第20卷第2期 上海财经大学学报 Vol. 20 No. 2
2018年4月 Journal of Shanghai University of Finance and Economics Apr. 2018

DOI: 10.16538/j.cnki.jsufe.2018.02.009

利用信息网络犯罪行为二元形态的教义解读

陈 伟[1], 熊 波[2]

(1.西南政法大学 法学院,重庆 401120; 2.西南政法大学 青少年犯罪研究中心,重庆 401120)

摘 要: 设置非法利用信息网络罪的部分前置预防行为,以此应对网络风险社会的虚拟性、技术超越性以及秩序的涉众性,是网络信息时代的背景所需。非法利用信息网络罪不应全盘定性为预备行为正犯化,从刑法规范的精确用语角度分析,利用信息网络犯罪的行为形态存在着"预备行为正犯化"以及"纯粹的实行行为"的二元定性标准。在利用信息网络犯罪行为形态二元论的基本指引下,设立的"网站"应当包括"三网融合"下的空间类型;发布的"信息"评价应当从"时间、性质、类型"的多元维度予以规范诠释。

关键词: 非法利用信息网络罪;网络风险社会;预备行为正犯化;纯粹的实行行为

中图分类号: DF792.7 **文献标识码:** A **文章编号:** 1009-0150(2018)02-0125-14

一、问题的引出

如同电气化作为工业时代之端倪一般,网络化是信息时代的标志。网络技术的革新与发展,释放出"潘多拉魔盒"式的幻想与乌云,网络信息时代的收益与弊端呈现出等同的发展趋势。在利用信息网络助益人类生产、生活之际,网络风险社会演变出其独特的性质,空间虚拟性、技术超越性以及对象涉众性已然成为网络信息时代的特有标签。"法律、规范、市场和代码(Code)",被喻为现实社会中规范人类行为的四种工具与价值类型,具有不可比拟的优越性。[①]借此,网络犯罪将行为的隐匿平台悄然转换为一种工具性的价值利用,非法利用信息网络罪契合"人类市场运作中代码工具的非法利用"的行为规范。有别于网络对象犯罪,[②]非法利用信息网络罪作为一种网络工具犯罪,罪名识别的关键在于立足网络工具的社会背景,追本溯源,考究网络时代社会下的工具特质,揭示传统刑法体系的文本滞后、技术性规范缺失以及风险规划格式化,以此解构信息网络利用型犯罪形态的刑法应对之策略。

非法利用信息网络罪中掺杂的技术变革,戕害着法益保护的行为规范目的价值以及客观归责的因果关系判断。诚然,网络空间相较于现实社会,其自身所具有的诱惑力、优越感作为网络风险社会的显著特征,促使部分人群铤而走险,谋求最大化的非法利益,进而诱发网络工

收稿日期: 2017-10-16

基金项目: 国家社会科学基金项目"刑罚退出机制的价值确立与实践运行研究"(17XFX009);中国法学会2017年度部级法学研究课题"侵犯公民个人信息罪司法实证研究"(CLS(2017)C24)。

作者简介: 陈 伟(1978－),男,湖北宜昌人,西南政法大学法学院教授、博士生导师;
熊 波(1992－),男,江西南昌人,西南政法大学法学院助理研究员,西南政法大学青少年犯罪研究中心研究人员。

①参见[美]理查德·斯皮内洛:《铁笼,还是乌托邦——网络空间的道德与法律》,李伦等译,北京大学出版社2007年版,第2页。

②网络对象犯罪是一种网络信息时代发展阶段的萌芽形态,诸如非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪、非法控制计算机信息系统罪以及扰乱无线电通讯管理秩序罪等罪名。

具犯罪新类型的衍生。但这并非是行为主体无法自我管控，所导致的预备行为可罚性现实评价的降低因素。[①]对此种潜在现象蔓延的遏制，一方面，在于行为人的内心风险识别能力以及自我约束水平的提升；另一方面，则仍需依赖刑法立法规范技巧的运用以及风险预期能力的规范操作。不可否认，非法利用信息网络罪是在网络风险社会的法益模糊化背景下孕育而生的，本身具有预备行为正犯化的一般预防之功效。但是，行为性质的规范定位以及行为要素的教义阐释，仍在于刑事立法规范的精确解读。从《刑法》第287条之一的条款编排来看，非法利用信息网络罪还显露出纯粹实行行为的设置模式。利用信息网络犯罪“预备行为正犯化”以及“纯粹的实行行为”的二元形态定性标准之证成，有益于化解行为立法罪状的正犯行为依托化的视角局限，彰显“设立”、“发布”行为规范要素的独立性、双重性以及关联性。

二、行为背景：网络风险社会的本体考察与积极应对

非法利用信息网络罪“预备行为正犯化”以及“纯粹的实行行为”二元形态定性标准的规范构建，是在网络风险社会背景下行为周全囊括的必要范式。“应当承认，在风险社会语境下，国家行为的预防走向对整个公法体系造成了重大的激荡与冲击，不管是刑法、行政法还是宪法，都遇到了自身无法应对的问题，但无论如何，只有将社会的预防现象纳入教义学体系之内，对其进行适当的规制才有可能”。[②]对此，风险社会的预防现象来源于具体环境与氛围的本体论考究。非法利用信息网络罪的二元定性标准的基本规范，能够在网络风险社会的本体特性中探寻其遁足之地。

（一）本体考察：技术变革助推刑法解构

网络风险社会的本体论考察与犯罪构成的本身存在形式的特性问题研究不谋而合，都旨在强调一种“区分”的理论分析工具。[③]不同于其他具体社会情境类型下的行为构造，网络风险社会背景下利用信息网络的犯罪行为具备较强的体系模糊性、技术分析性以及危害后果社会性。非法利用信息网络罪“预备行为正犯化”的属性是网络风险社会现象特殊预防的精准定位，也是利用信息网络犯罪行为的体系模糊性、技术分析性的必然遵循；但是，透过现象看本质，网络风险社会的具体语境探究，无法脱离一般社会的普适化结构而另辟蹊径。正如美国著名社会学家默顿所言：“社会的隐功能（latent functions），即具有某种或者某些意外结果，有助于维系所探讨的技术实践的持续再生产、再完善；而这一理性的本源还在于社会的显功能（manifest functions），即一般社会的行为形态或者模式。为具体社会场合的初步认识提供周期性的解释思路。”[④]非法利用信息网络犯罪“纯粹的实行行为”的价值定位，正是对一般社会的行为刑事违法性的积极评价。

如此一来，预备行为正犯化亦是考虑网络风险社会的诸多复杂因素后的理性选择，将网络信息时代的技术变革充分适配于刑法的体系构建之中。诸如，非法利用信息网络罪中“为实施诈骗等违法犯罪活动发布信息的”以及“设立用于传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组”等类似行为；再如，非法侵入计算机信息系统罪中对于国家事务、国防建设、尖端科学技术领域这三类特定的计算机信息系统的规定。由此可知，预备行为正犯化的立法趋势被广泛运用于潜在社会危害性的犯罪领域。而这一潜在的危险评价，

①[德]梅尔：《德国观念论与惩罚的概念》，知识产权出版社2015年版，第81页。

②劳东燕：《风险社会中的刑法：社会转型与刑法理念的变迁》，北京大学出版社2015年版，第71页。

③参见冯亚东：《犯罪构成本体论》，《中国法学》2007年第4期。

④Merton P K, Manifest and latent functions. Social Theory and Social Structure,Glencoe:Free Press ,1963：51.

