJ013）的阶段性成果。

作者简介：李　彦，女，河南财经政法大学法学院副教授，主要从事网络犯罪国际法治研究。

① 匿名者：《深网》，张雯婧译，北京：中国友谊出版公司，2020 年，第 20 页。

网请求，并通过随机的其他 IP 地址传递信息，使用户请求与用户保持独立以免被追踪。隐形互联网项目（Invisible Internet Project，I2P）是 2003 年公开发布的发送端、输入通道、输出通道、接收端 4 层加密的匿名技术，匿名性更强。[①] 不过，因操作简单，以 Tor 为依托的暗网资源更多。2004 年，美国海军不再为 Tor 提供资金支持，并将其转交“电子前哨基金会”（EFF）经营，Tor 开始面向公众使用，专门用于毒品买卖、儿童色情和恐怖主义的 Tor 域名开始出现。[②] 匿名技术或软件的推广和使用，为暗网犯罪的滋长提供了有利条件。

暗网犯罪是通过暗网实施的犯罪。暗网的匿名性、加密性和跨国性使其较一般网络犯罪更具特殊性。一是暗网的匿名性、加密性使暗网犯罪具有高度隐蔽性。暗网采用的加密技术，不仅可使网站、用户、IP 隐形，还有节点难发现、服务难定位、通信关系难确认、用户难监控等特点。以 Tor 为例，它不仅能使通信主体匿名，且支持隐藏服务（Hidden Service）机制。隐藏服务的用户和服务提供商都能掩盖身份，且位置皆不可追踪；加之服务提供商还常将网站托管到其他服务器上，执法机关更难追踪。[③] 二是暗网的匿名性使暗网交易支付更具特殊性。暗网的匿名性与数字货币的加密性契合，数字货币支付在暗网中盛行。与传统货币结算不同，数字货币结算因避开银行支付且是匿名交易，执法机关很难有效监管。如比特币因交易双方身份、比特币地址隐匿，且储存在加密的个人私钥中安全性高，吸引了大量犯罪分子借此进行非法交易。三是暗网的跨国性使暗网犯罪治理对国际合作提出更高要求。暗网的跨国性，扩张了暗网犯罪的危害范围和后果：匿名通信技术操作简单、上手容易的特点，降低了技术要求和准入门槛，政府、个人和企业均可能成为暗网犯罪对象，政治、经济、文化、军事事务等均可成为犯罪内容。且“随着犯罪与侦查对抗的升级，……暗网犯罪呈跨国有组织化发展”[④]。有组织犯罪对国际治理提出更高要求，亟需各国全面合作。2017 年 7 月，美国等国执法部门联合查封“阿尔法湾市场”（AlphaBay Market），就离不开相关国家的通力合作。行动中，执法部门搜索了美国、加拿大、泰国等国的多地，才最终确定网站管理者和网站服务器位置。

二、暗网犯罪国际法规制的现状

暗网犯罪国际法规制主要依赖一般性国际刑事规则、网络犯罪国际刑事规则，国际软法也产生一定的法律效果。

（一）主要依赖一般性国际刑事规则

一般性国际刑事规则包括打击洗钱行为、腐败犯罪、毒品犯罪、恐怖主义犯罪等领域的国际公约，可用于打击暗网犯罪。

暗网犯罪如洗钱行为、腐败犯罪、毒品犯罪等属跨国有组织犯罪，相关公约可适用。如《联合国禁止非法贩运麻醉药品和精神药物公约》第 3 条规定“兜售、分销、出售”麻醉药品或精神药物为犯罪，可适用于打击暗网中日益猖獗的毒品交易行为。在暗网中出售、分销毒品、教授制毒方法较为普遍，犯罪要素与传统毒品犯罪一致，公约可以适用。《联合国打击跨国有组织犯罪公约》第 5—8 条规定“参加有组织犯罪集团行为”“洗钱行为”“腐败行为”等为犯罪，《联合国反腐败公约》第 15—25 条规定“贿赂公职人员”“滥用职权”“资产非法增加”“对犯罪所得的洗钱行为”等为犯罪，可适用于打击暗网中的跨国有组织犯罪、洗钱犯罪、腐败犯罪。在暗网中利用数字货币进行非法交易支付、洗钱、资助恐

① Davis, S. & Arrigo, B. (2021). The Dark Web and Anonymizing Technologies: Legal Pitfalls, Ethical Prospects, and Policy Directions from Radical Criminology. *Crime, Law and Social Change*, 76(4), 370.

② Miloshevska, T. (2019). Dark Web as a Contemporary Challenge to Cyber Security. Criminal Justice Issues Journal of Criminal Justice, *Criminology and Security Studies*, 2019(5), 118.

