法学研究 Chinese Journal of Law
Vol.41，No.5（2019）

网络空间中犯罪帮助行为的类型化

——来自司法判决的启发

邓矜婷 *

内容提要：提供侵入、非法控制计算机信息系统的程序、工具罪和帮助信息网络犯罪活动罪项下公开的一审判决书显示，实践中对下游犯罪、“明知”的把握缺乏明确标准，并且对帮助行为本身较为关注。网络空间中犯罪帮助行为应依其危害性和独立性进行分类，确立不同的入罪标准。对下游犯罪实行行为的促进作用程度与网络帮助行为的危害性、独立性直接相关，据此可将网络帮助行为分为三类：对下游犯罪实行行为有极大促进作用类；对下游犯罪实行行为有部分促进作用类；帮助下游犯罪前后期类。第一类对应提供专门用于侵入、非法控制计算机信息系统的程序、工具犯罪，第二类对应明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具犯罪，第三类对应帮助信息网络犯罪活动罪。对于第一类，可以独立评价帮助行为的危害性；对于第二类、第三类，仍要求对帮助下游犯罪应具备“明知”要素以及应查实下游犯罪的不法性。

关键词：网络帮助行为　提供侵入、非法控制计算机信息系统的程序、工具罪　帮助信息网络犯罪活动罪　明知

引　言

2015 年 8 月 29 日，全国人大常委会通过刑法修正案（九），针对帮助他人实施信息网络犯罪活动的行为多发的情况，设立了帮助信息网络犯罪活动罪。这可以看作是在 2009 年刑法修正案（七）增设提供侵入、非法控制计算机信息系统的程序、工具罪（以下简称“提供程序、工具罪”）之后，立法对于网络空间中犯罪帮助行为（以下简称“网络帮助行

* 中国人民大学刑事法律科学研究中心、中国人民大学未来法治研究院研究员。
本文得到“国家重点研究计划（2018YFC0830905）”资助。

为”）的整体性回应。〔1〕在此期间，司法机关出台了司法解释，使得特定领域的网络帮助行为在认定时适当突破了传统共犯理论。

针对这些立法和司法解释规定，理论界存在不同解读。对于为网络帮助行为设置独立的法定刑，学界主要存在网络帮助犯的相对正犯化、〔2〕网络帮助犯独立性说、〔3〕网络帮助犯的量刑规则〔4〕等三种观点。三种观点主要在以下两方面存在争议：（1）下游犯罪应否查实以及查实的程度；（2）帮助者对下游犯罪的主观状态，是否要求共同故意，还是单向明知即可。虽然三种观点均认为网络帮助行为因其特殊的危害性和独立性，从而不同于非网络帮助行为，但在如何准确评价不同网络帮助行为所可能具有的不同危害性和独立性，以及将上述评价与其认定相联系等方面，却缺少进一步的研究。

现有的研究讨论了网络帮助行为的分类，主要有以下几种：（1）中立和非中立的网络帮助行为。〔5〕这是中立的帮助行为理论在网络犯罪领域的延伸。（2）分为网络内容提供者、网络接入服务商、网络平台商、网络存储服务者、网络缓存服务者等。这实际上是对网络行为分类的应用，有三分法、〔6〕四分法、〔7〕五分法〔8〕甚至六分法〔9〕等。（3）直接针对某类具有代表性的网络技术或服务进行研究，比如 P2P 软件、〔10〕深度链接行为、〔11〕网络搜索引擎〔12〕等。（4）作为和不作为的网络帮助行为。〔13〕

这些分类对于研究网络帮助行为有重要价值。不过，面对多种多样的网络帮助行为，这些分类要么过于笼统，不能将具有不同危害性的网络帮助行为区分开来；要么与网络帮助行为自身的危害性、独立性关联不够，从而可能出现同一类行为包括多个罪名的客观要件或者同一罪名包括多类行为等情况，未能起到合理分类的作用。

本文从司法判决入手，研究实务中对上述争议的把握及其问题，并基于从中得到的启发在理论层面提出另一种分类方法，即以对下游犯罪实行行为的促进作用程度为准，将网络帮助行为分为三类：对下游犯罪实行行为有极大促进作用类；对下游犯罪实行行为有部分促进作用类；帮助下游犯罪前后期类。这三类分别对应具有不同程度危害性、独立性的

〔1〕 参见于志刚：《网络空间中犯罪帮助行为的制裁体系与完善思路》，《中国法学》2016 年第 2 期，第 11 页。

〔2〕 参见张明楷：《论帮助信息网络犯罪活动罪》，《政治与法律》2016 年第 2 期，第 4 页；蔡桂生：《论帮助犯的要件及其归属》，《北大法律评论》第 16 卷（2015）第 2 辑，北京大学出版社 2016 年版，第 1 页。

〔3〕 参见上引张明楷文，第 6 页。

〔4〕 同上文，第 5 页。

〔5〕 参见陈洪兵：《中立的帮助行为论》，《中外法学》2008 年第 6 期；孙万怀、郑梦凌：《中立的帮助行为》，《法学》2016 年第 1 期。

〔6〕 参见欧阳本祺、王倩：《〈刑法修正案（九）〉新增网络犯罪的法律适用》，《江苏行政学院学报》2016 年第 4 期，第 127 页。

〔7〕 参见王华伟：《网络服务提供者刑事责任的认定路径——兼评快播案的相关争议》，《国家检察官学院学报》2017 年第 5 期，第 25 页。

〔8〕 参见王莹：《网络信息犯罪归责模式研究》，《中外法学》2018 年第 5 期，第 1303 页。

〔9〕 参见陈洪兵：《论中立帮助行为的处罚边界》，《中国法学》2017 年第 1 期，第 204 页。

〔10〕 参见杨彩霞：《P2P 软件和服务提供商著作权侵害刑事责任探究——以 P2P 技术架构为切入点》，《政治与法律》2016 年第 3 期，第 42 页。

〔11〕 参见欧阳本祺：《论网络环境下著作权侵权的刑事归责——以网络服务提供者的刑事责任为中心》，《法学家》2018 年第 3 期，第 154 页。

〔12〕 参见梁根林：《传统犯罪网络化：归责障碍、刑法应对与教义限缩》，《法学》2017 年第 2 期，第 13 页。

〔13〕 参见前引〔8〕，王莹文，第 1315 页。

网络帮助行为。在与犯罪类型的对应关系上，第一类对应提供专门用于侵入、非法控制计算机信息系统的程序、工具犯罪（以下简称“提供专门程序、工具犯罪”），第二类对应明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具犯罪（以下简称“明知而提供程序、工具犯罪”），第三类对应帮助信息网络犯罪活动罪。通过上述分类，可以规范对相关罪名的解释，使对相关罪名的理解更为统一，也更有层次、更加简单清晰。

一、司法判决中的发现

立法上对网络帮助行为的回应主要体现在提供程序、工具罪和帮助信息网络犯罪活动罪，所以笔者从“威科先行”〔14〕下载这两个罪名项下截至 2018 年 9 月 17 日的所有裁判文书，共 104 份。其中提供程序、工具罪的裁判文书 83 份，帮助信息网络犯罪活动罪的裁判文书 21 份。所有裁判文书均为一审判决书。

针对主要争议点，本文在研究判决书时考虑：（1）法院在认定网络帮助行为是否成立犯罪时，是否要求存在下游犯罪或者查实下游犯罪，以及如何理解“犯罪”概念。（2）法院是否要求帮助者明知被帮助者会实施犯罪，法院对“明知”要素是如何把握的。以这些问题为线索，本文有如下发现。

（一）下游犯罪认定的乱象

在帮助信息网络犯罪活动罪中，下游犯罪以诈骗类为主；在提供程序、工具罪中，下游犯罪以侵入、非法控制、破坏计算机信息系统、程序类犯罪为主，帮助行为主要表现为提供木马、病毒类程序、游戏外挂软件、身份证识别免刷软件。所有案件中，下游犯罪行为人明确的（包括已定罪、已到案、另案处理）共 27 件；未提及或不明确的有 77 件。在大多数案件中，法院并未对下游犯罪进行认定，而只是说明帮助行为如何支持某类不法行为。