正是基于“该行为一旦进一步实施或者实施完毕，其危害性将变得极为严重，其危害后果可能是难以预测、无法评估和难以挽回的”。[①]

然而，与此同时，我们无法忽视网络信息时代技术变革自身所带来的显性危害。对于单纯利用信息网络平台、空间，传播、发布招嫖、销售假证、假发票、赌博传销等违法犯罪信息；或者假借通过发布低价机票、旅游产品、保健品等商品信息，吸引他人购买，实则实施诈骗、传销手段的犯罪手段等纯粹实行行为，在网络犯罪侦查手段滞后于新兴技术变革的当下阶段，单纯将非法利用信息网络罪认定为一种“预备行为正犯化”，势必大大限缩罪名设置的科学性与现实性。因而，非法利用信息网络罪“纯粹的实行行为”的犯罪形态建立，也正是考虑网络风险社会的科技性规则，将网络信息时代的技术变革运用于网络刑法体系的应对方向、内容架构以及话语衔接之中。

其一，网络空间的虚拟性作为技术变革的现实映衬，形态的二元构建存留于双层空间。传统工业技艺被新型科技创新所取代，进而人类运用信息网络技术在现实社会之外，创建另一个维度物化场域——网络空间。网络空间的内部构造并非由真实、客观的物质组成，而是由信息数据库、信息通讯体系以及信息运输线路的电子数字分离组合而成。电子数字的分离组合形成不同的代码，因而不同的局域网形成区划的网络空间。[②]代码作为网络空间存留的数字信息，表现形式通常为“字符、源电子、信号”，且它们最为显著的特征便是不可视性与虚化性。在网络信息时代渐趋成熟的现阶段，网络的普及应用形成了网络空间和现实空间并存的局面，在计算机网络的虚拟空间中，不仅参与者的身份是隐匿的，网络空间也是虚拟的。[③]在此种虚幻的空间境况下，一味要求按照行为既遂模式的现实危害来认定信息网络利用行为的刑事可罚性，无法体现法益保护主义下客观的行为违法性与实质的罪责评价基准。

非法利用信息网络罪的预备行为正犯化，将网络虚拟空间下抽象危害的法益实质威胁评价在规范设置的模式之中，克服上述行为刑事违法性评价的法益模糊之弊端。预备行为正犯化的立法依据在于“修正的犯罪构成”，将构成要件符合性中的危害结果或者社会危害性进行抽象化或者实质化，以寻求形式的教义评价机制和实质的法益侵害根据。但是，修正的犯罪构成毕竟仅是基本犯罪构成理念的辅助与补充，网络信息时代作为现实社会的冰山一隅，基本犯罪构成应当作为非法利用信息网络罪的主要认定模式，即将利用网络空间虚拟性进行的犯罪行为认定为一种纯粹的客观、独立之样态，而并非仅局限于罪名行为要素的预备阶段之评断。在网络空间物理边界极度虚化的情形下，网络风险社会形成的最根本原因在于个体利益保障和公共利益维护的两端割裂，对公共利益的极力推崇以及对个体利益的片面追求，打破了实践发展过程中的自由提升和风险扩张之间的相对平衡状态，因而网络风险被极端地诱发。[④]在这种观点推导下，预备行为正犯化被视为一种网络社会中公共利益的极端化立法的制度产物，而纯粹实行行为的模式构建，是网络虚拟空间中沟通个体利益和公共利益两者之间的桥梁与纽带。

其二，网络技术的超越性作为技术变革的前进趋势，形态的二元构建具备规制的前瞻性。科学技术本身历经了不断研发、渐趋复杂化的发展过程，技术变革在先进技术的基础上汇聚前沿尖端科技，不断实现技术的超越，助推人类改造客观现实的能力与水平的提升。伴随着新能源技术的供给、生物技术的充沛、信息技术的高效以及海洋开发技术的开拓，网络技术的超越

①于志刚：《网络犯罪与中国刑法应对》，《中国社会科学》2010年第3期。

②参见许秀中：《网络与网络犯罪》，中信出版社2003年版，第4页。

③任彦君：《犯罪的网络异化与治理研究》，中国政法大学出版社2017年版，第10页。

④庄友刚：《跨越风险社会——风险社会的历史唯物主义研究》，人民出版社2008年版，第12页。

性在诸多新领域中得以展现。在传统刑法体系对犯罪行为形态认定呈现出单一化、滞后化以及平面化的程序规则之际，网络技术的超越性正在瓦解刑事法律防控模式构建，立法者逐渐将视角转向法律与技术鸿沟的化解与应对机制的塑造。网络技术的超越性致使刑事法规则无法及时化解网络工具犯罪行为的隐秘性以及潜在性，从而技术本位的思维理念灌输于刑事法规则的创建之中。[①]刑法作为网络犯罪行为模式认定的依据，非法利用信息网络罪二元形态的理念奠基，既是刑法规则教义解读的实然路径，更是技术变革超越性中规则前瞻性的应有之义。

非法利用信息网络罪作为一种网络工具型犯罪，其最为体现网络技术超越的前进方向，“技术反制技术”从而诱发网络犯罪的形态多样化现象已经是屡见不鲜。非法利用信息网络罪预备行为的规制，将实质的、未然的社会危害性消解在启蒙阶段，赋予刑事立法前瞻性规则。值得注意的是，在网络虚拟空间下，非法利用信息网络罪的“设立”“发布”行为虽极具模糊性和隐蔽性，但并不排斥刑法谦抑性原则。换言之，非法利用信息网络罪的前瞻“触角”无法涉及生活中的方方面面。对于公共利益“设立”“发布”的利用型网络工具犯罪，预备行为正犯化具备其现实基础；而对于涉及个体利益的非法利用信息网络犯罪行为要素的具体认定，则必须回归“纯粹的实行行为”的形态定位标准，明确利用型网络工具犯罪“着手”的判断形式，以便在基本人权保障与网络风险的潜在危险防控中，对技术变革超越性的前瞻规则设置，把握“度”与“量”的程序操作。

其三，网络秩序的涉众性作为技术变革的危害评价，形态的二元构建对应多元行为防范。网络空间的虚拟性以及新兴技术的超越性之所以值得刑法评价，不仅在于网络利用行为的个人利益侵犯，更为重要的是行为造就危害结果的涉众性评价。民众社会焦虑感的骤升，一方面来源于网络风险社会中诸多不确定性因素的存在；另一方面则是网络空间中社会秩序的妨害，更多地在于违法犯罪行为的“牵一发而动全身”的影响程度。网络信息时代的技术变革服务于人民大众，同时也广泛深入地牵制着群众的行为举止。应当明晰，信息网络的利用行为并非是一个固化的、单一维度的形式存在。正如有的学者评论道：“对网络犯罪客观要件的理解，不能简单地认为是某种单独的行为，而应当是若干行为的集合。”[②]因而，当前刑法体系在面对网络犯罪行为多元模式的客观处境下，应当将行为样态的评定，结合网络秩序的涉众性危害评价予以同步进行。

