法学与社会治理学刊
2026 Vol. 1, No.1，ISSN 3154-746X

跨境网络犯罪的司法管辖权竞合
——基于暗网交易平台的实证考察

刘新建

上海财经大学

通讯作者*：刘新建　E-mail：834956739@qq.com

论文信息

关键字
跨境网络犯罪；司法管辖权；暗网交易平台；管辖权竞合；刑事司法协助；《联合国打击网络犯罪公约》

摘要

暗网交易平台依托 Tor 网络匿名通信技术与加密货币支付体系，已成为全球跨境网络犯罪的核心场域。这类犯罪因犯罪行为实施地、结果发生地、服务器所在地、犯罪嫌疑人国籍国等多个管辖连接点分散于不同法域，引发严重的司法管辖权竞合问题，导致侦查取证受阻、引渡困难、资产追缴不畅等多重执法困境。本文以丝绸之路（Silk Road）、阿尔法湾（AlphaBay）、华尔街市场（Wall Street Market）等典型暗网交易平台案件为实证样本，系统分析管辖权竞合的表现形态与深层根源，揭示现行刑事司法协助机制（尤其是司法互助条约）的局限性。研究发现，管辖权竞合的本质是网络空间的无边界性与国家主权疆界之间的根本性冲突。《联合国打击网络犯罪公约》于 2024 年 12 月获得通过，为全球网络犯罪治理提供了首个具有法律约束力的多边框架，标志着治理格局的重要转折。本文据此提出以“犯罪结果发生地为主导”的管辖权协调原则、探索“数据存储地+数据获取地”双重同意机制、构建多边快速响应协作机制等制度改进方案，并主张以区块链存证与智能合约技术赋能跨境证据交换，为完善跨境网络犯罪治理体系提供理论参考。

Jurisdictional concurrence in cross-border cybercrime -- Empirical Investigation Based on Dark Web Trading Platforms

ARTICLE INFO

Keywords
Cross-border cybercrime Jurisdiction Dark web trading platform

Abstract

Dark web trading platforms, relying on Tor network anonymous communication technology and cryptocurrency payment systems, have become the core field of global cross-border cybercrime. This type of crime, due to the fact that multiple jurisdictional connection points such as the place where the criminal act was committed, the place where the result occurred, the location of the server, and the country of nationality of the criminal suspect are scattered across different jurisdictions, has triggered serious jurisdictional competition issues, leading

Citation：Liu, X. J. (2026). 跨境网络犯罪的司法管辖权竞合——基于暗网交易平台的实证考察 [Jurisdictional concurrence in cross-border cybercrime -- Empirical Investigation Based on Dark Web Trading Platforms]. *法学与社会治理学刊*, 1(1), 25–33.

https://doi.org/10.64744/law.2026.195.

Jurisdictional concurrence; Criminal judicial assistance "United Nations Convention Against Cybercrime"

to multiple law enforcement dilemmas such as obstructed investigation and evidence collection, difficulties in extradition, and poor recovery of assets. This article takes typical cases of dark web trading platforms such as Silk Road, AlphaBay, and Wall Street Market as empirical samples to systematically analyze the manifestations and deep roots of jurisdictional competition and cooperation. Reveal the limitations of the current criminal judicial assistance mechanism (especially the mutual judicial assistance treaty). Research findings reveal that the essence of jurisdictional competition and cooperation lies in the fundamental conflict between the borderlessness of cyberspace and the territorial boundaries of national sovereignty. The United Nations Convention against Cybercrime was adopted in December 2024, providing the first legally binding multilateral framework for global cybercrime governance and marking a significant turning point in the governance landscape. Based on this, this paper proposes a principle of jurisdiction coordination dominated by the location where the criminal result occurs, explores a dual consent mechanism of "data storage location + data acquisition location", and builds a multilateral rapid response collaboration mechanism and other institutional improvement plans. It also advocates empowering cross-border evidence exchange with blockchain evidence storage and smart contract technology, providing theoretical references for improving the governance system of cross-border cyber crimes.