表 1　网络帮助行为下游犯罪分布情况

可能的下游犯罪	侵入、非法控制、破坏计算机信息系统、程序类犯罪（包括翻墙、免刷软件）	侵犯公民个人信息罪	盗窃罪	诈骗类犯罪
出现次数	63	26	17	27
占比（%）	60.6	25	16.3	26

在下游犯罪可能为诈骗类犯罪的共 27 个案件中，有具体诈骗人的 15 件，有具体受骗人的 17 件（其中不少案件是仅有部分受骗人明确），有具体受骗/损害金额的 13 件，其余均是这些方面不明确或未提及的案件。案件中帮助者的获利在 0 至 30 万元之间，获利形式包括销售付费、租赁、提成利润、工资/劳务付费等。这些不同形式、程度的获利并没有在定罪量刑中有较准确的反映，量刑集中在缓刑和一年有期徒刑。帮助行为与受骗事实发生之

〔14〕“威科先行”是权威的法律数据库，检索能力较强。其中的裁判文书与中国裁判文书网保持一致，及时更新。

间的因果关系，在大部分案件中是明确的，但也有个别案件并不明确。〔15〕针对诈骗类犯罪的网络帮助行为的表现形态有：制作用于诈骗的网站、广告推广、支付结算、服务器托管、网络接入、域名解析、呼叫转移、提供突破安防措施的程序、隐匿身份。

下游犯罪可能为侵入、非法控制、破坏计算机信息系统、程序类犯罪的63个案件中，帮助者提供了用于实施侵入等行为的程序、工具，判决书未提及下游犯罪实施情况的，有14件，占22.2%。这说明法院认为无论下游犯罪是否使用所提供的程序、工具实施侵入等行为，只要帮助者在知道这些程序、工具的功能的情况下提供了程序、工具，就满足定罪标准。下游实施了侵入等行为的有49件，占77.8%；下游实施的犯罪行为能够锁定到人的有31件，其中仅有1件写明另案处理，其他均未说明下游犯罪行为人的去向；下游实施了侵入等行为的，其行为是否获利，判决书均未说明。而影响侵入等行为严重性的因素，比如侵入次数、侵入造成的损害等都没有在判决书中得到体现。帮助行为的表现形态即提供的程序、工具形态。这些程序、工具按功能可以分为：能否获取计算机信息系统数据；直接还是间接突破安防措施；突破部分还是全部安防措施等。在2个案件中帮助行为是无偿的，而大部分帮助行为是获利的，形式包括劳务报酬、销售付费、出租、提成等。同样，这些获利形式的区别没有体现在定罪量刑中。

由上述分析可知，在网络帮助行为的定罪量刑中，下游犯罪的认定是比较混乱的。首先，在不少案件中，下游犯罪的行为人是不明确的，甚至是不存在的；而且，即使有具体的行为人，也鲜有到案的，更别提定罪了。其次，对于存在下游犯罪且得到明确的，对下游犯罪严重性的把握并不明确。判断标准五花八门，把握尺度松紧不一。再次，下游犯罪所侵犯的法益及侵犯的严重程度，在不少案件中是不明确的。比如，在下游犯罪为诈骗类犯罪的案件中，有不少案件未提及受骗人或者受骗人不明确。即使在受骗人明确的案件中，法院把握的尺度也相差很大。比如，在下游的诈骗类犯罪中，诈骗金额为30万元的和诈骗金额为几百元的，上游的网络帮助行为的量刑却是相同的。最后，下游犯罪与网络帮助行为之间的因果关系，在很多案件中都没有被提及、讨论，在有些案件中这一因果关系明显难以成立。

（二）“明知”认定的混乱

理论上关于网络帮助行为的“明知”要素存在很多争议。〔16〕而且，“明知”的证明也是难点，其证明方法包括直接证明、推定和证明责任倒置等。在本文的样本中，所有案件都有帮助者的供述，但供述内容都未给出；判决书都没有写明其认定的“明知”是什么含义，也没有对“明知”为何成立的证明和解释。这使得了解法院如何把握“明知”变得十分困难。由于缺少直接途径，本文只能运用间接方法来推测法院对“明知”的把握。

如果“明知”是要求双向的意思联络，则被帮助者应当是具体的，且与帮助者有过联系。据此观察判决书，发现：没有具体的被帮助者，或者虽有具体的被帮助者但没有其与帮助者的联系记录的案件，有47件，占45.2%；有具体的被帮助者，并且有其与帮助者关于帮助行为内容及付费等的具体约定的案件，有41件，占39.4%；明确或者能够推定帮助

〔15〕 参见福建省上杭县人民法院（2017）闽0823刑初157号刑事判决书。

〔16〕 参见吴扬传：《论中立帮助行为的司法认定》，《法律适用·司法案例》2017年第12期，第3页。

者知道被帮助者将自己提供的帮助用于实施犯罪活动的案件，有 16 件，占 15.4%。

由此可知，在有些案件中法院认为“明知”应是双向的意思联络，而在有些案件中法院认为构成“明知”不需要双向的意思联络。进一步观察，要求双向意思联络的案件，涉及的下游犯罪有诈骗类犯罪、侵入、非法控制、破坏计算机信息系统、程序类犯罪、盗窃罪、侵犯公民个人信息罪等；不要求双向意思联络的案件，涉及的下游犯罪也包括这些犯罪。可见，对“明知”的不同把握，并不是以下游犯罪的类型来区分的。而且，在同样要求双向意思联络的案件中，有些要求帮助者明确知道被帮助者会将其提供的帮助用于实施犯罪活动，而有些只要求帮助者大概知道被帮助者可能会将其提供的帮助用于实施犯罪活动。比如，有判决书明确写道：帮助者“明知可能”被用于实施犯罪活动。〔17〕在仅要求“大概知道”的案件中，有些认为这种“大概知道”的程度应当比较高，比如有鉴定意见或者专家证言来说明所提供的程序、工具用于犯罪的专门性程度；有些则没有讨论这一问题。即使在这些案件中提供的帮助是比较中立的，也没有发现法院运用了“专门用于实施犯罪”的标准。〔18〕

表 2 “明知”的认定情况

序号	涉及罪名	双向意思联络		帮助者单向明知	
		有被帮助者，且帮助者与被帮助者有关于帮助行为内容及付费等的具体约定	明确或能够推定帮助者知道被帮助者将其提供的帮助用于实施犯罪活动	没有具体的被帮助者	虽有被帮助者，但没有帮助者与被帮助者之间的联系记录
1	帮助信息网络犯罪活动罪	10	8	2	1
2	提供程序、工具罪	31	8	11	33
共计		41	16	13	34
占比（%）		39.4	15.4	12.5	32.7

对于“明知”的认定，帮助者是否牟利、牟利多少、牟利与提供帮助以及下游犯罪之间的关系等，也是重要因素。据此观察判决书，发现：在有些案件中，帮助者是否牟利并不明确；在有些案件中，帮助行为是无偿的；〔19〕在有些案件中，法院没有关注牟利额度是否高得不正常；在有些案件中，法院则强调所得收益过高。在存在牟利情况的案件中，被认定为可推定存在“明知”的牟利形式包括：基于职务或雇佣关系提供帮助从而获得工资或佣金，销售、出租相应技术以获得费用，就被帮助者基于帮助行为而获得的利益予以提成等。理论上讲，工资与提成反映了不同程度的主观恶性，前者是被动接受，后者则是积

〔17〕 参见浙江省绍兴市上虞区人民法院（2016）浙 0604 刑初 1032 号刑事判决书。

〔18〕 有关判断中立帮助行为入罪的标准，参见前引〔9〕，陈洪兵文。

〔19〕 参见浙江省景宁畲族自治县人民法院（2018）浙 1127 刑初 21 号刑事判决书；四川省冕宁县人民法院（2015）冕宁刑初字第 141 号刑事判决书。