非法利用信息网络犯罪行为形态的二元教义阐释在涉众性危害结果的实质评价中，应当明确予以区分。首先，涉众性危害结果管控的形式要求，尽可能将预备行为正犯化包容的所有行为模式予以涵盖。对于“设立”“发布”关联的行为，在不违背罪刑法定基本原则的情形下，利用扩大解释等实质刑法观，将涉及的行为危害予以防控。其次，多元的行为模式构建要求，审慎对待预备行为正犯化中抽象危害的实质认定。[③]基于目前司法实践中预备行为不值得处罚或者并无犯罪化评价必要性的刑事政策存在，非法利用信息网络罪中预备行为正犯化的限制幅度可以从两方面予以考量：第一，危害结果的牵涉对象，将法益保护主义的侵犯仅局限于公共利益妨害的不法层面；第二，行为模式的具体要素，将行为构成要件的形态认定仅局限于“设立”“发布”以及与其具备关联性的行为，不可借用类推解释肆意扩张法益保护原则的范围。最后，纯粹的实行行为的理念主张应当予以适度扩大化，将利用信息网络犯罪的现实危害进行教

①具体如何在刑事法规则中构建技术性规则，以弥补法律程序中的技术鸿沟，笔者在下文将会予以详细阐述，此处便不再赘述。

②刘品新：《网络法学》，中国人民大学出版社2009年版，第121页。

③陈伟、熊波：《审慎认定“持有型”侵犯公民个人信息罪》，载《检察日报》2017年9月20日，第003版。

义确立。防止法益概念的实体内容在网络风险社会的焦虑维度下，日趋模糊与单薄。因而，在非法利用信息网络罪的纯粹实行行为的价值倡导下，超个人法益的纯观念化产物应当明确禁止。

（二）积极应对：弥补法律设置的技术鸿沟

鉴于当前网络犯罪行为的高发与多态，网络刑法体系构建应坚守“技术本位”还是“规则本位”，抑或是单设特殊网络刑法还是注重刑法模式的话语规则运用，刑法学界对此争论不休。不容置疑，利用信息网络犯罪行为形态的认定应当冀希于刑法规范的教义疏通，从形式刑法观到实质刑法观的工具合理性证成，最为基本的便是对刑法条文的字面规定进行理性解读。单设特殊的网络刑法是对网络风险社会的一种过激反映，仅凭借网络信息时代的技术超越以及物质虚拟，而割裂网络社会归依于现实社会的一般属性，既凸显刑事立法的冗杂，又导致网络犯罪行为认定的泛化。诚如，“网络犯罪与现行刑法规定的各种犯罪并没有明确的界限，换言之，由于网络空间逐渐和现实空间相互交织甚至难解难分，网络犯罪与传统犯罪便融合在一起”。[①]笔者认为，面对信息网络工具犯罪的预备行为可罚性认定的扩张趋势，刑事立法应当注重技术程序规则的构建，弥补法律设置的技术鸿沟，而并非一味强调网络犯罪形态认知的特殊化。

对于非法利用信息网络犯罪行为形态认定依据的技术规则设置，同样应当遵照“预备行为正犯化的限缩以及实行行为的扩展”这一理性基准。因而，技术规则的鸿沟填补，势必考察网络犯罪导致的诸多新领域的抽象危害以及潜在威胁，同时应当灵敏感应到网络工具犯罪的新环境变化，紧密围绕刑事法领域罪责追诉的新问题进行展开。此外，尤为重要的是，技术规则的设置应当立足复杂行为的多元模态以及全球化的角度分析，来看待信息网络时代的行为特征与传统社会法律行为规则的属性对立。[②]亦即，用实行行为构成要件的技术规范视角来主导并偏正抽象行为危害的前置预防，以期聚焦技术规则的综合效应，缓冲风险规制的焦虑现象。对此，可以从如下三个方面具体把握信息时代下网络工具犯罪的技术规则的设置要求：

第一，技术规范设置的比例性原则。网络犯罪的技术规范在刑事立法中的体现，不同于“规则本位”下的行为话语，前者更为突出文本的技术含量。[③]“技术规范作为一种规范的构成要件要素，需要我们借助感官、精神以及经验知识的具体理解，才能获知其涵盖的内容要素”。[④]由于法官个人感知具有较大的差异性，对技术规范的具体把握和分析通常在时刻变化。因而，首先承认，这种主观评断造就的客观迥异无法避免，对于非法利用信息网络犯罪行为形态的技术参考，应当遵循预备行为风险防御的比例性原则。

预备行为风险的比例性原则要求充分考虑网络信息时代风险社会中利用行为的特点，根据风险辐射的对象、范围以及舆情等因素进行判断。在利益权衡与风险规划的综合考察基础上，决定网络利用预备行为的正犯化分析是否符合利益与风险的比例关系，进而判定预备行为的特定要素是否有必要动用实行行为的可罚性理论评价，对此加以规制以及规制范围的大小。[⑤]技术规范的比例性原则在刑事法的网络风险的防控运用中，具备一定的时代价值。正如张明楷教授评论道：“遵循比例性原则是法益保护主义的时代衡量，应当注重从法益的侵犯性、刑法的补充性以及法益的权衡性予以体现。”[⑥]

①张明楷：《网络时代的刑事立法》，《法律科学》2017年第3期。

②[德]乌尔里希·齐白：《全球风险社会与信息社会中的刑法》，周遵友、江溯译，中国法制出版社2012年版，第13页。

③诸如，《刑法修正案（九）》新增的帮助信息网络犯罪活动罪的“互联网接入”“服务器托管”；再如，《刑法》第288条扰乱无线电通讯管理秩序罪中的“无线电频率”等。

④C.Roxin，Strafrecht Allgemeiner Teil，Band I，4.Aufl.，C.H.Beck，2006，S.308.