③ Kerr, S.O. & Murphy, S. D. (2017). Government Hacking to Light the Dark Web: What Risks to International Relationsand International Law?, *Stanford Law Review Online*, 70(58), 63.

④ 杨亚飞、王诺亚：《暗网犯罪情报分析研究》，《情报杂志》2023 年第 4 期。

怖组织等较为普遍，公约当然可以适用。

暗网犯罪如恐怖主义、儿童色情、侵犯知识产权等多由个体实施，也可适用现有国际法规范。联合国框架下有多项打击恐怖主义的国际公约，如《制止恐怖主义爆炸事件的国际公约》《制止向恐怖主义提供资助的国际公约》《制止核恐怖主义行为国际公约》等，可适用于打击暗网恐怖主义爆炸犯罪、资助恐怖主义和核恐怖主义等。利用暗网筹集资金、传播恐怖主义和极端主义思想、购买武器弹药等未超出恐怖主义行为的一般范畴，上述公约可适用。联合国《儿童权利公约》第 19 条和《〈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》禁止儿童色情，可适用于打击暗网儿童色情。暗网中的色情信息尤其是儿童色情信息相当丰富，付费观看儿童色情视频本质上属于买卖儿童色情服务产品，公约可以适用。

（二）网络犯罪国际刑事规则发挥重要作用

网络犯罪国际刑事规则包括以欧委会《网络犯罪公约》为代表的区域公约和正在谈判的《联合国打击网络犯罪公约》，可用于打击暗网犯罪。

区域层面，《网络犯罪公约》《阿拉伯打击信息技术犯罪公约》规定了非法访问、滥用设备、儿童色情、侵犯知识产权等 9 类罪名；《西非国家经济共同体打击跨国网络犯罪指令》第 2—3 章规定了与信息及通信技术相关的特定罪行（第 4—23 条）和包含传统犯罪的信息和通信技术罪行（第 24—27 条）；《上海合作组织成员国保障国际信息安全政府间合作协定》第 2 条指出“信息武器的研制和使用”“信息恐怖主义”“信息犯罪”等是国际信息安全领域的主要威胁，并在后续条款中提出了合作的方向、原则、方式和机制等；《独立国家联合体打击计算机信息领域犯罪合作协定》第 3 条规定了“非法访问、恶意使用软件、有访问权限的人越权使用、侵犯知识产权”4 类犯罪。暗网犯罪是在暗网中或借助暗网实施的犯罪，上述规范网络犯罪的公约可适用于打击暗网儿童色情、非法访问、滥用设备、武器贩卖、恐怖主义、侵犯知识产权等犯罪。

全球层面，全球性网络犯罪公约可能有助于解决暗网犯罪国际法规制问题。自 2021 年以来，根据联大第 74/247 号决议成立的特设政府间专家委员会（Ad Hoc Committee）（以下简称“特委会”）已先后举行六届谈判会议，以制定关于打击将信息和通信技术用于犯罪目的的国际公约（即《联合国打击网络犯罪公约》）。其中，2022 年 11 月 7 日，在筹备第四届会议过程中，特委会主席在秘书处的支持下，编纂了《关于打击为犯罪目的使用信通技术的全面国际公约的总则、刑事定罪、程序措施和执法条款的合并谈判文件》（A/AC.291/16），不仅涵盖非法访问、滥用设备、与计算机相关的伪造、在线儿童性虐待等罪行，还包括煽动颠覆或武装活动、与恐怖主义有关的犯罪等。[①] 非法入侵、破坏计算机、网络诈骗和盗窃、雇佣杀人等犯罪在暗网中时有发生[②]，但近年来，儿童性虐待、色情服务等在暗网中高发，毒品交易、武器贩卖、物品销赃、个人信息和数据倒卖、实施恐怖主义等有组织犯罪成为常态[③]。以专门条款规范上述罪行，将在暗网中高发的网络犯罪纳入全球性法律规范体系，有利于全面、有效打击暗网犯罪。

（三）国际软法产生一定的法律效果

国际软法包括国际组织和国际会议的决议等，涉及诸多国际社会普遍关注的刑事犯罪，可为打击暗网犯罪提供借鉴和指引。

以联合国为代表的国际组织通过决议、建议、行动指南等为人类生活的各领域创制规则。联合国曾通过诸多与网络犯罪、恐怖主义相关的决议，虽不具有法律拘束力但产生了法律效果，对打击暗网犯罪有借鉴和指引作用。以联大与恐怖主义相关的决议为例，2006 年联大通过的《联合国全球反恐战略》（A/

① UN. A /AC.291/16, pp. 3-12.

② Kethineni, S., Cao, Y. & Dodge, C. (2018). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *American Journal of Criminal Justice*, 43(2), 134-145.