一、引言

（一）暗网交易平台的兴起与跨境网络犯罪的严峻态势

暗网（Dark Web）作为互联网深层架构中需借助特定匿名工具（如 Tor 网络）方可访问的隐蔽空间，自其诞生之日起便因其匿名性和去中心化特征成为各类非法活动的技术温床。当 Tor 网络的匿名通信技术与比特币等加密货币的匿名支付功能相结合时，毒品交易、洗钱、黑客工具交易、武器买卖、人口贩运、个人信息倒卖等传统犯罪获得了前所未有的“数字庇护所”。丝绸之路（Silk Road）作为首个大规模暗网交易市场，于 2013 年被美国联邦调查局查封；其后继者阿尔法湾（AlphaBay）于 2014 年崛起并于 2017 年被多国联合执法行动摧毁；华尔街市场（Wall Street Market）的覆灭则进一步印证了暗网交易平台迭代演化的规律。

暗网犯罪的全球蔓延态势令人忧虑。国际调查记者联盟（ICIJ）于 2025 年发布的“Coin Laundry”系列调查报告显示，非法资金通过主要加密货币交易所进行洗钱活动，被追踪的加密货币资金与全球犯罪集团广泛关联，涉及朝鲜黑客组织、中俄犯罪团伙的人口贩卖活动、芬太尼等毒品交易以及墨西哥贩毒集团的运作。在中国与东盟跨境犯罪治理实践中，类似情形亦不容忽视：在重庆检察机关办理的董某澜跨境贩毒案中，嫌疑人通过暗网获取交易信息、以虚拟货币完成毒资支付，境外交易平台数据分散于缅甸等东盟国家服务器，境内仅能固定快递收货记录等间接证据，传统取证规则难以适用。

（二）问题提出：多连接点导致的管辖权竞合

暗网交易的典型流程涉及多个法域：犯罪嫌疑人可能在一国策划、通过暗网平台（服务器位于第三国）发布交易信息、以加密货币完成支付、货物从第四国寄出、最终在第五国被收货。这一链条使犯罪行为实施地、犯罪结果发生地、服务器所在地、犯罪嫌疑人国籍国等多个管辖连接点分散于不同国家，各国有权依据属地管辖（行为地或结果地）、属人管辖、

保护性管辖乃至普遍管辖原则主张刑事司法管辖权，从而产生管辖权的积极竞合。

管辖权的重叠直接引发执法困境：数据跨境侦查取证与一国国家主权密切相关，根据国际法一般原理，除获得本国同意外，任何其他国家不得直接通过单边措施获取他国境内数据。电子数据的弱地域性与司法管辖的强地域性之间的冲突，导致暗网犯罪案件侦查普遍面临电子证据溯源难、取证难、认证难等问题。暗网犯罪因跨国性、技术迭代与法律冲突特性，挑战传统管辖权并引发执法合法性争议。

（三）研究方法与结构安排

本文采用典型案例实证考察与比较法分析相结合的研究方法。实证层面选取丝绸之路、阿尔法湾、华尔街市场三个最具代表性的暗网交易平台案件，分析其中涉及的管辖权争议类型及执法实践的应对方案；比较法层面梳理《网络犯罪公约》（布达佩斯公约）、《联合国打击网络犯罪公约》等国际法律文件的管辖权规则及协调机制。全文结构安排如下：第二部分阐述暗网交易平台的运作模式与主要犯罪类型；第三部分系统分析管辖权竞合的表现形态与深层根源；第四部分评估现行刑事司法协助机制的局限性；第五部分提出管辖权协调原则与制度改进方案；第六部分总结全文并提出政策建议。

二、暗网交易平台的运作模式与犯罪类型

（一）暗网的技术基础

暗网的运作依托于多层加密的匿名通信架构。Tor（The Onion Routing，洋葱路由）网络通过分布式节点（入口节点、中继节点和出口节点）实现通信双方的匿名化保护，节点密钥由全球志愿者定期更新，显著增加了追踪难度。暗网站点通常使用.onion 或.i2p 等特定域名后缀，无法通过常规搜索引擎或浏览器直接访问。

加密货币则构成了暗网交易的支付基础。比特币等加密货币的去中心化特征和无需银行账户的特点，使其特别受犯罪分子青睐。近年来，犯罪团伙更借助区块链钱包、混币器、跨链转移等工具实现资金流向混淆与身份关联切断，使传统电子取证技术面临失效风险。技术性反侦查策略的持续升级，进一步加剧了跨境追查的难度。