⑤参见郝艳兵：《风险刑法：以危险犯为中心的展开》，中国政法大学出版社2012年版，第72页。

⑥张明楷：《法益保护与比例原则》，《中国社会科学》2017年第7期。

第二，技术规范中被允许危险原则。虽说技术规范的合理设置是信息网络社会风险应对的时代必然，但并不意味着技术规范的设置必然遵从网络犯罪行为的“为现象立法”之论断。诚然，网络犯罪学的行为与技术研究为网络刑法学提供了更为深层次的教义反思，网络犯罪预备行为可罚性的本质仍在于刑法制度调节的领域，应当明显较其他规范触及的范围更为狭窄。亦然，技术规范可以包容被允许的网络危险存在。譬如，为推动电商发展，而被允许的网络平台的夸大宣传行为；为侦破特殊性质案件而搭建的网络秘密侦查技术平台的行为等等，上述信息网络的预备利用行为，亦需被纳入技术规范应当考量的被允许危险的范畴。

值得强调，这一原则的规范倡导并不同于上述的比例性原则之构建，比例性原则重在突出所有预备行为类型“度与量”的统一规制；而被允许的危险原则旨在划分出预备行为的特殊类型，在现实社会的行为体系中，具体权衡值得刑罚处罚的预备行为正犯化的种类。简言之，技术规范的被允许的危险原则是在比例性原则的基础和前提之上，另辟蹊径探寻特殊预备行为种类的可罚性来源。被允许的危险建立在注意义务的实施可能性基础之上，因而在该种情形下，即使预备行为具备严重侵害法益结果的危险或结果存在，也应当否决行为的刑事违法性。“被允许的危险问题具有作为实质违法性的具体现象一面的意义”，[①]同理，非法利用信息网络纯粹实行行为的刑罚可罚性的类型评价，也应当摒弃现象立法的“一览无遗”。

第三，技术规范编排的类型化原则。刑法立法的行为方式界定无法一应俱全，出于立法的精简和明确，不可将网络技术的专业术语一成不变地照搬于非法利用信息网络罪的行为对象描述之中。因而，唯有依靠技术规范编排的类型化原则，方可化解预备利用行为的非类型化技术构造致其范围评价的不确定性，以及由此演化而来的预备行为实行化处罚幅度的越轨。当前各国法域预备行为独立评价之窘境在所难免，[②]技术规则的明确运用，赋予司法实践中行为认定的实质依据以及规范定型化。网络时代的技术超越性以及风险社会中新型化因素干扰，要求刑法的技术规范构建充分考虑社会生活的涵盖性和适应性。法律条文的明确性与类型性，一来为非法利用信息网络罪的预备行为认定提供必要的限度；二来为利用行为本身的纯粹实行行为的补充指引明定方向。

其实，技术规范的类型化立法已然成为刑法修订的焦点之一。例如，非法利用信息网络罪的设立对象“网站、通讯群组”；扰乱无线电通讯管理秩序罪的媒介“无线电台（站）”等，由此可知，引申出技术规范类型化设置的稳定性是尤为必要的，“稳定性”强调技术规范作为一种立法确立，不能动辄就朝令夕改，否则便丧失其应有的权威性和确定性。[③]因而，技术规则的设置作为立法修订的方向之一，无论是罪名增设中体现的技术规范，还是行为方式与行为对象描述的技术规范，都应当疏通刑事立法类型化原则的适用。[④]

三、行为定性：预备行为正犯化与纯粹的实行行为

非法利用信息网络罪的行为形态究竟如何界定，不能凭空依据个人感官随意认知，亦不能刻意追求司法实践的便捷操作而轻易划定。犯罪形态的升华和总结应当实现法秩序的安宁与实质正义价值的和谐统一，对于非法利用信息网络罪的行为形态定性，注重规范文本的教义考察以及实现事实经验的实质解释，是其唯一的范式操作。而具体的内容理解则可以尝试“从规

①[日]大塚仁：《刑法概说（总论）》，中国人民大学出版社2009年版，第350页。

②[日]日高义博：《刑法总论》，成文堂2015年版，第408页。

③ 参见卢建平、姜瀛：《犯罪“网络异化”与刑法应对模式》，《人民检察》2014年第3期。

④参见张明楷：《网络时代的刑事立法》，《法律科学》2017年第3期。

范中来”以及“到规范中去”这两个方面循序渐进。

首先,“从规范中来”明确要求将“规范”作为解决实际问题的落脚点。刑法权威的塑造和确立来源于其预定的行为指引,并为形态理论的证立或裁判结论的得出,提供依据、框架和基础。《刑法》第287条之一规定的设立型信息网络利用行为冠以“设立用于实施”,以及发布型信息网络利用行为冠以“为实施诈骗等违法犯罪活动发布”,以此表明此处预备利用行为的正犯化的立法处断;而发布型信息网络利用的另一性质行为则借以“发布有关制作和销售信息”,来论证纯粹的实行行为模式的立法明定。综上,立足行为的教义解读,显而易见非法利用信息网络罪的行为形态呈现,并非目前刑法学界一贯予以支持的“预备行为正犯化”单一标准样态,[①]而是“预备行为正犯化”以及“纯粹的实行行为”的二元定性标准。

其次,“到规范中去”意指结论合理性评价最终以“规范”作为证立的依据。行为形态的二元论考究并不强化严守文本规范的形式理解,在教义解读过程中,法安定性的实质内涵与价值容量,可以借助经验事实与价值判断予以填充。从行为教义学的原理阐释,网络风险社会治理的经验事实警示利用信息网络行为的前置预防具有一定的时代性和必要性,本文并不否定预备行为正犯化的规范设置,既然立法将某种特定的预备行为作为一种独立的构成要件予以区分对待的话,那么该预备行为的可罚性可能就是正当的。[②]然而,出于犯罪化渐趋退出机制的倡导以及刑罚惩治的机能转换,理性的立法者应当游弋于对规范体系性的坚守与政策指引之间,极力限制预备行为正犯化的扩张,适度扩充纯粹实行行为的认定,以达到司法效率预期效果的最大化和最优化。

（一）预备行为正犯化:“用于”实施违法犯罪的认定

非法利用信息网络罪的部分构成要件之所以被称为“预备行为的正犯化”,主要在于“用于”实施违法犯罪的分则规范界定。其实,“为实施诈骗等违法犯罪活动发布信息的”同样是“用于”实施违法犯罪框架内的内容要素,即发布信息用于实施诈骗等违法犯罪活动的。鉴于此,笔者将《刑法》第287条之一的两项“用于”实施违法犯罪的规定,统一评价为预备行为正犯化。不同于刑法总则设置的一般性、抽象性以及形式性的预备行为的文本规定,非法利用信息网络罪的独立预备行为的构成要件,作为特定罪名的一种转化型实行行为,其已然强化未来预备行为的犯罪化应然情势。

综观各国预备行为的设置体例,当代刑法预备行为制度已初步形成共识与基准:世界主要法域的立法格局遵循从预备犯的刑事可罚性、处罚范围、处罚模式三方面进行全方位限缩,法国刑法全面切断预备犯处罚的教义来源,或德日刑法原则上不处罚预备犯,仅仅出于有效保护重大法益的刑事政策考虑,例外地处罚预备犯。[③]我国《刑法》第22条对犯罪预备的范式进行了界定,即“为了犯罪,准备工具、制造条件”的是预备行为。为顺应预备行为处罚的趋势和潮流,笔者认为,《刑法》第22条是对犯罪行为预备阶段的认可,而并非一概认为只要符合预备阶段“准备工具”和“制造条件”的行为表征,即作为预备犯进行看待。[④]质言之,该条的犯罪预备仅是