③ Weimann, G. (2016). Terrorist Migration to the Dark Web. *Perspectives on Terrorism*, 10(3), 123-125.

RES/60/288）强调：“打击可能与恐怖主义有关的犯罪，包括贩毒的所有方面的活动、非法军火贸易、洗钱，及核材料、化学材料、生物材料、放射性材料和其他潜在致命性材料的走私。”[①] 它是联合国会员国首次同意采取共同战略和行动以打击恐怖主义的决议：不仅关注到预防和打击恐怖主义的措施、健全缔约国预防和打击能力等；还强调打击频发于暗网中的罪行，如贩毒、非法军火交易等，对打击暗网犯罪具有指引和借鉴作用。联合国大会每两年审议 1 次该战略，至 2023 年已审议 8 次，将恐怖主义的国际法规制逐步向统一实体法方向推进。其中，2014 年进行的第 4 次审议通过决议（A/RES/68/276），要求各国关注利用信息技术从事的煽动、招募、资助或策划恐怖活动；2023 年进行的第 8 次审议通过决议（A/RES/77/718），促请所有国家努力缔结国际恐怖主义公约。虽然联大决议没有法律拘束力，但其法律影响不容忽视。由于联大决议对恐怖主义犯罪内容的界定、规制路径和方式的判断符合国际法治的基本规律，为国际社会所广泛接受：“特委会”明确将网络恐怖主义写入 A /AC.291/16，且涉及的内容基本与上述决议一致。

三、暗网犯罪国际法规制存在的问题

暗网犯罪国际法规制存在一般性国际刑事规则局限性明显，网络犯罪国际刑事规则的适用不具有普遍性，国际软法不具有法律拘束力等问题。

（一）一般性国际刑事规则局限性明显

一是缺失专门规制暗网犯罪的罪名条款。现有国际刑事规则仅从不同侧面间接、部分、笼统地规制暗网犯罪，未关注到暗网评价机制的特异性及暗网犯罪技术的复杂性，从而影响其作用效果。一方面，暗网中对特定行为的评价机制与传统社会存在显著差异，一般国际刑事规则所具有的规范、指引、教育、评价作用很难落实。在表网上，基于社会对毒品贩卖、儿童色情、恐怖主义和极端主义等行为的消极评价，各国基本将上述涉网犯罪纳入法律范畴进行规范，上述国际刑事规则亦可适用。而在暗网中对上述行为的评价却往往是积极的，在暗网服务提供者、社群管理者等的放任下，用户可充分展示其特殊癖好、犯罪过程和方法等，并能获得其他用户的认同、好评甚至是支持。[②] 在暗网极端自由的环境中，一般国内法规范及传统国际刑事规则常被无视甚至肆意违反，法律对暗网犯罪行为的规范作用被削弱，追究暗网犯罪行为可能耗时数载。如在臭名昭著的查德·郝克尔（Richard Huckle）性侵案中，自 2006—2014 年 Huckle 先后侵犯两百多名马来西亚儿童，并在暗网平台分享了系列作案照片和录像。其间，Huckle 不但未被追责还因拥有丰富的作案“经验”被暗网网站中的恋童癖用户推崇。直至 2014 年，警方在破获暗网恋童论坛时，才发现了 Huckle 的存在，并于 2016 年对他作出判决。[③] 另一方面，匿名通信技术的使用显著降低了犯罪风险和违法成本，一般国际刑事规则对暗网犯罪的规制效能大大降低。匿名通信技术使犯罪分子不易受到追查，即使被追查也有充分的规避机会，承担国际刑事规则否定性评价的可能性极小，降低了犯罪风险；暗网中有特定违法目的的个体集中，犯罪分子能轻易搭建犯罪链条，降低了犯罪成本。在低风险和低成本的暗网中，非法交易数量剧增，传统国际刑事规则很难直接、有效发挥作用。如由于匿名通信技术的使用，且缔约国对数字支付的合法性存在分歧，暗网跨国有组织犯罪、洗钱犯罪、腐败犯罪中怎样认定赃款、如何没收数字货币和没收后如何处置等问题都有待解决，现有《联合国打击跨国有组织犯罪公约》《联合国反腐败公约》难以有效适用。

二是对暗网犯罪的规制存在法律漏洞且滞后性明显。一方面，现有国际刑事规则存在法律漏洞，引发暗网犯罪治理真空。暗网犯罪国际法规制问题突出表现在匿名访问与个人隐私保护间的矛盾上，现有

① UN. A/RES/60/288, pp. 6-7.