极索取，在量刑时应有所区分。但在实际案件中，仅有较少的案件在涉及工资形式的牟利时，讨论了帮助者基于职务被动提供帮助和参与下游犯罪分赃所体现的不同程度的主观恶性。而大部分案件都没有对不同形式的牟利予以区分，只要帮助者从其提供的帮助中获利，就构成牟利，从而推定存在“明知”。在那些下游犯罪没有查实，甚至不存在下游犯罪的案件中，“明知”都得到了认定，判决书并没有给出特别的解释。在一些案件中，即使帮助者的获利与下游犯罪并无明确联系，甚至不存在联系，也会被认定构成牟利，从而推定存在“明知”。

由上述分析可知，实务中在网络帮助行为的定罪量刑上，对“明知”的把握是比较混乱的。有些案件认为，成立“明知”应要求双向意思联络；有些案件则认为，只要帮助者单向明知即可；有些案件认为，成立“明知”，帮助者应当知道具体要实施的下游犯罪；有些案件则认为，帮助者大概知道要实施的下游行为是犯罪活动即可。关于“大概知道”的程度，有些案件认为，应达到专门性的程度；有些案件认为，只要帮助者知道其提供的帮助有可能被用于实施下游犯罪即可。关于牟利与认定“明知”的关系，有些案件认为，成立“明知”要求帮助者有牟利；有些案件则要求，牟利须明显不正常，才能成立“明知”；有些案件则认为，帮助者即便未牟利也可构成“明知”。

（三）司法判决的启发：同类网络帮助行为的定罪标准较为一致

法院的上述做法无法用理论上关于网络帮助行为的争议来解释。在一个判决中，法院的意见往往是几种观点揉合在一起。比如，部分意见可以看作是遵循帮助犯正犯化理论，部分意见又是支持帮助犯独立性理论。而判决之间的异同，也很难用理论观点之间的异同来解释。虽然帮助犯正犯化说、帮助犯独立性说、量刑规则说在很多方面的具体观点是一致的，但仍有不小差别。比如，帮助犯正犯化说强调，网络帮助行为的危害性突出，足以被提升为正犯，所以被正犯化后的网络帮助行为成立犯罪，不以下游犯罪的成立为前提，故不需要查实下游犯罪；网络帮助犯罪有独立的主观要件，在认定“明知”时不要求帮助者与下游犯罪行为人有双向意思联络，甚至不要求具备单向的明知。〔20〕据此观察判决书，在那些下游犯罪行为人和具体行为不明确或未被提及的案件中，有不少案件在认定“明知”时又强调帮助者与被帮助者之间有意思联络，〔21〕有些则强调帮助者单向明知被帮助者的实行行为。〔22〕虽然在帮助犯正犯化之后，仍然可以成立对帮助者进行帮助的帮助犯，但在这些不关注下游犯罪的案件中，虽然事实上有发现对帮助者进行帮助的人，但没有一个案件对这些帮助帮助者的人采取刑事措施，也没有提及任何处理措施，更没有对其提起公诉。〔23〕而在强调或查实下游犯罪行为人和行为的案件中，有些案件在认定“明知”时又不要求存在双向意思联络，仅要求具备单向明知或大概知道帮助行为的整体危害性即可。〔24〕

本文在发现上述难以用现有理论解释的乱象后，尝试理解司法实践的逻辑，寻找能够

〔20〕 参见前引〔1〕，于志刚文，第 9 页。

〔21〕 参见福建省厦门市同安区人民法院（2018）闽 0212 刑初 204 号刑事判决书。

〔22〕 参见浙江省景宁畲族自治县人民法院（2018）浙 1127 刑初 21 号刑事判决书。

〔23〕 在许多案件中，帮助者提供的程序、工具或者技术都不是自己制作的，而是从他人那里获得的。参见广东省东莞市第一人民法院（2017）粤 1971 刑初 250 号刑事判决书等。

〔24〕 参见浙江省绍兴市上虞区人民法院（2016）浙 0604 刑初 1032 号刑事判决书。

解释司法实践的统一理论维度。本文认为网络帮助行为本身的危害性、独立性是理解和解释司法实践中不同做法的关键。虽然样本反映的网络帮助行为形态多样，但基本可以分为三类：（1）提供以木马、病毒类程序、游戏外挂、免刷软件、钓鱼网站等为代表的程序、工具的帮助行为。通过这类程序、工具，可以在未被授权的情况下侵入计算机信息系统，进而修改或控制计算机信息系统的程序并对其进行维护。（2）提供以秒拨、〔25〕验证码自动识别、租用微信等支付账号、呼叫转移等为代表的程序、工具和服务的帮助行为。通过这类程序、工具和服务，可以隐匿身份、间接突破计算机信息系统的安防措施。（3）提供广告推广、支付结算、服务器托管、网络接入、域名解析等服务的帮助行为。这三类帮助行为大致对应相关罪名。第一类大多被认定为提供程序、工具罪，第三类大多被认定为帮助信息网络犯罪活动罪。第二类被认定的罪名虽然是上述两种罪名皆有，但所占比例很小。如果以上述分类为视角进行观察，可以发现，法院对下游犯罪和“明知”等的认定标准是较为一致的。涉及木马、病毒类程序、游戏外挂、免刷软件、钓鱼网站的案件，大多没有关注是否存在下游犯罪；其他的网络帮助行为案件则更多地关注了下游犯罪的具体情况，对“明知”的认定也提出了更加具体的要求乃至要求须具备双向意思联络。

二、类型划分的依据

在上述实证研究发现的启发下，本文认为，网络帮助行为的定罪应关注提供帮助的行为本身，对其进行类型化应以网络帮助行为本身的危害性、独立性为重心。理由如下：

其一，面对多种多样、性质差别很大的网络帮助行为，很难脱离网络帮助行为本身来讨论其下游犯罪和“明知”要素。不同的网络帮助行为会有不同的危害性和独立性，不可一概而论。正是因为其特别的危害性和独立性，才使得在认定网络帮助行为成立犯罪时，可以突破传统共犯理论。而不同网络帮助行为在危害性和独立性上的不同，会影响到其能否突破传统共犯理论以及突破的程度，进而影响其定罪标准。

其二，由于网络技术快速更新，网络空间快速拓展，网络秩序难以稳定，网络空间很多方面的利益分配机制尚未确定、具体的权利义务尚不明确，所以，被网络帮助行为直接侵犯的利益在立法上经常未得到确认。比如，以自动切换 IP 地址、自动识别验证码、自动发现网络安全漏洞等为代表的具有突破或躲避网络安防措施功能的技术，其直接侵害的诸如 IP 地址资源、安防程序代码或者算法规则等，并不是法律明确规定的公共利益或者私人权利。〔26〕而且，这类网络资源因其本身的特性，也很难被认定为属于某一私人主体、公共主体或者中间组织。但是，这类技术可以突破或绕开全部或部分网络安防措施，且极易传播，用户可在这类技术的基础上使用和接续开发更多的功能。〔27〕也就是说，这类技术可借

〔25〕 关于秒拨的技术原理、犯罪路径、性质分析等，参见《中国检察官》2018 年第 3 期以“提供‘秒拨’动态 IP 服务的行为定性”为主题的系列论文。

〔26〕 程序代码或设计可能会受到知识产权的保护，但这种保护是针对复制、抄袭等行为的，而不针对攻击、突破等行为。

〔27〕 参见门美子：《提供动态 IP 服务的行为定性》，《中国检察官》2018 年第 3 期，第 8 页；邓矜婷：《“秒拨”动态 IP 切换技术的性质评析》，《中国检察官》2018 年第 3 期，第 6 页。

由网络扩散，从而引发大面积、大规模的危害。此时，刑法的规制就变得迫切了，从而出现为人诟病和引发担忧的“刑法先行”现象，[28] 也催生了“打早打小”的网络犯罪刑事政策。[29] 在这种情况下，由于其直接侵害的利益在立法上往往未得到确认，通过非网络帮助犯罪的刑法分则罪名独立探论上述网络帮助行为的刑事可罚性就十分困难。所以，通过网络帮助行为可能间接侵害的、已得到刑法明确保护的法益，以单独的网络帮助行为类犯罪来评价其刑事可罚性，就成为目前相对审慎的方法。