①对非法利用信息网络罪的形态认定持“预备行为正犯化”单一标准的观点论述,可参见张明楷:《刑法学》,法律出版社2016年版,第1051页;此外,周光权教授认为非法利用信息网络罪的客观方面表现为为实施其他违法犯罪活动而进行的各类准备的预备行为,并作为立法体例上“拟制的正犯”。参见周光权:《刑法各论》,中国人民大学出版社2016年版,第355页。诸如此类的观点还有沈德咏:《〈刑法修正案(九)〉条文及配套司法解释理解与适用》,人民法院出版社2015年版,第265页。

②参见[德]恩施特·贝林:《构成要件理论》,王安异译,中国人民公安大学出版社2006年版,第179页。

③详情可参见《最新法国刑法典》,朱琳译,法律出版社2016年版,第134页;[德]乌尔斯·金德霍伊泽尔:《刑法总论教科书》,蔡桂生译,北京大学出版社2015年版,第461页;[日]大谷实:《刑法总论讲义》,黎宏译,中国人民大学出版社2008年版,第312页。

④这一合理论断的得出,亦可从《刑法》第13条“但书”中情节程度所对应的社会危害性的认定与要求中予以实现。

从刑事违法性层面对预备行为的含义予以界定，而并非指犯罪构成要件模式的预备犯罪。因而，基于非法利用信息网络罪中的部分实行行为具备行为预备的特征，为防止其辐射面的扩张，因而有必要从预备条件符合性、阶段性以及对象判断进行限制。

1. 预备条件的具体符合

基于本文的主题定位，非法利用信息网络罪的实行行为条件的具体符合，应当遵照《刑法》第22条的规范践行教义解读，以此为司法实践审慎对待非法利用信息网络罪的预备行为正犯化的认定提供参考。

其一，“为了犯罪”强调犯罪目的与预备行为的对应性。预备行为的转化不同于纯粹实行行为，由于犯罪前期行为的互通性，预备行为的主观条件一旦符合，则较易认定为某种特定预备犯。在预备行为正犯化的构成要件中，则轻易满足构成要件的不法和有责。如伺机蹲点、紧密尾随以及购买作案工具，可以被定性为故意杀人罪、抢劫罪、盗窃罪等各类罪名的预备行为。因而，强化非法利用信息网络罪的犯罪目的与客观行为的直接对接性，意在规范非法预备利用行为的司法认定。具言之，如果信息网络利用行为人主观上根本不存在后续“实施违法犯罪活动”这一主观目的，或者虽然具备此种主观目的，但发布的网络信息和设立的网络平台行为，根本无法触发后续的诈骗、传授犯罪方法、制作销售违禁物品等犯罪活动的发生，此时，都不得判定其作为非法利用信息网路罪的预备行为正犯化情形。

其二，“准备工具”必须限定为直接的工具准备行为。预备行为中的行为类型的认定是罪责适配的客观依据，理性化的科技发展滋生与促成了风险行为的不确定性，因而，非法利用信息网络罪的“准备工具”的评价较易发生道义偏离和肆意扩张。作为自然行为学派的奠基人李斯特认为：“行为是可以归咎于自然人意志的，使外部世界发生变化的一种任意性举动……并且这种变化或者一种结果是罪责承担的原因或者非阻碍因素。”[①]网络风险社会中行为的复杂性以及潜伏性自然不言而喻，因此设置特定预备行为形态的正犯化具有一定的合理性。但考虑到刑法作为一种“后盾法”的保障工具，非法利用信息网络罪中的准备工具型的利用行为应当限定为一种直接的信息网络利用的预备，而不包括准备工具的预备。譬如，设立的用于诸如诈骗、传授犯罪方法等违法犯罪活动的网站和通讯群组的行为本身就是一种“准备工具”的预备行为，因而，为设立网站和通讯群组的购买材料、学习网络技术等预备行为则不具备刑事处罚性。

其三，“制造条件”不具备预备利用行为的具体模式。对于网络风险社会中法益保护的模糊和扩大，德国刑法学界认为信息网络技术的发展使得行为界限模糊，并且各异行为方式的实现得以可能。[②]因而，在网络工具犯罪领域中，预备行为的“准备工具”和“制造条件”难以有一种明确的界分方法。[③]诸如，云端信息平台在特殊储存环境下，其具备虚拟操作交互性、信息高度聚合性、引擎搜索立体性。因而，侵犯公民个人信息犯罪的特有预备行为，难以同等性科处刑事处罚，应当结合行为抽象的涉众危害以及具体场合进行犯罪认定。[④]通常而言，非法利用信息网络罪中准备工具的过程也是一种制造条件的环节。陈兴良教授将预备行为划分为两种类型：

①转引自[德]克劳斯·罗克辛：《德国刑法总论（第1卷）》，王世洲译，法律出版社2005年版，第149页。

②See Ch. Jones,in：J.Herczeg/E. Hilgendorf/T.Grivna（Hrsg.）,Internetkriminalität und die neuen Herausforderungen der Informationsgesesllschaft des 21. Jahrhumderts，2010，S.130.

③依据《刑法》第22条之规定，笔者并不否定准备工具型预备犯罪和制造条件型预备犯罪，准备工具的过程也是一种制造条件的环节，其实仅限于网络工具犯罪之中。

④陈伟、熊波：《审慎认定“持有型”侵犯公民个人信息罪》，载《检察日报》，2017年9月20日，第003版。

“准备工具”为有形预备；“制造条件”为无形预备。[①]制造条件的主要表现形式为“制造实行犯罪的主、客观条件”，如调查犯罪场所与被害人行踪。出发前往犯罪场所或者守候被害人到来，诱骗被害人前往犯罪场所、排除实行犯罪的系列障碍以及商议犯罪实行计划等。[②]

考虑到信息网络利用犯罪空间的“线上”操作特质较为明显，以及网络空间虚拟性所导致的受害对象的不明确性，制造条件的预备行为根本无法在网络平台予以实现，现实中也无此必要。而制造实行行为的主观条件一旦被纳为非法利用信息网络罪预备行为的“制造条件”体系之中，则表明网络犯罪的处罚根基则不仅局限于行为本身还关注行为人的思想，这完全背离法益保护原则的现实危害结果以及抽象危险的防控机能。况且，行为刑法聚焦点仍在于行为对法益侵害的严重性，“商议犯罪计划”这一行为本身的法益侵害程度认定具有较大不明确性。综上，《刑法》第22条对预备行为的制造条件与准备工具并非“且”的关系，而仅是“或”的二择一规范依据；又或是，在网络工具犯罪之中，制造条件仅起着作为一种对准备工具的用位语的强调作用，而并不涵盖预备利用行为的具体模式。

2. 预备行为的阶段历程

预备阶段作为犯罪特殊形态的一部分，其仅能存留于犯罪过程之中，对于犯罪既遂之后的再预备，则可能评价为他类犯罪行为的预备状态。犯罪特殊形态的产生缘由在于犯罪过程中出现的某种原因致使终局性的停止状态的呈现，[③]因而，其并非一种漫无止境的阶段历程。但这是否就意味着该预备行为如同实行行为的认定一般，非法利用信息网络罪的行为认定也存在着起点和终点的阶段性历程标志？笔者认为，这一标准的认识应当防止网络工具型犯罪行为的预备性识别，轻易与其他类罪的实行行为的认定相混淆。非法利用信息网络罪与其他类罪名在犯罪形态认定方面存在着如下几种区别：