② 陈嘉鑫、董紫来：《社会控制理论视域下的暗网犯罪治理研究》，《政法学刊》2023 年第 3 期。

③ UNODC(2020). *Darknet Cybercrime Threats to Southeast Asia*. Retrieved on 27th Aug. 2023 from: https://www.unodc.org/roseap/uploads/documents/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf.

国际刑事规则基本未对此作出明确规定。如暗网的跨国性与匿名性吸引了各国犯罪分子建立平台或在暗网市场上售卖公民个人信息，国际法上除个别区域性数据保护条约（如欧盟《一般数据保护条例》第 10 条“与刑事定罪和犯罪相关的个人数据的处理”）涉及侵犯个人信息罪外，现有国际刑事规则基本未涉及。另一方面，现有国际刑事规则滞后性明显，很难规制相关暗网犯罪。现有国际刑事规则虽规制儿童色情、毒品贩卖等罪行，但仅涉及这些罪行的基础内容，很难有效规制具有特殊性的暗网犯罪。如《联合国禁止非法贩运麻醉药品和精神药物公约》可用于打击暗网涉毒犯罪，但在暗网环境下毒品犯罪行为已异化，交易场所和交接方式的变化，使交易时间（买家支付的时间还是到货的时间）、地点（买家所在服务器地还是卖家服务器所在地）等节点不易判断，从而给刑事司法认定带来困难，公约恐难有效适用。《儿童权利公约》第 19 条规定保护儿童不受“身心摧残、伤害或凌辱，忽视或照料不周，虐待或剥削，包括性侵犯”，强调的是直接施害的行为，而暗网儿童色情犯罪则更偏重通过传播儿童色情资源、性剥削视频获利，现有国际刑事规则无法有效适用。如在韩国的“N 号房间”事件中，案犯在暗网社交软件 Telegram 上开设聊天室，散布 3762 份性剥削视频以谋取利益。事件中，案犯因销售和传播了海量的性剥削视频被韩国警方逮捕，购买并制作非法性剥削视频的多人被逮捕或被立案。但依据现有国际和国内法，非法传播性剥削视频的则基本未受实质处罚。为此，韩国在事件发生后半年，修订了本国法律——从 2020 年 6 月 2 日起，《儿童与青少年性保护法》中的“儿童和青少年淫秽视频”改为“儿童和青少年性剥削视频”以有效规范非法传播性剥削视频的行为。

（二）网络犯罪国际刑事规则不具有普遍适用性

一是已生效区域性网络犯罪公约局限性显著。首先是缺乏普遍性和代表性。上述公约未能摆脱一般区域性公约的局限性——由于缔约方多局限于相关组织的成员国，它们的参与主体明显缺乏普遍性和代表性，开放性也略显不足。虽然个别区域性公约（如《网络犯罪公约》）确实具有不小的影响力，但它们均未能获得全球大多国家的签署、批准或加入。截至 2023 年 7 月 25 日，共 68 个国家签署、批准或加入《网络犯罪公约》。[①] 其次是适用效力欠佳。上述公约往往仅确立了基础性标准，公约的适用缺少必要的保障：公约如何实施，未履行公约义务的法律责任等均未涉及。部分公约规定了相当多的保留条款，赋予缔约方的自由裁量权较大。保留条款本身不是问题，但过多的保留条款减损了公约的效力。最后是存在立法空白。上述公约往往制定时间较早（如《网络犯罪公约》是 2001 年 11 月 8 日通过并于 2004 年 7 月 1 日生效），设置的罪名条款仅针对当时历史条件间亟需规制的犯罪，如非法入侵、滥用计算机设备、网络诈骗、网络盗窃等基础罪名，甚至近年来备受关注的网络恐怖主义都未列入罪名条款。暗网虽然由来已久，但暗网犯罪是近年才开始备受关注的，上述公约并未着力于解决暗网犯罪问题，规则的缺失显然不利于有效规制暗网犯罪。

二是正在拟定的全球性公约前景不明。《联合国打击网络犯罪公约》的制定可能有助于解决暗网犯罪国际法规制问题，然而，公约谈判走向不明，最终文本尚未确定，短期内无法实际发挥作用。“特委会”第五届会后编纂的公约草案与 A /AC.291/16 相去甚远，删除了诸多暗网上频发的罪名：侵犯著作权、网上跟踪儿童、未成年人参与实施非法行为、鼓励或胁迫自杀、煽动颠覆活动或武装活动、与极端主义有关的犯罪、与恐怖主义有关的犯罪、与分销麻醉药品和精神药物有关的犯罪、与贩运武器有关的犯罪、非法分销假冒药品和医疗产品等。删除上述条款可能会严重影响打击暗网国际合作的效能：它们大多是在暗网中高发的犯罪，删除后将使缔约国在规制上述犯罪时无法直接适用上述条款，反而需参照其他条款规制具有特殊性的暗网犯罪，这就容易引起缔约国间法律适用的争端。打击暗网犯罪国际合作不仅涉及定罪、量刑，还涉及跨国刑事司法协助、引渡和陪判刑人员移交等问题，若就基础罪名设置存在分歧，