其三，网络帮助行为的类型决定了下游犯罪、明知、帮助行为与下游犯罪之间的因果关系等要素需要查实的程度。样本研究已经表明，不同类的网络帮助行为在定罪的主客观要件方面，其具体的把握标准是不一样的，而同类网络帮助行为在这些方面则基本一致。本文认为这不是偶然的。网络帮助行为可能实现的不同功能对下游犯罪所产生的促进作用是不同的，这使得认定主客观要件成立的难度也会不同。木马、病毒、免刷软件、钓鱼网站等程序、工具具有使计算机信息系统或者程序的主要功能无法正常运行的破坏作用，从而使得下游犯罪实行行为的实施变得轻而易举。因此，这些程序、工具的提供者通常知道这些程序、工具会被用来干什么，从而容易推定“明知”的成立。同理，被帮助者在获得这些程序、工具后通常会将其用于实施犯罪，而且往往在安装之后这些程序、工具会自动运行，所以很容易证明下游犯罪的存在。而根据所提供的程序、工具的数量和运行时长，能够大致推算下游犯罪的严重程度。如果这些程序、工具是有偿提供的，认定相关要素的依据就更加充分了。相比之下，提供服务器托管、网络接入、域名解析、呼叫转移、微信等支付账户、广告推广等服务，则不像提供前述程序、工具那样，仅能用于使计算机信息系统或者程序丧失主要功能。因此，不能仅凭提供了这些服务，就推定提供者具备“明知”要素并推论下游犯罪的存在和严重程度。要作出这些推定和推论，需要更多的证据。

其四，网络帮助行为的刑事立法、司法活动及其演变，也体现了对网络帮助行为类型区分的关注。立法上，网络帮助行为不是作为一个整体来入罪的，而是迫于不同种类网络犯罪的发展形势而逐步、分类进行犯罪化的。司法上，一方面，为顺应立法变化，更好地实现立法目的、更准确地理解立法原意，司法机关出台了一系列司法解释和规范性文件。[30] 另一方面，对于特定领域内几类关键性的网络帮助行为，司法机关出台了有针对性的规范性文件，引入了片面共犯、共犯正犯化等原理。[31] 总之，刑事立法、司法活动对网络帮助

〔28〕 关于个人信息保护领域内的“刑法先行”现象，参见石亚淙：《网络时代的刑法面孔——“网络犯罪的刑事立法与刑事司法前沿问题”学术研讨会综述》，《人民检察》2016 年第 15 期。

〔29〕 参见喻海松：《网络犯罪二十讲》，法律出版社 2018 年版，第 9 页。

〔30〕 例如 2004 年《最高人民法院关于审理破坏公用电信设施刑事案件具体应用法律若干问题的解释》，2011 年《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》，2014 年《最高人民法院、最高人民检察院、公安部、国家安全部关于依法办理非法生产销售使用“伪基站”设备案件的意见》，2017 年《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，2017 年《最高人民法院、最高人民检察院关于办理扰乱无线电通讯管理秩序等刑事案件适用法律若干问题的解释》。

〔31〕 参见 2010 年《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）》，2010 年《最高人民法院、最高人民检察院、公安部关于办理网络赌博犯罪案件适用法律若干问题的意见》，2016 年《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》。

行为没有采取“一揽子”的入罪化处理，而是根据网络犯罪的发展形势，应急性地“因技而变”，采取分别入罪、降低入罪门槛等方法，对不同种类的网络帮助行为作区别对待。〔32〕

其五，对网络帮助行为按照该行为自身的危害性、独立性进行分类，可实现行为类型的合理区分，实现违法性、有责性的合理匹配，并防止刑罚圈过分扩张。由于网络技术的快速更迭，刑事立法和司法都出现了应接不暇的情况，而法律的稳定性、刑法的谦抑性也是重要的法治价值，此时就出现了如下的两难局面：既担心刑事治理不及时，又害怕刑事治理不当、处罚过度。而对于网络帮助行为这一极具技术色彩的刑事规制领域，法律与技术既要保持一定的距离，又不能过于脱离技术，因此，一种介于两端之间的中间性概念或许有助于化解上述两难局面。而网络技术本身所蕴含的危险性以及相对的独立性，既能充分反映技术本身的特性，并能随着技术的发展而变化，又不会因为技术的某些微小变化而改变，从而是具有一定稳定性的中间性概念，同时这一概念又与刑法所关注的法益侵害性（社会危害性）直接相关，也可与行为的有责性相匹配。因此，以此为标准来划分网络帮助行为的类型，可以实现网络技术快速更迭与法律稳定性的对接，使法律可以更好地因应网络技术的发展。

三、具体的类型

（一）应以网络帮助行为所能实现的全部功能来划分网络帮助行为的类型

无论是以程序、工具的形式还是服务的形式体现的网络帮助行为，都可能具有多项功能。这些在提供帮助时就可能具有的功能，应一并作为评价标准来评价网络帮助行为的刑法意义。而经过升级或加工之后才具有的功能，则不应被包括在网络帮助行为危害性的评价中，因为这些功能不是出自帮助者提供帮助的行为。但是，通过对所提供的程序、工具稍加修改就能实现的功能，应当被包括在相应评价标准里。这是因为，程序功能往往都需要经过环境参数修改、设定路径等调试，才能在新的计算机信息系统中运行。比如，有些木马程序需要经过一些路径、环境参数等的设定、修改，才能被用来攻击具体的计算机信息系统，但不会因此就认为这些木马程序不具有攻击性。而如果这些木马程序本来不具有获取数据的功能，但经过修改具有了获取数据的功能，则此时不能认为原木马程序具有破坏性。

在进行功能评价时，不应以下游犯罪已使用的功能为限，也不应以可能被用于实施犯罪的功能为限。如果作出上述限制，则相当于要求查实下游犯罪。另外，如果以下游犯罪实际使用的功能为限，会导致对同样的网络帮助行为作出不同的危害性评价。而且，与下游犯罪的联系可以在网络帮助行为的危害性、独立性与犯罪主客观要件的联系中体现，帮助行为的危害性、独立性包括但不限于所提供的帮助被用于实施犯罪的可能性，还包括所实施的犯罪行为的性质、恶劣程度等，因此，以可能被用于实施下游犯罪的功能为限，过于片面。

（二）网络帮助行为的具体类型

1．网络帮助行为的全部或部分具有可极大促进下游犯罪实行行为的功能

由于网络帮助行为本质上仍是犯罪帮助行为，其危害性主要源于其帮助的犯罪行为的

〔32〕 参见前引〔29〕，喻海松书，第 6 页以下。

危害性，而被帮助的犯罪行为的危害性集中体现在该犯罪的实行行为上，所以，以帮助行为对下游犯罪实行行为的促进作用程度为标准划分网络帮助行为的类型，可以与网络帮助行为本身的危害性直接关联。这是因为网络帮助行为多呈现出一对多、迅速广泛传播等特点，故在评价网络帮助行为的危害性时，多以其单次帮助的危害性乘以帮助的量（比如提供帮助的次数，提供的程序、工具、服务的数量）为准，而单次帮助的危害性主要体现在对下游犯罪实行行为的促进作用程度。因此，网络帮助行为对下游犯罪实行行为的促进作用程度，会显著影响网络帮助行为的危害性，从而使具有不同危害性的网络帮助行为相互区别开来。

本类网络帮助行为是指能在极大程度上促进下游犯罪实行行为的网络帮助行为。能在极大程度上促进下游犯罪的实行行为，是指在获得这类帮助后，下游犯罪的实施就只差很简单、很小的一部分，就好像只需按一下键、点一下鼠标、安装一下软件等，就能实现犯罪目的。如果以量来打比方，可以认为这类帮助行为已经促成下游犯罪 80% 以上的进度，实行行为只是完成剩余的 20%。由于同样的程序、工具可以被不同的帮助者以不同的程度来促进下游犯罪的实行行为，所以应以当前社会情势下客观的一般人或者网络技术标准来判断，该程序、工具能否被用于极大地促进某类或某几类下游犯罪的实行行为。