首先，非法利用信息网络罪的行为起点和终点无法完全界分。网络工具型犯罪的法益类型是信息网络纯净化、生态化以及文明化的公共秩序，因而，非法利用信息网络罪的行为着手点在于对此类网络公共秩序产生的紧迫威胁和现实危害。对接到非法利用信息网络罪的具体行为要素，设立、发布行为要能够产生现实的抽象危害或者现实的概括化威胁，必须是等待设立用于违法犯罪的网站、通讯群组，又或是发布用于违法犯罪活动的信息这两种行为既遂之后，才会产生具体的现实危险和实质的法益威胁。正如前文所述，非法利用网络信息犯罪由于其特殊空间的“线上操作”和物理边界的欠缺，非法利用网络信息罪的预备行为情形既不存在，也不具备可罚性的罪责基础。因而，基于非法利用信息网络罪的部分预备行为正犯化的行为特质，以及预备犯实质形式认定的限缩，其不同于其他类型的实行犯，网络工具犯罪并不具备犯罪的未完成形态。

其次，非法利用信息网络罪的起点认定应当严格限制“着手论”。一般而言，跨越行为的着手点，便意味着特定犯罪行为正式从预备行为阶段迈入实行行为阶段。在大陆法系，犯罪行为的未完成形态之所以存在，就在于法益侵犯客观且现实的危险；而在英美法系，其存留根基就在于特定犯罪行为非常接近犯罪结果，以至于极具成功犯罪的危险性。[④]对比可知，前者侧重于法益保护理念的现实威胁；后者偏向危害原则的具体危险，其实，两者实属异曲同工，都表明预备行为可罚性的基础在于危险的现实化、具体化。在抽象的现实危险之下，部分学者开始

①陈兴良：《规范刑法学》，中国政法大学出版社2013年版，第129 页。

②张明楷：《刑法学》，法律出版社2016年版，第333页。

③张明楷：《刑法学》，法律出版社2016年版，第330页。

④[美]约书亚·德雷斯勒：《美国刑法纲要》，姜敏译，中国法制出版社2016年版，第236页。

主张取消着手的认定，主要理由在于：抽象危险犯的界定及其处罚本身就背离实害结果的客观属性，将“着手”引入危险犯的法益侵害原则，早已背离其原先具有的实质内涵。究其原因，仍在于抽象危险支撑的客观材料之缺乏，导致主观意识评判的泛滥。[①]例如，未遂犯“犯罪分子意志以外的原因”的认定依据以及预备犯“为了犯罪”的规范评价，都难逃主观要素依赖之窠臼。在主观主义甚嚣尘上占据预备犯罪行为的学理根据之时，“着手”的现实价值能否在非法利用信息网络罪的抽象危险认定中发挥其实质性的可罚性奠基，仍值得进一步商榷。

然而，问题在于“危险”如何具体认定，其是否包涵具体的危险与抽象危险的二元论？上述问题的化解是非法利用信息网络罪的着手起点评判的关键与核心。论者指出，在现代信息科技中，线上行为所致的线下行为抽象危险其实根本就不存在，“如果将‘危险’概念理解为一种情形时，在该情形之下，根据日常生活经验知识可知，如果不加阻止地任事情在时间上朝前发展，可预期会损及法益，则肯定会有或多或少具体的危险存在，而不完全是抽象的。”[②]在此种观点支撑下，非法利用信息网络罪的预备利用行为所产生的类型危险难以抽象化。对此笔者认为，该罪的预备行为正犯化的归责基础来源于信息网络利用行为所产生的具体危险，质言之，非法利用信息网络罪中利用行为的实行起点应当以“是否具备独立的预备性可罚依据”为标准，即在具体、翔实的信息网络情境下对危险予以谨慎识别，而不应当依据一般化的生活常识或者现实经验水平，予以抽象化、概括化判断。

3. 预备行为的对象判断

非法利用信息网络罪的预备条件符合性、历程阶段性的探讨，为后续罪名“设立”“发布”行为的精细化认定提供必要的框架指引和深厚的理论奠基。然而，深入挖掘具体行为要素的实质价值，以仔细甄别设立、发布行为的自身预备性，从而在外部行为体系中，区分独立存在的设立、发布行为的实行性；在内部行为体系中，划定《刑法》第287条之一款的第二项和第三项发布行为本身的纯粹实行性和预备实行性的明确界限，主要仍在于从规范中实现预备行为具体要素的精确教义解读。

第一，从行为针对的主体对象来看，存在着他人预备与自身预备两种类型。预备行为正犯化理念并不排斥共同犯罪形态的存在，刑法条文对于“设立用于实施违法犯罪行为”和“发布有关制作和销售违法犯罪物品信息”，并未明确表示局限于对自己后续犯罪行为的预备，而排除共同犯罪中他人犯罪行为的预备。支持仅限于自身犯罪行为预备的学者，从构成要件理论和预备行为正犯化的限缩主张中，论证单纯的自身预备行为的合理性和合法性。如日本野村稔教授就认为，预备行为正犯化是预备行为中的一种，应当亦具备预备行为的共性，犯罪目的本身就是秉持自身的主观动机和目的去实现基本构成要件的内容，而并非顺带包涵他人的目的性要素，即为了他人的实行行为而实施的所谓他人预备行为，其不符合预备犯的行为要件。[③]对此持有同种观点的梁根林教授也认为，基于目的论的限缩解释立场，主张预备行为要件“为了犯罪”的具体符合并不包括为了他人实行犯罪，而仅止于为自己实行犯罪。[④]

笔者认为，从基本构成要件与修正构成要件方面来识别预备行为针对的主体对象，并不具备科学性和合理性。“修正的构成要件（犯罪停顿状态）的存在，是刑事立法以同一犯罪构成为

①高艳东：《着手理论的消解与可罚行为起点的重构》，《现代法学》2007年第1期。

②[德]埃里克·希尔根多夫：《德国刑法学：从传统到现代》，北京大学出版社2015年版，第403–404页。

③[日]野村稔：《日本刑法总论》，全理其等译，法律出版社2001年版，第372–373页。

④梁根林：《预备犯普遍处罚原则的困境与突围——〈刑法〉第22条的解读与重构》，《中国法学》2011年第2期。

基础而进行修正或者截短后作出的特殊规定，它们是同一犯罪构成的不同表现形式”。[①]据此可知，预备行为这一修正的构成要件要素，仅是作为论证预备犯构成要件符合性或是犯罪构成延伸范围的手段和形式目的，并不能据以阐明“设立”“发布”行为人仅是针对自己后续违法犯罪的预备犯而言。此外，本文支持他人预备与自身预备这两种类型并不会导致预备行为的过度犯罪化。其一，预备行为正犯化的教义限缩，应当遵循基本犯罪行为状态理论（如共同犯罪）的体系协调，在体系既存的基本特征中进行限制，而并非为了限制而打破文本规范存在的一般规律。其二，预备行为的风险考察，势必要求充分挖掘并分析出潜在行为所具备的特质，以适配复杂网络技术行为的罪责承担。但预备行为正犯化的可罚性效力的削弱，可以尝试从网络利用的行为对象、后续违法犯罪的种类等方面予以规范。