① COE (2023). *Chart of Signatures and Ratifications of Treaty 185*. Retrieved on 25th July. 2023 from: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

势必影响量刑及后续程序事项，从而导致国际合作无法落到实处。[①] 总之，这些条款不仅要在全球性公约中予以规定，还应结合暗网犯罪的特殊性作出必要补充。若公约草案得以通过，因缺失上述条款其对暗网犯罪的规制无疑将是相当弱的。

（三）国际软法不具有法律拘束力

一是国际软法不具有强制性。虽然国际软法符合稳定国际秩序、规范跨国交往和国际合作等的需求，对国际法治具有示范作用；但其缺乏强制性、缺失责任和制裁机制，主要依靠相关行为体自愿履行。联大决议具有促进确立国际法规范的作用，但缺乏强制性——《联合国宪章》第 10 条至第 14 条规定联大决议具有建议性质，且未要求会员国遵守和履行。[②] 实践中，诸多会员国实施了与联大决议相关的行为，如中国将网络恐怖主义纳入《网络安全法》规制范畴（第 12 条），但并不构成对决议法律拘束力的默示肯定，只能证明联大决议产生了法律效果。

二是国际软法的法律效果不具确定性。“国际软法能够辅助国际决策者确立国际法的实质规范，成为日后拟定和谈判条约的基础。”[③] 但国际软法的实效受制于国际社会的需求，需求越迫切越有利于软法的适用和遵行，反之亦然。且国际软法的法律效果是动态弹性的，初始可能毫无拘束力，但随着行为体的关注和重视，可能实现类似硬法的效力。[④] 但从无拘束力至硬法应然效力的过程不具确定性，可能在较短时间内实现，也可能需要数载。联合国相关恐怖主义的决议虽已是海量，但国际社会并未形成一致的认知和需求，相关决议能否实现从软法向硬法的过渡仍具有不确定性。以《网络犯罪公约》缔约国为代表的国家和以中俄为代表的国家对网络恐怖主义国际法治的认知存在显著差异，前者认为没必要设置专门条款规制网络恐怖主义，后者则认为应设置专门条款。由此，国际软法短时间内恐怕很难产生实质法律效果。

四、暗网犯罪国际法规制的进路

除上述法律问题外，暗网犯罪国际法规制还存在一系列技术障碍。突出表现为各国治理技术存在显著差异，对合作打击暗网犯罪产生消极影响。以美国为代表的国家拥有先进的网络技术，而广大发展中国家技术水平相对落后。美国 FBI 早在 2002 年就开发了“网络调查技术”（ NIT: Network Investigative Technique）以调查非法入侵计算机系统、儿童色情、敲诈、恐怖主义及追踪 Tor 黑客。美国还不断更新和改进以适应现实需求：国防部高级研究项目局（DARPA) 2014 年启动并于 2015 年 4 月 17 日公开发布 Memex 研究项目，以提升执法部门的暗网搜索能力。而中国等发展中国家暗网犯罪治理技术和手段有限，相关部门和企业网络安全研究机构加强了对暗网的监控，设置了暗网数据实时监测与智能分析系统等，但并未取得实质性突破。[⑤] 公安机关侦破的案件大都是通过表网侦查发现罪犯，再根据供述调查取证。[⑥] 技术水平差异大的国家间很难有效合作，实践中的多次跨国执法合作主要发生在技术水平相当的发达国家之间就是例证。另外，暗网犯罪分子与执法部门的技术攻防战继续不断，不同研发主体对技术治理的需求差异大，也对暗网犯罪治理造成阻碍。[⑦] 因此，暗网犯罪治理应坚持技术与法治相结合的原则，并在此基础上完善顶层设计方案、强化国际执法合作。

（一）确立技术与法治相结合的原则

一是以法律规范和保障技术发展。国际社会应以法律规范暗网技术的使用、保障和促进暗网技术的

① 江溯：《打击网络犯罪的国际法新机制》，《法学》2022 年第 11 期。
② 蒋圣力：《联合国大会决议法律效力问题重探——以外层空间国际法治实践为例》，《国际法研究》2020 年第 5 期。
③ 何志鹏：《逆全球化潮流与国际软法的趋势》，《武汉大学学报（哲学社会科学版）》2017 年第 4 期。
④ 何志鹏、申天娇：《国际软法在全球治理中的效力探究》，《学术月刊》2021 年第 1 期。
⑤ 谢玲：《暗网犯罪刑事治理研究》，《学术论坛》2020 年第 5 期。
⑥ 王枫梧：《我国暗网犯罪现状、治理困境及应对策略》，《中国人民公安大学学报（社会科学版）》2020 年第 1 期。
⑦ 罗俊：《滋蔓的暗网及网络空间治理新挑战》，《学术论坛》2020 年第 5 期。