这类网络帮助行为不仅在网络空间有较强的破坏性，其还可以通过对下游犯罪实行行为的高度促进作用，在物理空间造成直接危害，而且这一危害会因为网络技术易迅速广泛扩散的特点而成倍增长，所以在认定成立犯罪时，对于主观方面和查实下游犯罪，就应当在各类网络帮助行为中作最低要求。也就是说，由于此类帮助行为使下游犯罪实行行为的实施变得非常简单，帮助者通过此类帮助行为一般就会知晓下游犯罪所可能造成的危害，进而认识到此类帮助行为本身的危害，所以，不需要查实下游犯罪即可独立评价此类帮助行为的危害性。另外，由于此类帮助行为能够在极大程度上促进某类或某几类下游犯罪的实行行为，所以，只要帮助者知道此类帮助行为具有何种功能，一般就会知晓该帮助行为对下游犯罪实行行为的高度促进作用，因此原则上不需要具备双向的意思联络。

综上，在认定本类网络帮助行为是否成立犯罪时，只需对本类帮助行为作独立评价。尤其是主观要素上，只要帮助者知道所提供的帮助能在极大程度上促进下游犯罪的实行行为即可。在危害程度的评价上，只要考虑所帮助的下游犯罪的严重程度、帮助的人数、提供帮助的次数、提供的程序、工具等的数量、提供帮助获利的情况等因素即可。

2．排除第一类帮助行为所具有的功能，网络帮助行为的全部或部分具有可部分促进下游犯罪实行行为的功能

本类是除去第一类帮助行为之后进行的再分类。这类网络帮助行为是指，帮助行为只能部分促进下游犯罪的实行行为，下游犯罪的主要部分仍需要由下游犯罪的实行行为来完成。如果以量来打比方，可以认为本类帮助行为已经促成下游犯罪 30% －80% 的进度，下游犯罪的实行行为仍然要完成剩余的 20% －70%。此类帮助行为的典型，是提供以自动切换 IP 地址、自动识别验证码为代表的突破部分或全部网络安防措施的程序、工具的行为。〔33〕

〔33〕 参见前引〔27〕，门美子文，第 8 页。

通过这类程序、工具，可以不侵入计算机信息系统而间接获取数据，这是网络犯罪产业链化的一种表现。因为不能直接促成侵入、非法控制计算机信息系统等犯罪活动，这类帮助行为的危害性应被认为小于第一类帮助行为，所以，在定罪时对于主观方面和查实下游犯罪，相较于第一类帮助行为，应有更高的要求。

这类帮助行为在实践和理论上存在很多争议。以自动切换 IP 地址为例，相关研究就持有各种不同的观点。〔34〕在把握本文的这一分类时，应当尤为注意以下两点：

首先，应以帮助行为所具有的全部、整体功能为对象，在确定不具有第一类帮助行为所具有的功能之后再考虑是否属于本类帮助行为。比如在有的案件中，帮助者不只是提供自动切换 IP 的技术，还打包提供了其他程序，或实施了“撞库”，即同时完成了侵入计算机信息系统和获取数据的行为，最终提供的是公民个人信息等。〔35〕像这样的帮助行为就属于第一类帮助行为。

其次，由于本类帮助行为只能部分促进下游犯罪的实行行为，所以在实施了本类帮助行为后，被帮助者不一定就实施了下游犯罪，也可能利用该帮助实施了其他并非违法犯罪的行为。因此，还不能认定帮助者在提供帮助时就明知被帮助者要实施下游犯罪，也不能只根据提供的帮助就认定帮助者部分地促进了下游犯罪的实行行为、造成了较大的社会危害。因而在评价本类帮助行为的危害性时，不能只看帮助行为本身，还需要考虑其与下游犯罪的关联程度以及下游犯罪的实施情况。具体而言，在主观要素上，帮助者应明知被帮助者要利用自己所提供的帮助实施下游犯罪；在客观方面，应查实被帮助者是否利用帮助者所提供的帮助实施了下游犯罪；在评价危害程度时，应考虑被帮助者利用帮助者提供的帮助所实施的下游犯罪的严重程度、提供帮助的次数、帮助的人次、提供帮助获利的情况等因素。

3．排除第一、二类帮助行为所具有的功能，网络帮助行为的全部或部分具有帮助下游犯罪前后期的功能

第一、二类网络帮助行为对下游犯罪实行行为都具有较大程度的促进作用，而本类帮助行为出现在下游犯罪实施的前期或者后期，其对下游犯罪实行行为的促进作用是很小的。如果以量来打比方，可以认为本类帮助行为使下游犯罪进行到 30% 以下的进度。下游犯罪实施的前期，一般认为是犯罪实行前的宣传、推广、网络接入等阶段，而后期一般认为是犯罪实行终了后的支付结算、转移赃款等阶段。不过，前后期是相对于下游犯罪实行行为而言的，不能认为这些具体阶段永远是前期或者后期，也不能认为这些阶段所涉及的技术、程序、工具永远不会涉及第一、二类帮助行为。比如，对于虚假广告罪、洗钱罪等犯罪，所谓前后期阶段的行为就会被认定为虚假广告罪、洗钱罪。此时，这些所谓的前后期行为在这些犯罪中就成了实行行为。

由于本类帮助行为是在下游犯罪的前后期阶段实施帮助，对下游犯罪实行行为的促进作用甚小，相比第二类帮助行为，本类帮助行为距离下游犯罪的完成更远，也更有可能被用于开展并非违法犯罪的正当行为，所以，帮助者在提供帮助时更加不一定知晓被帮助者

〔34〕 参见前引〔25〕，《中国检察官》2018 年第 3 期刊发的系列论文。
〔35〕 参见前引〔27〕，门美子文，第 8 页。

会利用自己所提供的帮助来实施下游犯罪，帮助行为的危害性评价也更加依赖对被帮助的下游犯罪的查实。具体而言，在主观要素上，帮助者应明知被帮助者要利用自己所提供的帮助实施下游犯罪。对于客观方面，应查实被帮助者是否利用帮助者所提供的帮助来实施下游犯罪。在评价危害程度时，应考虑被帮助者利用帮助者提供的帮助所实施的下游犯罪的严重程度、提供帮助的次数、帮助的人次、提供帮助获利的情况等因素。相比于第二类帮助行为，本类帮助行为对下游犯罪的促进作用甚小，就同样的下游犯罪而言单次帮助的危害也更小，所以，对于本类帮助行为，应当达到更大的帮助量才宜定罪处罚。

四、与犯罪类型的对应关系

前文在对司法判决进行归纳后，得出了以网络帮助行为对下游犯罪实行行为的促进作用程度为标准进行划分所得到的网络帮助行为类型。这一分类必须被涵摄进刑法规定的相应犯罪类型才具有法律规范意义，下面就讨论前述分类与提供程序、工具罪和帮助信息网络犯罪活动罪的对应关系。

（一）第一类网络帮助行为对应提供程序、工具罪的次类型提供专门程序、工具犯罪

刑法关于此类犯罪所规定的“专门用于”，应当被解释为该程序、工具可以极大地促进下游犯罪（即侵入、非法控制计算机信息系统罪）的实行行为。而且，与第一类帮助行为相同，构成此类犯罪，在主观要件上，不要求帮助者对被帮助者利用自己所提供的帮助实施下游犯罪有明知。客观方面则明确规定提供“专门用于”侵入、非法控制计算机信息系统的程序、工具，〔36〕相关司法解释为确定是否属于“专门用于”，给出了具体的界定和确定的程序。〔37〕

“专门用于”不是指相关程序、工具仅具有侵入、非法控制计算机信息系统的功能，而是指该功能在众多功能中最为突出、明显，以至于成为该程序、工具最显著的特征。换句话说，该程序、工具使得下游犯罪的实施变得极为容易，以至于被认为是“专门用于”实施该犯罪的。目前相关司法解释给出的界定标准是，“避开或者突破计算机信息系统安全保护措施”。〔38〕这实际上就是将“专门用于”解释为使得侵入、非法控制计算机信息系统等犯罪的实施变得极为容易，只要安装并运行该程序、工具即可。而且，由于避开或者突破安防措施只是其中的一种方法，还有通过网络抓包获取密码、通过扫漏软件发现没有安装杀毒软件的系统并进行攻击等方法，〔39〕所以相关司法解释特意设置了兜底条款。〔40〕