（二）主要犯罪类型

暗网交易平台支持的犯罪类型极为多元。毒品交易始终是暗网市场上规模最大的非法商品类别。在曼哈顿地区检察官办公室于 2025 年披露的“FireBunnyUSA”暗网毒品贩运案中，该网络在美国 50 个州运送了超过 10,000 个包含可卡因、MDMA 和氯胺酮的包裹，并通过加密货币洗钱数百万美元。

黑客工具与网络攻击服务交易是暗网平台的另一重要犯罪类型。研究显示，黑客服务在 Tor 暗网市场中占据主导地位，相关服务数量达 57,233 项。此外，个人信息倒卖、武器交易、洗钱等犯罪活动亦在暗网平台上形成完整的黑市产业链。

（三）典型平台案例

丝绸之路（Silk Road，2011—2013 年）是暗网交易平台的鼻祖，主要交易毒品等违禁品，由罗斯·乌布利希（Ross Ulbricht）运营，2013 年被 FBI 查封。2025 年，乌布利希获得减刑后，其钱包收到一笔约 300 枚比特币（价值约 3100 万美元）的匿名捐赠，区块链分析公司 Chainalysis 怀疑这些资金来源于阿尔法湾早期供应商，揭示了暗网市场之间资金流转的复杂网络。

阿尔法湾（AlphaBay，2014—2017 年）作为丝绸之路的“继任者”，大幅扩展了非法交易的范围和规模，不仅涵盖毒品，更将数字商品、伪造物品乃至黑客服务纳入交易范畴。其查封行动由美国、加拿大、泰国等多国执法机构联合开展，集中体现了多国管辖主张的重叠与协作的必要性。

华尔街市场（Wall Street Market）则是德国主导查封的典型案例，其服务器位于德国但用户遍布全球，进一步印证了暗网交易的跨境本质。

（四）暗网犯罪的特征

综合分析上述案例，暗网交易平台所涉犯罪呈现出三个核心特征。跨境性表现为犯罪行为链条的多个环节分布于不同法域，单一国家的执法力量难以独立完成全链条打击。匿名性来自 Tor 网络的通信隐匿与加密货币的身份隐匿，二者叠加使犯罪主体的身份识别成为执法实践中的最大障碍。证据易灭失性则体现为暗网交易数据的瞬时性、可删除性和加密性，平台运营者常在执法行动前销毁服务器数据，用户可通过加密通信工具的自动删除功能消除交易痕迹，传统取证手段难以及时固定证据。

三、司法管辖权竞合的表现与根源

（一）连接点的多元化

传统国际刑法中的管辖权原则主要包括属地管辖（犯罪行为地或犯罪结果发生地）、属人管辖（犯罪嫌疑人国籍国）、保护性管辖（受害国）和普遍管辖（国际公认的严重犯罪）。在暗网交易平台案件中，上述连接点被高度分散于不同法域，形成多元化的管辖主张基础。

属地管辖原则的适用最具争议。暗网交易的“行为地”至少包括：犯罪嫌疑人的计算机操作地、暗网服务器的物理所在地、加密货币支付指令的发送地与接收地、违禁品货物的发

货地与收货地。同一宗暗网交易可能使上述所有地点分别成为主张管辖权的依据，各国有权依据其国内法中的属地管辖条款对案件整体或部分主张管辖权。

（二）国家间管辖主张的重叠案例

丝绸之路案件是管辖权竞合的典型样本。美国以服务器位于美国境内、交易使用美国邮政系统为由主张属地管辖；冰岛因部分服务器节点位于冰岛境内亦主张管辖权；德国则因部分加密货币交易涉及德国境内的银行账户而主张管辖连接点。多国对同一暗网平台及相关犯罪活动同时提出管辖主张，导致侦查合作中的主导权争议、证据共享范围受限、引渡请求冲突等问题。

在数据跨境取证层面，跨境网络犯罪因涉及不同国家的法律体系，治理困难重重。管辖权的积极冲突与消极真空同时存在：当多国均主张管辖权时形成积极冲突，导致执法程序的重叠与摩擦；当各国均以“缺乏充分连接点”为由拒绝管辖时，则形成管辖真空，使暗网犯罪得以利用制度缝隙逃避法律制裁。