研发。一方面，在国际技术法律规范中强调应加强对匿名通信系统和技术的监管。各国可通过监控暗网网站的入口和链接、分析暗网内容数据等，掌握匿名通信系统和技术的使用人数、交易规模和趋势等，以有效预防和打击暗网犯罪。另一方面，在网络犯罪立法中强调强化各国技术合作，保障和促进去匿名化技术的研发。各国可基于匿名通信系统提供服务的原理和匿名路由协议，合作研发流量识别、节点发现、内容分析、定位追踪等技术，设计出有针对性的暗网服务定位方法，以快速有效地发现、定位和治理非法暗网服务。如各国执法机关可合作研发：网络侦查和安全漏洞检测技术，以分析暗网用户网络行为、追踪暗网流量和确认通信关系等；蜜罐技术、端口扫描和指纹识别技术、应用程序级侦察技术和瞬时漏洞捕捉技术等，通过远程访问计算机系统发现暗网用户异常行为、暗网浏览器漏洞，追踪暗网犯罪信息；自动采集暗网站点信息的爬虫技术，以对暗网重点社区进行技术布控和人员分析。

二是以技术拓展法律的规制范式。用技术促进立法的专门化、民主化、科学化，提升执法和司法运作的合理性、客观性和效率，技术进步往往伴随着法律规范的创制和法律部门的诞生。各国应积极促进公共部门与私营机构合作发掘漏洞、深化技术合作，不断研发去匿名化和识别隐藏服务的技术，以发现需要法律规制的暗网非法行为和服务内容，为拓展法律的规制范式奠定技术基础。一方面，赋予网络服务商新义务，拓展法律监管的内容。暗网犯罪的特殊性导致仅针对行为和主体本身很难有效打击之，应赋予网络服务商发掘匿名通信系统的漏洞、安插监管后门等义务，以发现新的暗网非法行为和服务内容。Tor、I2P 等存在的漏洞为发现匿名通信系统提供可能性，如转发协议或代码本身存在的漏洞可能使部分标识未被彻底清除；而网络服务商在发现协议和代码漏洞上具有天然的优势，立法可明确要求网络服务商承担发现和识别漏洞的法律义务。匿名通信系统中有大量分布式的节点，执法人员可通过留有后门的中继节点加入。立法可要求网络服务商提前安插留有后门的中继节点，以截获非法数据包、发现暗网犯罪信息，为执法机关提供便利。另一方面，以技术反制技术，将传统法律规制范式拓展至技术治理范畴。实时定位匿名通信系统、发现隐藏服务，需不断研发可识别特定标识的去匿名化技术。本质上，研发新去匿名技术以定位和识别匿名通信系统是以技术“反制技术”。传统法律规制范式以主体和行为中心，暗网犯罪却更强调匿名技术的发现和挖掘，这不仅要对传统刑事规则和网络刑事规则扩张解释，还要以新角度认识和发展该领域的法律规则。事实上，在暗网犯罪治理中，技术治理的有效性更高。“区块链技术比法律在规范个人行为和交易时更为有效，区块链代码技术开辟了一种前所未有的崭新的规制范式。”①

（二）推进暗网犯罪国际法规制的立法进程

解决暗网犯罪问题，除强有力的技术支撑外，更要加强顶层法律设计。暗网犯罪是全球性问题，建立各国协同打击暗网犯罪的法律机制势在必行。②

国际法层面，应推进将暗网犯罪国际法规制纳入国际立法进程。一方面，推动国际软法讨论进程中，纳入暗网犯罪议题。虽然国际软法不具法律拘束力，但对未来国际立法具有指引和示范作用，暗网犯罪国际法规制可以软法先行，以为硬法的达成“投石问路”。联合国大会对国际事务的关注是全方位的，中国可推动其设立暗网犯罪国际法治议题：呼吁多元主体参与，就暗网犯罪的技术、法律和国际合作等问题进行充分讨论；在了解各方诉求基础上，有针对性地提出监管责任划分标准、管辖权行使条件、电子证据取证和采纳依据等规则方案。另一方面，推动网络犯罪国际立法进程中，写入暗网犯罪条款。《联合国打击网络犯罪公约》已形成草案，但草案删除了 A/AC.291/16 中涉及的诸多在暗网中频发的罪名条款，不利于暗网犯罪的国际法规制。不过，考虑到缔约国对网络犯罪定罪条款的理念差异（有国家主张扩大定罪范围，也有国家反对过度定罪），中国可推动在后续谈判中增加规定“暗网犯罪”条款，但仅先作粗略的规定：“缔约国应采取必要的立法和其他措施：1. 打击通过暗网实施的犯罪；2. 最大限度地鼓励非国家行为体参与打击暗网犯罪国际合作。”