第二，从设立对象之媒介来看，网站与通讯群组应当以“三网融合”为背景。非法利用信息网络作为一种网络工具犯罪，其司法适用必然面临着利用行为对象或平台的种类问题。非法利用信息网络罪的设立行为作为预备行为正犯化的行为种类之一，其设立对象仅包括“网站”与“通讯群组”。立法者认为，“‘网站’是指设立者或者维护者制作的用于展示特定内容的相关网页的集合，便于使用者在其上发布信息或者获取信息的一种平台；‘通讯群组’则是网上供具有相同需求的人群集合在一起进行交流的平台和工具，如QQ群、微信群等”。[②]然而，这一立法论断显然违背朴素自然法意义上的事实经验。就单纯通过虚设伪基站，准备用于实施群发诈骗短信的行为，并无法从该罪中寻求法律依据。

基于此，笔者认为，此处的网站和通讯群组应当实质解释为计算机互联网、电信网以及有线电视网的“三网融合”，[③]即非法设立三网融合平台用于实施违法犯罪的，都应当依附于文本中的网站和通讯群组。而此处的三网融合具体是指“在信息传输过程中，将不同传输载体网络中的储存和传输数据融合在一起，实现计算机互联网、电信网与有线电视网三大网络信息传输的统一”。[④]

（二）纯粹的实行行为：“发布”有关违法犯罪的信息

非法利用信息网络罪行为形态的二元构建的另一实质层面，则是纯粹实行行为的教义倡导。之所以明确界分网络工具利用型预备行为正犯化与纯粹实行行为的规范基础理论，就在于罪名识别的关键要义：文本实质评价基准上的利用预备行为的限缩与利用纯粹实行行为的适度扩张。正如前述，利用预备行为的限度规范内的规制，能够及时化解网络平台中设立、发布行为的利用类型的风险泛化；而利用的纯粹实行行为的适度扩展则应借助“发布行为”的合理包容性，以此抵御网络社会中发布型利用行为的风险类型新潮。从非法利用信息网络罪的预备行为正犯化的单一行为形态主张，到双向衔接的二元论新解，昭示着罪名涵盖的行为要素的实行化认定之趋势，而尽量避免过多掺杂着处罚早期化所致的国民“体感治安”的降低。[⑤]

“发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息”的网络利用行为，为何不同于《刑法》第287条之一款的第一项与第三项的设立、发布的利用预备行为，本质就在于第二项的发布行为本身并不需要依托制作与销售违禁物品与管制物品

①杨兴培：《犯罪构成原论》，北京大学出版社2014年版，第273页。

②全国人大常委会法制工作委员会：《中华人民共和国刑法释义》，法律出版社2015年版，第502–503页。

③三类网络平台的统一、融合并非简单的三大网络之间的物理维度上的聚合。如设置互联网平台的伪基站信号，并借助无线的电信网传播诈骗信息，进而实施系列违法犯罪行为的行为就是虚化维度上信号的互动反映。

④于志刚：《网络刑法的体系构建》，中国法制出版社2016年版，第25页。

⑤[日]松原芳博：《刑法总论重要问题》，王昭武译，中国政法大学出版社2014年版，第17页。

的行为犯罪化与否的前提认定，质言之，发布的实行行为本身便具备单独处理刑事可罚性的理论基础，即一旦发布违法犯罪信息行为达到严重社会危害性程度或是严重法益侵害性的，扰乱网络平台社会管理秩序的，则无需再次循环依靠发布信息对象行为的制作销售毒品、枪支、淫秽物品等违禁物品、管制物品的刑事处罚性，立足第二项发布行为的教义解读，无此必要亦无惧司法操作的冗杂无序，同样能规避网络信息发布风险的提升概率。

首先，立足信息发布的时间维度分析，发布仅限于行为时的非法信息。毋庸置疑，以行为人行为时制造的客观风险条件为焦点，意图与轻率的分析才有可能。[①]由此可知，意图与轻率（故意和过失）的心态认定来源于行为时的具体客观条件。同样，非法利用信息网络罪的发布信息的时间认定，亦应仅停留于行为时的发布信息的现实基础上进行评判。因而，基于第二项的发布信息行为的纯粹实行性之时间思维，发布时信息合法，但被他人利用于从事违法犯罪活动的，则无法将其纳入此处的发布违法犯罪信息的规范实质之中。此外，发布仅限于行为时的信息还应强调，其并不依赖于违法犯罪活动的先行为发生。亦即，虽第二项的违法犯罪活动信息并未予以网络化与现实化公开，又或是违法犯罪性质本身无法具体化、精确化的界定，但并不妨碍行为人将其发布的公开行为亦认定为此处的发布信息行为。由此可以消解预备行为正犯化的界定依托于“违法犯罪活动”这一前提行为性质的混淆，所致的发布信息行为本身的可罚性基础的削减，进而防止行为肆意地脱逃刑法的规制与评价。[②]因为在某种程度上可以说“刑事立法将可罚性的起点置于阴谋阶段或者预备阶段，而设阴谋犯或预备犯的处罚规定，不但存在刑事证据上的盲点，而且存有故意入罪的危险”。[③]

其次，鉴于发布的多元类型的实质解读，变相发布信息行为亦具可罚基础。《刑法》第287条之一款第二项的发布信息并非仅限于将秘密信息予以直接公之于众的过程。例如，借助发帖、追帖在网络平台散播违法犯罪信息的。由于司法实践操作的便捷，直接发布信息行为作为网络利用行为的原型化判断，占据着较大的教义理论市场。但不可否认，部分虽不具备发布信息的表面构成要件要素的形式特征，但其行为最终效果与直接发布信息行为并无二异，甚至可理解为一种发布行为的真正构成要件要素，即一种间接发布信息行为，为非法利用信息网络犯罪的理性且客观的处罚提供违法且有责的实质要素。[④]而这一间接发布信息的网络行为类型，则避免了刑法文本规范的呆滞且固化之形式预判。如，行为人为逃避网络犯罪的刑事制裁，而借助发布特定的信息承载实体，链接地址、处理截图以及部分可见且不完全公开的通讯工具（微信、QQ），更甚是将诸如网盘、云盘等包含信息文件的资源储存空间程序设置的密码账号予以发布，以此掩盖发布违法犯罪信息的实质可罚基础。而上述诸如此类的发布信息行为，亦即非法利用信息网络罪的纯粹实行行为的教义理论，是基于客观罪责要求的实用性功效之思量，同时亦是信息网络时代风险扩展概况的现实依托。