（三）根源分析：网络空间的无边界性与国家主权疆界的根本冲突

管辖权竞合的深层根源在于网络空间的技术逻辑与国家主权的制度逻辑之间的根本张力。从数据自然属性看，数据依托网络产生，以互联网为载体，具有跨地域的天然属性。然而，数据跨境侦查取证与一国国家主权密切相关，一国对本国数据具有排他性支配权。这种电子数据的“弱地域性”与司法管辖的“强地域性”之间的冲突，正是管辖权竞合问题的制度本质。

正如美国联邦调查局局长在谈及暗网治理时所言，暗网不属于任何国家的管辖范围，必须超越边界打击其毒品犯罪等非法活动。这一论断揭示了暗网犯罪的治理困境：在技术层面，暗网不受任何地理边界的约束；在法律层面，各主权国家对其领土范围内的行为和数据享有排他性管辖权。管辖权竞合问题并非简单的规则适用争议，而是数字时代国际法体系面对新型犯罪形态时的结构性困境。

四、国际刑事司法协助机制的局限性

（一）传统协助机制的效率低下

刑事司法互助条约（Mutual Legal Assistance Treaty, MLAT）是当前国家间跨境取证的主要制度框架。然而，MLAT 机制在实际运行中面临严重效率问题。请求过程往往缓慢、官僚化，且可能因不同国家的隐私法律差异而失败。暗网犯罪中电子数据具有易转移性、易灭失性，传统司法协助因效率低下而捉襟见肘。以阿尔法湾案件为例，当多国执法机构同时

获取关键服务器数据时，MLAT 机制的数月乃至数年等待周期与暗网数据可被瞬间销毁的现实形成了尖锐矛盾。

MLAT 框架的价值不在于效率，而在于制度性控制——强制令的签发与执行属于一国法律权威的行使行为。这意味着，追求效率与尊重主权之间存在内在的此消彼长关系。在网络犯罪案件中，侦查时效性往往直接决定证据能否被固定，MLAT 机制的制度逻辑与案件侦查的实际需求之间存在根本性张力。

（二）数据调取与证据采信的跨国分歧

各国对电子证据真实性、合法性、关联性的证明标准存在显著差异，导致证据采信的跨国分歧。一国通过司法协助获取的证据，在另一国法庭上可能因取证程序不符合该国证据规则而被排除。跨境电信网络诈骗犯罪中电子数据是核心证据，但因各国法律数据保护规则差异，数据获取受限于技术壁垒和司法主权障碍，导致电子数据取证“碎片化”。

数据出境监管的差异进一步加剧了这一困境。在数字时代的跨国诉讼中，域外取证与数据出境监管之间的冲突日益明显。数据跨境取证的国际法规范呈现碎片化和单边化态势，可能引发管辖权冲突。

（三）判决承认与执行的缺失

管辖权竞合不仅影响侦查阶段的数据取证，亦延伸至追诉阶段的引渡与资产追缴环节。暗网交易平台的经营者多利用国籍国与犯罪实施国之间缺乏引渡条约的现状规避引渡。丝绸之路创始人乌布利希最终在美国受审，主要得益于其本人最终进入美国境内被抓获，而非依赖引渡程序。对于大多数隐藏于匿名技术背后的暗网犯罪参与者而言，引渡障碍使刑事追诉难以实现。

在资产追缴方面，虚拟货币跨境洗钱已形成全球化的“黑灰产业链”，犯罪分子利用混币器、去中心化交易所等工具，能在瞬间将非法所得在全球范围内转移、隐匿。加密货币的去中心化特性使传统资产冻结与追缴机制难以适用，涉案财产的跨境认定、追缴与处置成为司法实践中的突出难题。

五、管辖权协调原则与制度改进

（一）理论探讨：以“犯罪结果发生地为主导”的协调原则

面对管辖权竞合的治理困境，学界与实务界提出了多种管辖权协调方案。有学者主张应立足《联合国打击网络犯罪公约》，在联合国框架内细化管辖权规则及冲突解决方案，坚守网络主权和合作主义原则，以法益侵害原则作为管辖权行使标准，以利益衡量原则和构