① 刘蓓：《智能社会中技术治理与法律治理关系论纲》，《上海师范大学学报（哲学社会科学版）》2022 年第 2 期。

② 焦康武：《总体国家安全观视域下我国暗网犯罪应对研究》，《犯罪研究》2017 年第 6 期。

国内法层面，应推动暗网犯罪法律规制的具体化，以为其国际法治奠定基础。暗网犯罪国际法规制尚处于初级阶段，短时间内很难在国际法层面形成具体规则，国内法先行有助于推进暗网犯罪国际立法进程。多数国家都通过刑法、网络安全法等对暗网犯罪涉及的罪名作出规定，但还应进一步细化。一方面，强化对暗网加密服务的监管。贩卖枪支、毒品等的暗网网站颇受恐怖分子和瘾君子喜爱，但很难通过瞬息万变的信息对利用暗网非法购买枪支、毒品的行为进行监管。各国可借鉴美国、德国等暗网治理经验，明确规定加密服务商应建立留档备案制度，以为侦破暗网犯罪提供有力制度保障。另一方面，加强对数字货币支付的监管。对暗网犯罪的监管应正确认识数字货币的滥用问题，加快监管立法进程。美国、俄罗斯等国采取了一系列监管数字货币的措施，提高了暗网犯罪的监管效能，各国可借鉴之。如可借鉴美国 2017 年《统一虚拟货币经营监管法》（Uniform Regulation of Virtual Currency Business Act），要求从业者真实保留、提供完整的财务、交易和客户信息，并对无证经营、违法从事虚拟货币业务活动等规定处罚措施和刑事程序。

（三）强化打击暗网犯罪国际执法合作

暗网犯罪国际治理并非毫无进展，各国及国际社会通过各种路径参与暗网犯罪国际治理。一是国家层面。美英等发达国家通过设立专门机构、组织协调相关部门联合打击暗网犯罪等系列措施，参与暗网犯罪国际治理。如 2023 年初，由美国 FBI 和德国、荷兰执法部门领导，加拿大、法国、瑞典等国参与的国际联合行动，关闭了被用来攻击和勒索全球各地企业、涉案金额高达 1 亿美元的蜂巢链（HIVE）软件。[①] 二是国际组织层面。国际刑警组织（International Criminal Police Organization，Interpol）、欧洲刑警组织（European Police Office，Europol）等正着力于发现暗网犯罪国际治理问题并提出解决方案。Interpol 成立的暗网和加密货币工作组（Interpol Working Group on Dark Net and Cryptocurrencies）为实现其打击暗网犯罪、规范加密支付的宗旨，已相继举办数次会议。[②] 2018 年 5 月，Europol 宣布成立的暗网小组（Dark Web Team）致力于开发暗网调查工具、战术和技术，识别主要威胁和目标；加强联合调查行动和技术、组织培训和能力建设、预防暗网犯罪和提高认识。[③] 三是多利益攸关方层面。多利益攸关方参与暗网犯罪治理和预防日益常态化，改变了传统模式过度追求监管效能的弊端，提升了治理的科学性。[④] 例如，2016 年，兰德欧洲公司与曼彻斯特大学合作开展了持续监测暗网社区论坛、加密货币市场、收集和分析相关数据的研究项目[⑤]，为政府深入了解暗网非法武器贸易情况、完善相关立法提供了实践基础。虽然上述治理活动为暗网犯罪调查提供了专门知识、开发工具、战术和技术等支持，为共享应对策略、技术和信息提供协调办法，但除国家层面的国际执法合作外，多仅增加了边际效益，并未产生太大实际效用。

国家层面的国际执法合作成效显著，应继续强化，并将发展中国家纳入其中。国际执法合作成效斐然，如 2017 年 7 月，多国执法部门采取联合行动，先后查封暗网中最大的交易平台 AlphaBay Market，第三大交易平台“汉萨市场”（Hansa Market），第四大交易平台“俄罗斯匿名市场”（Russian Anonymous Marketplace）。同年 8 月，全球第二大暗网交易平台“梦幻市场”（Dream Market）供应商盖尔 • 瓦莱里

① Europol (2022). *Cybercriminals Stung as HIVE Infrastructure Shut Down*. Retrieved on 14th July. 2023 from https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down.