由于此类犯罪的危害性在于其能够极大地促进侵入、非法控制计算机信息系统等犯罪

〔36〕 参见前引〔29〕，喻海松书，第41页。

〔37〕 参见2011年《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第2条、第10条。

〔38〕 参见2011年《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第2条第1项、第2项。

〔39〕 有关威胁网络安全的可能方法，参见［美］William Stalling：《网络安全基础：应用与标准》，白国强等译，清华大学出版社2014年版，第1章。

〔40〕 参见2011年《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第2条第3项。

的实施，所以成立此类犯罪不要求帮助者对被帮助者利用自己所提供的程序、工具实施下游犯罪有明知，因此也不需要查实下游犯罪。

值得注意的是，在目前的立法下，第一类网络帮助行为与此类犯罪实为包含关系。这是因为，此类犯罪仅针对提供专门程序、工具的行为，而第一类网络帮助行为能够极大促进的下游犯罪多种多样，并不限于侵入、非法控制计算机信息系统罪。比如，利用程序直接抓取传输中的数据包或信号从而获得公民个人信息，就不需要侵入或者非法控制计算机信息系统。〔41〕所以，针对第一类网络帮助行为，还有进一步严密刑事法网的需要。

（二）第二类网络帮助行为对应提供程序、工具罪的次类型明知而提供程序、工具犯罪

此类犯罪的要件是，明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，所以该程序、工具不是一般的仅具有正常功能的程序、工具。与第一类网络帮助行为一致，提供此类程序、工具对侵入、非法控制计算机信息系统等犯罪的实施有实质促进作用。本类犯罪与提供专门程序、工具犯罪被规定在同一条文中，适用同一罪名，只是没有“专门用于”的限定，在促进下游犯罪实行行为的作用程度上也有不同。因此，本类犯罪应被解释为对下游犯罪（即侵入、非法控制计算机信息系统罪）的实行行为有部分促进，从而与第二类网络帮助行为相对应。在主观要素方面，成立明知而提供程序、工具犯罪，要求帮助者明知被帮助者实施下游犯罪。在评价危害性时，由于只是部分促进下游犯罪的实施，距离下游犯罪的完成不像提供专门程序、工具犯罪那么近，所以，无法单纯从提供帮助行为本身来确定危害性的大小，还需要结合下游犯罪的情况进行评价。具体而言，应查实被帮助者是否利用帮助者所提供的程序、工具实施了下游犯罪。

同样，明知而提供程序、工具犯罪也仅针对侵入、非法控制计算机信息系统罪，而实际能够为这些程序、工具所促进的下游犯罪肯定不止这一种，所以第二类网络帮助行为与明知而提供程序、工具犯罪也是包含关系。因此，前述严密刑事法网的建议在此也适用。

（三）第三类网络帮助行为对应帮助信息网络犯罪活动罪

立法设立此罪引发了很大的争议。有学者认为，此罪是将网络帮助行为正犯化，鉴于网络帮助行为所具有的巨大的量，应对其进行独立评价，实行“积量构罪”。〔42〕另有学者认为，此罪仍然是在传统共犯理论的基础上对网络帮助行为进行评价，但其涵盖的范围太广，把很多中立帮助行为也包括了进来，必须对其进行限缩解释。〔43〕还有很多研究所持的观点处于两者之间。〔44〕本文认为，产生争议的关键点是，争论各方所针对的网络帮助行为是不同的。当学者认为应将网络帮助行为正犯化时，所考虑的是具有很高危害性的网络帮助行为；而当学者认为应在共犯理论的框架下对网络帮助行为作限缩解释时，所考虑的是更多具有中立帮助行为色彩的网络帮助行为。本罪针对的是利用信息网络实施犯罪的情形，

〔41〕 参见前引〔39〕，Stalling 书，第 1 章。

〔42〕 参见皮勇：《论新型网络犯罪立法及其适用》，《中国社会科学》2018 年第 10 期，第 126 页；刘仁文、杨学文：《帮助行为正犯化的网络语境——兼及对犯罪参与理论的省思》，《法律科学》2017 年第 3 期，第 123 页。

〔43〕 参见张婷：《中德网络帮助犯规制体系之评介反思》，《重庆邮电大学学报（社会科学版）》2017 年第 1 期，第 45 页。

〔44〕 参见阎二鹏：《法教义学视角下帮助行为正犯化的省思》，《社会科学辑刊》2016 年第 4 期。

学者们从相关刑法条文的字面都能解读出支持自己观点的意思，因此，要解决争议，还是要厘清此罪所指的到底是怎样的网络帮助行为。

本罪的法定刑设置轻于提供程序、工具罪，故本罪对应于危害性低于第一、二类网络帮助行为的网络帮助行为。而且，从刑法条文列举的互联网接入、服务器托管、支付结算等行为方式看，本罪也只是参与了下游犯罪实施的前后期阶段。关于本罪的主观要素，根据刑法的规定，帮助者须明知自己在帮助他人利用信息网络实施犯罪。所以，本罪与第三类网络帮助行为相对应。

由于第三类网络帮助行为具有更低的危害性，所以对帮助信息网络犯罪活动罪应适用更高的认定标准，即要求更确切的明知和查实下游犯罪。这样也能合理限制处罚范围。由于将此罪限定在下游犯罪实施的前后期，对于具有更高危害性、独立性的能够极大或部分促进下游犯罪实行行为的网络帮助行为，就可以提供程序、工具罪来定罪量刑。将帮助信息网络犯罪活动罪中对帮助行为方式的具体列举，解释为对下游犯罪前后期阶段的列举，既符合这些帮助行为方式的共同特点，又使得将来对帮助行为方式进行立法扩充时有相应的依据，从而不会无限扩充。而且，正如前文所述，互联网接入、支付结算等行为不会永远只是下游犯罪的前后期，它们也可能被单独入罪。比如，如果出现了专门帮助洗钱的网络技术，提供这种技术的行为就应当按提供专门程序、工具犯罪进行评价。

（四）帮助信息网络犯罪活动罪与明知而提供程序、工具犯罪中下游犯罪的查实程度

在网络帮助行为中有这样一类行为，它们为多个下游违法行为提供帮助，但这些下游违法行为都没有达到成立相应犯罪的严重危害程度，从而无法构成违法意义上的犯罪。〔45〕但是，这些网络帮助行为能够为很多下游违法行为提供帮助，被认为具有特别的社会危害性。对于这类帮助行为，是否应当入罪、应当如何入罪，学界存在较大争议。有的学者认为，不应当全面入罪。〔46〕这就好像在物理世界中分别帮助10个小偷偷自行车，每个小偷只偷了1辆价值不足千元的自行车，由于每个小偷的行为都不构成犯罪，所以帮助者的行为也无法入罪。〔47〕有的学者则认为，应当入罪。因为在网络帮助行为的情形下，帮助的不是10个小偷，而是上万、上百万甚至上千万的小偷，虽然单次帮助或者单个帮助行为的危害性较小，但多次帮助或者多个帮助行为的整体危害性就会由量变发生质变，即所谓“积量构罪”。〔48〕据此，即使被帮助的下游违法行为都不构成相应犯罪，但只要网络帮助行为帮助了足够多的下游违法行为，累积起来对社会的危害就足够大，帮助行为就能够入罪。

本文认为，这类网络帮助行为不属于第一类网络帮助行为，因为此类帮助行为不可能极大地促进下游犯罪的实行行为，但此类帮助行为可以构成第二、三类网络帮助行为，从而成立明知而提供程序、工具犯罪或帮助信息网络犯罪活动罪，因此不应仅以相应犯罪的帮助犯来加以评价。当网络帮助行为仅部分促进下游犯罪的实行行为时，提供了帮助后仍然存在被帮助者未实施下游犯罪的可能性，或者只实施了部分行为从而不构成相应犯罪，