建阶梯性优先次序解决管辖权冲突问题。

在此基础上，本文主张构建以“犯罪结果发生地为主导”的协调原则。暗网犯罪的危害最终落实于受害国境内——无论是毒品流入的终点国、个人信息泄露的受害国，还是洗钱所得资金流入的最终目的地国。以法益侵害的实际发生地作为行使管辖权的核心依据，既能体现保护性管辖的正当性基础，也有助于抑制过度宽泛的属地管辖主张引发的“管辖扩张竞赛”。这一原则需要与利益衡量原则配合使用：当多个国家均可主张“结果发生地”时，应综合考虑案件证据的集中度、受害者的主要分布、侦查成本与效率等因素，确定最具管辖合理性的国家作为主导追诉方。

（二）数据本地化制度的制约与突破

数据本地化制度要求特定类型的数据必须在生成国境内存储，不得跨境转移。这一制度与跨境取证需求形成了直接冲突。电子数据的弱地域性与司法管辖的强地域性在数据跨境问题上产生冲突，导致案件侦查存在电子证据溯源难、取证难等问题。然而，数据本地化制度本身也具有保护数据主权、维护国家安全的正当性。

本文主张探索“数据存储地+数据获取地”双重同意机制作为调和方案。在此框架下，数据存储地国家保留对本地数据的最终控制权，数据获取地国家在获得存储地国家明确同意后，可直接向境内网络服务提供者调取数据。这一机制的核心在于将跨境取证的同意程序前置化和制度化，避免针对每次取证请求逐案谈判的低效模式。从国际立法趋势看，《联合国打击网络犯罪公约》已在多边合作框架下通过数据分级和侦查措施分级等方式建立了数据跨境取证协作的程序框架。

（三）构建多边快速响应机制

《联合国打击网络犯罪公约》于 2024 年 12 月 24 日在第七十九届联合国大会上由全体会员国以协商一致方式正式通过，标志着全球打击网络犯罪的崭新征程正式开启。《公约》的六轮谈判始终关注人权保障、管辖权协调等暗网治理核心问题，多轮会议都强调应将打击暗网滥用行为纳入《公约》范围。《公约》通过统一立法标准、构建跨国协作与证据共享机制消减管辖权壁垒，提升制裁效能，并依托“两国共认犯罪”原则确保跨境追责。

在《公约》框架下，本文主张从以下三个层面推进制度改进。一是完善区域性司法协助协议。 以中国—东盟跨境犯罪治理为例，2024 年云南检察机关依法起诉了电信网络诈骗及关联犯罪、跨境犯罪 8500 多件 1 万余人，近年来重庆法院受理的涉外、涉东盟跨境犯罪案件年均增长 15%以上。在这一区域背景下，升级《网络犯罪公约》的适用机制，推动签署电

子证据快速调取协议尤为迫切。

二是建立证据互认协议与联合调查组常态化机制。 证据互认协议可事先约定各签署国在电子证据真实性、合法性审查方面的统一标准，减少逐案审查的制度成本。联合调查组的常态化运作则能突破信息壁垒，实现多国执法资源的整合与情报共享。在阿尔法湾案件中，多国联合行动的成功经验为联合调查组机制的推广提供了实证基础。

三是强化《公约》框架下的公私合作。 《公约》通过构建公私合作机制和国际协作框架，明确了服务提供者在数据保全、共享、实时通信监控和技术支持中的核心角色。实践中，中国与“一带一路”沿线国家的国际司法协助已实现从机制构建到实战突破的转变，分别与东盟、柬埔寨、泰国、缅甸等多个国家签署司法协助协定。未来应进一步细化服务提供者的协助义务，平衡隐私保护与执法需求之间的冲突。

（四）技术赋能：区块链存证与智能合约辅助的跨境证据交换

技术手段的运用可以在制度改进之外为管辖权协调提供新的路径。区块链存证技术利用分布式账本的不可篡改性和时间戳功能，为跨境电子证据的真实性验证提供了技术解决方案。当多国执法机构共同参与暗网犯罪调查时，区块链存证平台可作为各方上传证据、验证数据完整性的可信基础设施。