② Interpol (2018). *INTERPOL Holds First Dark Net and Cryptocurrencies Working Group*. Retrieved on 5th July. 2023 from: https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2018/INTERPOL-holds-first-DarkNet-and-Cryptocurrencies-Working-Group.

③ Europol(2018). *Crime on the dark web: law enforcement coordination is the only cure*. Retrieved on 10th July. 2023 from: https://www.europol.europa.eu/media-press/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure#:~:text=Crime%20on%20the%20dark%20web%3A%20law%20enforcement%20coordination,approach%20to%20-0tackling%20crime%20on%20the%20dark%20web.

④ 江溯：《论网络犯罪治理的公私合作模式》，《政治与法律》2020 年第 8 期。

⑤ Rand (2016). *International Arms Trade on the Dark Web*. Retrieved on 7th July. 2023 from: https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html.

乌斯（Gal Vallerius）被捕，随后经营者宣布网站下线。各国对暗网犯罪的治理需求存在差异，实体国际法规范短期内难以达成，未来暗网犯罪国际法规制道阻且长，应充分发挥国际执法合作的作用。然而，国际执法合作多发生在国际组织和欧美发达国家间，它们很少和发展中国家间进行打击暗网犯罪执法合作。暗网犯罪的实施没有地域限制，但因法律机制不完善、执法效能差和技术水平弱等，发展中国家暗网人口贩卖、器官贩卖、毒品贩卖等更猖獗，对国际执法合作的需求更强烈，继续加强国际执法合作尤其是发达国家和发展中国家间的合作确有必要。上述国际执法合作多由 Interpol 或 Europol 牵头或支持，发展中国家可积极参与两组织的相关会议，提交本国暗网犯罪情况报告，充分讨论并明确本国暗网犯罪治理的问题；并通过参与相关国际执法合作，提升暗网治理能力。

五、结　论

近年来，暗网犯罪日益猖獗，贩卖毒品、非法买卖枪支、贩卖人口、儿童色情、绑架、暗杀、极端主义、恐怖活动等泛滥，暗网犯罪成为国际社会共同关注的重要问题。然而，暗网犯罪国际法规制存在诸多法律问题：主要依托其他领域的国际立法，但一般性国际刑事规则往往具有较强的时代性、滞后性，且没有关注到暗网犯罪的特殊性；网络犯罪国际刑事规则的局限性显著，全球性公约短期内无法实际发挥作用；而国际软法虽确有法律效果，但不具有法律拘束力，很难有效打击暗网犯罪。暗网犯罪国际法规制需确立技术与法治相结合的原则，完善暗网犯罪国际治理的顶层设计，强化打击暗网犯罪国际执法合作。

暗网犯罪是通过或借助暗网实施的犯罪，中国作为新兴网络国家，在网络犯罪国际法治中发挥了重要作用，需提前对暗网犯罪的国际法规制进行布局。虽然中国已出台《网络安全法》等系列法律，并结合《刑法》相应条款对包括暗网在内的秘密信息传输途径进行源头控制；但相关理论研究刚起步，执法部门对暗网的监控和治理能力尚待提高。可从以下几方面进行努力：首先，完善国内立法。强化互联网企业和执法机关合作，对暗网犯罪进行信息源头治理；强化执法机关和金融机构的合作，对暗网支付工具进行金融风险治理。其次，推进国际立法进程。推动联合国框架下全球性网络犯罪公约立法，将暗网犯罪的国际法规制纳入国际法治进程。最后，加强暗网犯罪执法合作与情报交流，深入挖掘、发现和治理暗网犯罪。

Issues and Approaches of International Law Regulation of Darknet Cybercrime

LI Yan

(School of Law, Henan University of Economics and Law, Zhengzhou, 450046)

Abstract: The anonymity, encryption and transnational nature of the dark net make darknet cybercrime more specific than ordinary cybercrime. The limitation of general international criminal rules and international criminal rules for cybercrime, as well as the lack of binding force of international soft law, affects the effectiveness of international law regulation of darknet cybercrime. To solve the problem of international law regulation of darknet cybercrime, higher requirements are put forward for technology governance, top-level design and law enforcement cooperation. The principle of combining technology and rule of law should be established, the law should promote and safeguard the development of technology, and the regulation paradigm of law should be expanded by technology. It is necessary to construct and improve the top-level design of international governance of darknet cybercrime, promote the addition of "darknet cybercrime" provisions in the international criminal rules of cybercrime and the elaboration of domestic regulations on darknet cybercrime. It is also important to continually strengthen international law enforcement cooperation against darknet cybercrime, and ensure the inclusion of developing countries.

Keywords: Darknet Cybercrime, Anonymity, Encryption, United Nations Convention against Cybercrime

[责任编辑：陈慧妮]