〔45〕 参见付立庆：《违法意义上犯罪概念的实践展开》，《清华法学》2017年第5期，第68页。

〔46〕 参见刘艳红：《网络犯罪帮助行为正犯化之批判》，《法商研究》2016年第3期，第20页以下。

〔47〕 参见最高人民法院刑事审判第一、二、三、四、五庭主办：《刑事审判参考》第104集，法律出版社2016年版，第91页。

〔48〕 参见前引〔42〕，皮勇文，第126页。

如此一来，相应的网络帮助行为就只是帮助了多个不构成犯罪但违法的行为。对于这种网络帮助行为，因其是部分促进下游犯罪的实行行为而不是帮助下游犯罪的前后期，故存在以第二类网络帮助行为所对应的犯罪类型来评价的可能性。如果帮助的下游违法行为是侵入、非法控制计算机信息系统类的犯罪行为，则应以明知而提供程序、工具犯罪来评价。

上述网络帮助行为所提供的帮助的量可能非常大，所以虽然单次帮助不会对法益构成严重危害，但是乘以其帮助量，可能会对网络管理秩序构成危害，因而可能需要刑法予以规范。〔49〕事实上，学界对于此类网络帮助行为应适当入罪不存在争议，普遍认同对网络帮助行为的刑法评价应反映其一对多、迅速传播等特点。〔50〕只是，可以“积量构罪”不表示此类网络帮助行为就一定能够脱离下游犯罪作独立评价。虽然此类网络帮助行为因其自身特点可以突破对单个罪量的质的要求，但“积量构罪”的前提仍是要有足够多的单个非法在量上的积累，没有被帮助的违法行为，就不会有帮助行为的社会危害性。

不过，既然肯定此类网络帮助行为因其帮助量大对网络管理秩序造成足以应当以刑罚干预的严重危害，那么主要关注的就应当是危害性整体的量有多少，而与某次帮助或者某个帮助行为所帮助的违法行为的具体情况无甚关联。所以，只要能够确定某次帮助或者某个帮助行为所帮助的是违法行为，即可将其计入危害性整体的量的评价，从而最终确定网络帮助行为的危害性。如此，既可使此类网络帮助行为在达到整体上巨量不法的情况下能够定罪，又不会完全脱离被帮助行为对网络帮助行为作单独评价。这也意味着，在设定“积量构罪”应达到的量的标准时，这个标准应当是很高的，需要达到能够危害网络管理秩序的程度。但是，如果能够确定被帮助的行为是违法有责行为，即构成违法有责意义上的犯罪，则入罪所需的帮助的量的标准应远低于“积量构罪”所要求的标准，因为在这两种情形下网络帮助行为所侵犯的法益不同，比如是网络管理秩序和财产权的差别，所以危害性严重与否的判断标准应有所不同。因此，在帮助信息网络犯罪活动罪和明知而提供程序、工具犯罪中，设定情节严重的标准时应当为“积量构罪”的情形设置单独的量的要求。

综上可知，在提供专门程序、工具犯罪的场合，可以对网络帮助行为作独立评价，即所谓帮助犯正犯化。在明知而提供程序、工具犯罪和帮助信息网络犯罪活动罪的场合，主观上应要求帮助者须对下游犯罪有明知，但不要求具备共同故意；客观上应要求对下游犯罪有一定程度的查实，所以这是对传统共犯理论的有限突破，但不属于帮助犯正犯化。

五、对应关系的验证

（一）统计方法说明

前文从司法判决中总结了网络帮助行为场合下“明知”要素和下游犯罪等情况的分布，并引发了后续的理论思考，最终构建了以网络帮助行为对下游犯罪实行行为的促进作用程

〔49〕 参见前引〔42〕，皮勇文，第 133 页以下。

〔50〕 即使是批判以正犯化方式处理网络帮助行为的学者，也肯定网络帮助行为的社会危害性高于一般的帮助行为。参见前引〔46〕，刘艳红文，第 22 页；前引〔2〕，张明楷文，第 8 页以下。

度为依据的网络帮助行为类型，并论述了这些网络帮助行为类型与犯罪类型之间的对应关系。那么，这种对应关系能否得到司法判决中实际情况的验证？对此进行验证，有两种思路：一是看在认定为某种犯罪类型的案件中，有多少属于该犯罪类型所对应的网络帮助行为类型，又有多少不属于。二是看在属于某类网络帮助行为的案件中，有多少被认定为该类网络帮助行为所对应的犯罪类型。由于本文提出的网络帮助行为类型涵盖的罪名超出了提供程序、工具罪和帮助信息网络犯罪活动罪，所以，若采取第二种思路，需要补充考察其他相关罪名案件的情况，才能掌握整体上网络帮助行为类型与犯罪类型的对应情况。为与前文的发现相对应，本文选择第一种思路，仅统计提供程序、工具罪和帮助信息网络犯罪活动罪案件的情况，统计样本是2018年9月17日之前公布的两罪案件一审判决书。

由于提供专门程序、工具犯罪和明知而提供程序、工具犯罪被规定在刑法中同一条同一款，从条文上不易区分，所以本文在确定案件的具体犯罪类型时，原则上看判决书的裁判部分是否写明“提供专门用于……的程序、工具”或者“明知……提供”；在语句表述不清时，则结合判决书对“明知”和下游犯罪查实程度的要求来确定。在确定犯罪类型后，对于某一被认定为提供专门程序、工具犯罪的案件，如果被定罪的网络帮助行为属于第一类网络帮助行为，则认为该案件的定罪符合网络帮助行为的类型划分；如果不属于第一类网络帮助行为，则认为不符合。据此统计提供专门程序、工具犯罪项下的所有案件中有多少符合、有多少不符合，并计算符合率。明知而提供程序、工具犯罪和帮助信息网络犯罪活动罪等场合的统计，与此同理。统计得出的情况如表3。

表3　网络帮助行为类型与犯罪类型的对应情况

法院认定的犯罪类型	案件总数	符合数	符合率
提供专门程序、工具犯罪	74	71	95.9%
明知而提供程序、工具犯罪	9	6	66.7%
提供程序、工具罪	83	77	92.8%
帮助信息网络犯罪活动罪	21	16	76.2%
整体情况	104	93	89.4%

（二）统计数据的意义

首先，总体上看，犯罪类型与网络帮助行为类型的对应关系很强，在提供程序、工具罪和帮助信息网络犯罪活动罪的案件中，犯罪类型与网络帮助行为类型的符合率达到了89.4%。也就是说，在大部分案件中，被认定为提供专门程序、工具犯罪的网络帮助行为属于第一类网络帮助行为，被认定为明知而提供程序、工具犯罪的网络帮助行为属于第二类网络帮助行为，而被认定为帮助信息网络犯罪活动罪的网络帮助行为属于第三类网络帮助行为，具体的符合率分别是95.9%、66.7%、76.2%。虽然明知而提供程序、工具犯罪案件的符合率较低，但不符合的案件只有3个，而且提供程序、工具罪案件整体上的符合率也达到了92.8%。

其次，统计数据说明司法实践中的犯罪类型认定需要网络帮助行为类型的指导。在提供程序、工具罪案件中，与网络帮助行为类型不对应的6个案件中，有3个案件的帮助者提

供的是通过自动切换 IP 地址来避开部分安保措施的帮助（即所谓秒拨类案件），这 3 个案件全部被认定为提供专门程序、工具犯罪。在提供程序、工具罪的全部 83 个案件中，共有 7 个是秒拨类案件，其中 4 个被认定为明知而提供程序、工具犯罪，3 个被认定为提供专门程序、工具犯罪。

由此可见秒拨类案件的犯罪类型认定在司法实践中有较大分歧。如果将“专门用于”解读为仅具有侵入、非法控制计算机信息系统的功能，而不具有其他正当功能，就容易将秒拨类案件中只是部分帮助实现侵入、非法控制计算机信息系统的功能的行为，按照提供木马程序等极大地帮助实现侵入、非法控制计算机信息系统的功能的行为同等对待。实践中，一部分法官看到，秒拨类帮助行为具有绕开监管的作用，使得安保措施部分失效，而这些功能都不是正当的，所以会认为秒拨类帮助行为具有专门性，从而认定案件为提供专门程序、工具犯罪。另一部分法官则看到，秒拨类帮助行为与提供木马程序不同，不会侵入或非法控制某个计算机信息系统，所以秒拨类帮助行为不是提供专门的程序、工具。