智能合约则可辅助跨境证据交换的流程管理。通过将司法协助的程序规则编码为智能合约，可实现证据请求的自动化分发、接收确认的实时反馈、数据访问权限的条件控制等功能，从而提升跨境协作的效率和透明度。跨境犯罪依托数字技术持续升级工具手段，执法机构亦需以技术对技术，以数字手段应对数字犯罪。

需要强调的是，技术赋能不能替代制度协调，但可以作为制度协调的有效补充。区块链存证解决了证据真实性的技术信任问题，却无法解决管辖权归属的法律争议；智能合约提升了协作效率，却无法替代国家间在主权让渡问题上达成的政治共识。技术路径与制度路径应当并行推进、互为支撑。

六、结论

跨境网络犯罪的司法管辖权竞合问题是数字时代国际刑法领域最具挑战性的课题之一。暗网交易平台的兴起使这一问题从理论推演转变为司法实践中亟须破解的现实困境。管辖权竞合的本质是网络空间的技术无边界性与国际法体系的国家主权疆界之间的根本冲突。传统属地管辖原则在暗网犯罪的多节点分布面前捉襟见肘，刑事司法互助机制的低效与证据规则的跨国差异进一步加剧了执法困境。

本文认为，管辖权竞合问题的解决需要多层次的协同努力。在国际法层面，《联合国打击网络犯罪公约》的通过为全球网络犯罪治理提供了前所未有的多边制度框架，各国应积极推动《公约》中管辖权规则的细化和完善。在区域协作层面，以中国—东盟为代表的高频协作区域应率先探索证据互认协议与联合调查组常态化机制，为全球多边协调提供区域样本。在技术支撑层面，区块链存证与智能合约等新技术手段应被纳入跨境证据交换的制度工具箱，提升协作效率。

治理跨境网络犯罪需要平衡主权与效率的双重价值。完全的管辖权排他性必然导致打击真空，而无序的管辖权扩张则会引发国际摩擦与执法冲突。唯一的出路在于以《联合国打击网络犯罪公约》为契机，推动管辖权规则的体系性重构——坚守网络主权原则的同时，以利益衡量和阶梯性优先次序化解管辖权冲突，以多边协作和制度创新回应暗网犯罪带来的全球性挑战。

参考文献

[1] 裴炜.《联合国打击网络犯罪公约》框架下的公私合作与中国因应[J].中国刑事法杂志,2025(2).
[2] 张印.跨国网络犯罪刑事管辖困境及冲突解决[J].江苏警官学院学报,2025(2):26-36.
[3] 韩希霖.跨境网络犯罪中电子数据取证的现实困境与调适路径[J].贵州警察学院学报,2025(5).
[4] 姜伟.回应司法实践需求 破解刑事跨境数据取证难题——〈刑事跨境数据取证：边界重构与制度革新〉序[N].检察日报,2025-11-27.
[5] 李莉,钟佩.跨境电信网络诈骗犯罪的检察应对[N].检察日报,2025-07-29.
[6] 暗网犯罪国内外存在的问题与因应[EB/OL].朔州市中级人民法院,2025-07-31.
[7] 跨境犯罪治理需要更完善的司法保障[EB/OL].法治日报,2025-12-22.
[8]
[9] 数据跨境取证的国际法规范整合——以〈联合国打击网络犯罪公约〉为视角[EB/OL].湖北社科专家成果数据库,2025-11-10.
[10] 跨境犯罪中网络服务提供者的责任边界[N].检察日报,2025-07-22.
[11] Chainalysis.丝绸之路创始人收到的300枚比特币或来源于AlphaBay[EB/OL].2025-06-06.
[12] ICIJ.加密行业已成全球犯罪“影子金融系统”[EB/OL].CoinDesk,2025-11-17.
[13] D.A. Bragg Announces Guilty Pleas In Dark Web Cryptocurrency Drug Trafficking Ring That Laundered $7.2 Million[EB/OL].Manhattan District Attorney‘s Office,2025-10-23.
[14] Challenges of Obtaining Encrypted Data in Drone-Related Crime Investigations[EB/OL].2025-08-11.
[15] SoK: cross-border criminal investigations and digital evidence[EB/OL].
[16] 构建虚拟货币犯罪协同治理机制[N].法治日报,2025-05-14.