从对所帮助的下游犯罪实行行为的促进程度看，秒拨类帮助行为只是部分实现侵入、非法控制计算机信息系统的功能。一般而言，要侵入、非法控制计算机信息系统，需要避开安保措施，然后进入计算机信息系统获取数据或控制该系统。而秒拨类帮助行为只是实现了避开部分安保措施的目的，在该部分安保措施、防火墙限制等未被当作某一罪名的保护对象之前，秒拨类帮助行为并未极大地促进任何犯罪的实行行为，故不能被归入第一类网络帮助行为，而应当被归为第二类网络帮助行为。

再次，样本案件反映出司法实践关于“积量构罪”的尝试。虽然在 3 个案件中法官将秒拨类帮助行为界定为提供专门程序、工具犯罪，在定罪时既没有认定意思联络也没有查实下游犯罪，甚至没有去确定被帮助者是否实施了下游犯罪，但在这几个案件中，法官都考虑了如下因素：秒拨类帮助行为提供的帮助量（以人次为计算单位）非常大，涉及的案件金额也很大；秒拨类帮助行为不具有其他正当功能，为大量躲避监管的不法行为提供了帮助。这体现了司法实践中“积量构罪”的尝试，即当帮助行为的量较大时，秒拨类帮助行为就可能构成对网络管理秩序的破坏。

不过，这种尝试缺乏理论指导，还显得有些盲目和粗糙，存在不少问题。比如，在一个案件中，行为人提供的是绕开淘宝网站的某些安保措施实现自动抢拍的软件。〔51〕行为人的行为被认定为提供专门程序、工具犯罪，判决中给出的理由是行为人将该软件提供给很多用户，扰乱了淘宝网站正常的抢拍秩序。但有疑问的是，这种秩序是否属于刑法要保护的网络管理秩序。又如，在一个案件中，行为人提供的是可以绕开防火墙限制浏览境外网站的软件。〔52〕行为人的行为被认定为提供专门程序、工具犯罪，理由是这种帮助行为可以让很多人绕开防火墙，妨碍国家的网络监管秩序。同样有疑问的是，这种防火墙限制是否属于刑法要保护的网络管理秩序。这些问题都有待进一步研究。

最后，样本案件显示帮助信息网络犯罪活动罪有被宽泛解释的情况，应当根据第三类网络帮助行为的标准，明确该罪所指帮助行为的界限和帮助行为在量上的要求。考察帮助

〔51〕 参见河南省郑州市金水区人民法院（2017）豫 0105 刑初 1616 号刑事判决书。
〔52〕 参见广东省东莞市第一人民法院（2017）粤 1971 刑初 250 号刑事判决书。

信息网络犯罪活动罪案件中与网络帮助行为类型不对应的5个案件发现，其中4个案件中的帮助行为是建设用于诈骗的虚假彩票、虚假经营网站或游戏。这些帮助行为应属第二类网络帮助行为，而不应认定为与第三类网络帮助行为相对应的帮助信息网络犯罪活动罪。仔细阅读判决书可以发现，这4个案件之所以会被认定为帮助信息网络犯罪活动罪，而不是明知而提供程序、工具犯罪，很可能是因为在这4个案件中提供的帮助都不是帮助实现侵入、非法控制计算机信息系统，故无法认定为明知而提供程序、工具犯罪，而帮助信息网络犯罪活动罪可以被解释得很宽泛，把第一、二类网络帮助行为也包括进来。然而，长此以往，会把本来应当被归为第一、二类网络帮助行为，其独立性、危害性均大于第三类网络帮助行为的网络帮助行为以帮助信息网络犯罪活动罪来定罪；同时也会将帮助信息网络犯罪活动罪对帮助的量的要求降低，从而使得那些属于第三类网络帮助行为，只是在下游犯罪实施的前后期阶段提供帮助，所具有的独立性、危害性均小于第一、二类网络帮助行为的网络帮助行为，按照与以帮助信息网络犯罪活动罪定罪的第一、二类网络帮助行为相同的帮助的量的标准来定罪，而这并不符合罪责刑相适应原则的基本要求。比如在一个案件中，提供帮助者仅提供1人次的微信支付帮助，仅获利3400元，就被认定构成帮助信息网络犯罪活动罪。〔53〕这再次表明，急需明确成立帮助信息网络犯罪活动罪对帮助的量的要求。

结　论

本文从现有理论的争议点出发（如对“明知”要素和下游犯罪查实程度的不同要求），将其形式化为具体表现（如是否有意思联络、被帮助者是否明确等），并根据这些差异总结、归纳司法判决，以判断司法实践的现实状况是否符合理论设想、符合怎样的理论设想，从而对理论进行验证。在现有理论无法解释司法实践状况时，立足于司法判决，以不同犯罪类型项下判决所具有的不同类特征来启发关于不同犯罪类型之间联系与区别的理论讨论，并提出自己的理论方案。

从司法判决中发现不同犯罪类型项下判决所具有的类特征，需要不断往返于不同犯罪类型项下的不同判决，发现同一犯罪类型项下判决之间的相同点，并且这种相同点是其他犯罪类型项下判决通常不具有的；然后，将这些相同点进行量上的比较，最终发现同一犯罪类型项下判决通常具有而其他犯罪类型项下判决通常不具有的类特征，从而能够较好地将该犯罪类型项下判决与其他犯罪类型项下判决区分开来。

对于这种类特征，还需要确定其是否具有稳定的区分作用，而不是偶然的发现。经过本文的理论抽象发现，网络帮助行为对下游犯罪实行行为的促进作用程度是具有稳定区分作用的类特征，而且该特征与网络帮助行为的危害性、独立性直接相关。

但是，上述分类仍然是一种事实性分类，只有将这种分类涵摄进刑法规定的相应犯罪类型，这种分类才具有法律规范意义。所以，应当考察这种分类与刑法规定的犯罪类型之间是否存在对应关系，以及这种对应关系能否得到刑法解释和罪责刑相适应原则的支持。对事实性分类的法律规范意义的讨论，可以启发对刑法相关规定的理论讨论，帮助发现其

〔53〕 参见江苏省徐州市云龙区人民法院（2017）苏0303刑初369号刑事判决书。

他潜在的合理解释路径。

本文的研究方法不同于以往刑法学界的相关研究。之前多数学者运用刑法学的相关理论、学说，通过理论阐释和逻辑推理来研讨、解决相关问题。本文则是在理论阐释、逻辑推理不足以厘清纷争、解决难题的情况下，采用对司法判决进行归纳、总结的方法，最终建立起具有法律规范意义的理论分类。如此提出的分类方案既能较好地解释司法实践状况，又能从理论层面论证分类的正当性和稳定性，从而实现司法实践与理论的对话与互动。

Abstract: Analysis of written judgments indicates that, in judicial practice relating to cybercrime aiding activities, attention has been focused on the chaotic standards on the aided crimes and the *mens rea* of the act of aiding the crime, as well as the *actus reus* of the aiders. Acts of providing aid for cybercrimes can be categorized according to such criteria as their harmfulness and independency, and convicted according to corresponding standards. The completion degree of the *actus reus* of the aided cybercrimes is directly related to the harmfulness and independency of the aiding activities. According to the completion degree, acts of providing aid for cybercrimes can be categorized into three types: aiding substantial part of the *actus reus* of cybercrimes; aiding some part of the *actus reus*; and aiding in the preparation for the crime or at the late stage of the crime. The first type corresponds to the act of providing programs or tools for the commission of the crime of hacking into or illegally controlling a computer information system. The second type corresponds to the act of knowingly providing programs or tools to a person who is about to commit the crime of hacking into or illegally controlling a computer information system. The third type corresponds to the act of providing aid for the commission of information network crime. The above relations of correspondence are supported by textual interpretation, legislative and judicial intentions, characteristics of cyber programs, and the harmfulness of the aiding activities. The first type can independently evaluate the harmfulness of the crime, while the second and the third types require the ascertainment of the act of knowingly aiding a crime and the illegality of the aided crimes. The act of providing aid for large number of activities that have only small harms individually or cannot be convicted as a crime can be evaluated as the second or the third type.

Key Words: providing aid for the commission of cybercrimes, providing programs or tools for the commission of the crime of hacking into or illegally controlling a computer information system, providing aid for commission of information network crime, *mens rea*