①[美]乔治·弗莱彻：《反思刑法》，邓子滨译，华夏出版社2008年版，第323页。

②非法利用信息网络罪中的“违法犯罪活动”的行为性质认定存在着较大的争议，有学者认为，“只有发布违法犯罪信息属于相应犯罪的预备行为，而且情节严重时，才能成立非法利用信息网络罪。”亦即违法仅是刑事违法性层面的强调，而并非拘泥于违法行为的性质认定（参见张明楷：《网络时代的刑事立法》，《法律科学》2017年第3期）。再如，有的学者认为，《刑法修正案（九）》中“针对所有违法犯罪活动的某一特定预备行为的实行化。与第120条之二正好相反，第287条之一‘准备网络违法犯罪活动罪’的立法特色，是针对所有违法犯罪活动的某一特定预备行为的实行化”。亦即，其认为非法利用信息网络犯罪活动罪的违法行为的预备行为实行化也是刑事立法的亮点所在（参见车浩：《刑事立法的法教义学反思——基于〈刑法修正案(九)〉的分析》，《法学》2015年第10期。）

③林山田：《刑法通论》，北京大学出版社2012年版，第296页。

④张明楷：《犯罪构成体系与构成要件要素》，北京大学出版社2010年版，第121页。

最后，对发布信息的性质评断，应避免与发布预备行为中的信息种类相混淆。基于非法利用信息网络罪的二元行为形态之构建，预备行为转化的实行行为要素必然应当与纯粹实行行为要件予以区分开来。在预备行为侵害的法益严重程度与不法意志下刑罚惩罚性的现实依据模糊的背景下，预备行为正犯化的确立恐怕是对于人毫无节制的工具化反映。[①]从《刑法》第287条之一款的发布预备行为与发布施行行为来看，第二项中发布的信息对象本身应当具有明显的违法犯罪性质，而针对第三项中发布的信息，从性质上看并不要求本身的刑事违法属性。但应当肯定的是，两者发布的信息都应当是真实的信息类型，否则将其定性为编造、故意传播虚假信息罪，完全足以适配其罪责评价。[②]从数量上看，正因为实行行为的发布信息的社会危害性，较发布信息预备性行为的更为严重，因而，两者在具体的司法认定与教义解读方面，对罪刑搭配的数量认定应当有所界分，以此体现预防刑法中相应违法犯罪行为时点介入的区分立场。[③]

四、结论

在预备行为正犯化立法趋势饱受理论界诟病之际，非法利用信息网络罪作为一种网络工具犯罪，应当及时扭转其预备性转化实行行为的扩大化的话语形式与事实构造之认定。为克服网络风险社会潜在因素所造成的不确定法益侵害，将非法利用信息网络罪的行为形态，定位于预备行为的正犯化与纯粹的实行行为的二元构建，具备现实可行性、规范疏通性以及理论周延性。罪名罪量要素中的存在论与价值论，无法实现教义阐释的规范越轨，文本规范具有天然的明定指引与常情、常理、常识的自由心证之理性评判。“设立”“发布”网络利用行为的教义解读应当体现实定法规范的约束性、支配性的程序规则构建，在此基础上搭配技术性规范，以便刑法与时代思想相对应，在这种法规范不断适应新事实的解释现象中，“学者的解释与法官的论断，在文化的长河中被赋予了独立地位之属性，因此，他们最终的任务便是衔接并调和法律与时代思想之间的冲突与鸿沟”，[④]进而，二元形态的理念证成亦能服务并充实着司法实践的时代与新潮。

主要参考文献：

[1] Graif C，Lungeanu A I，Yetter A M. Neighborhood isolation in Chicago：Violent crime effects on structural isolation and homophily in inter-neighborhood commuting networks[J]. Social Networks，2017，51：40–59.

[2] Hadji-Janev M. Toward effective national cyber security strategy：The path forward for Macedonia[A]. Vaseashta A，Susmann P，Braman E. Cyber Security and Resiliency Policy Framework[M]. IOS Press，2014：57–64.

[3] Hanser R D. Gang-related cyber and computer crimes：Legal aspects and practical points of consideration in investigations[J]. International Review of Law，Computers & Technology，2011，25（1–2）：47–55.

[4] Helfgott J B. Criminal behavior and the copycat effect：Literature review and theoretical framework for empirical investigation[J]. Aggression and Violent Behavior，2015，22：46–64.

[5] Kouziokas G N. The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment[J]. Transportation Research Procedia，2017，24：467–473.

①黄荣坚：《基础刑法学》(下)，中国人民大学出版社2009年版，第310页。

② 陈伟、熊波：《网络谣言型涉众事件的刑事归责理论之匡正》，《现代传播（中国传媒大学学报）》2017年第11期。

③何荣功：《预防刑法的扩张及其限度》，《法学研究》2017年第4期。

④[日]中山研一：《牧野英一の刑法思想》，[日]吉川经夫等：《刑法理论史の综合的研究》，日本评论社1994年版，第307–308页。

[6] Kouziokas G N. The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment[J]. Transportation Research Procedia，2017，24：467–473.

[7] Lagazio M，Sherif N，Cushman M. A multi-level approach to understanding the impact of Cyber Crime on the financial sector[J]. Computers & Security，2014，45：58–74.

[8] Pettersson T. Ethnicity and violent crime：The ethnic structure of networks of youths suspected of violent offences in Stockholm[J]. Journal of Scandinavian Studies in Criminology and Crime Prevention，2003，4(2)：143–161.

[9] Sindhu K K，Meshram B B. Digital forensics and Cyber Crime datamining[J]. Journal of Information Security，2012，3(3)：21340.

[10] Summers L，Johnson S D. Does the configuration of the street network influence where outdoor serious violence takes place？ Using space syntax to test crime pattern theory[J]. Journal of Quantitative Criminology，2017，33(2)：397–420.

[11] Yang C C，Li K W. An associate constraint network approach to extract multi-lingual information for crime analysis[J]. Decision Support Systems，2007，43(4)：1348–1361.

The Interpretation of the Doctrine of Binary Form of Information Network Crime

Chen Wei[1], Xiong Bo[2]

(1. *School of Law, Southwest University of Political Science and Law, Chongqing* 401120, *China*; 2. *Research Center of Youth Crime, Southwest University of Political Science and Law, Chongqing* 401120, *China*)

Summary: In the network information era, it is necessary to set partial pre-prevention behavior of the crime of illegal use of information network to respond to virtuality, technical transcendence and stakeholder-based order of network risk society. Crime of illegal use of information network, should not be determined as a ready behavior of principal offender as a whole, and from a perspective of precise language norms of criminal law, there exists a dual qualitative standard in behavioral form of information network crime, namely ‘preparation act of principal offender’ and ‘pure perpetrating act’. The practice of ‘pure perpetrating act’ as a criminal form in crime of illegal use of information network considers the technological rules of network risk society, and applies technological changes in the network information age to coping direction, content structure and discourse cohesion of network criminal law system. The technological rules of cyber criminal law include the proportion principle of technical specification setting, the allowable risk principle in technical specifications, and the typed principle of technical specification arrangement. In view of this, the virtual nature of cyberspace is regarded as the reality of technological changes and its dual form construction remains in double space. The transcendence of network technology is seen as the advance trend of technological changes, and its dual form construction has the prospectiveness of regulation. The stakeholder of network order is regarded as the hazard evaluation of technological changes, and its dual form construction corresponds to pluralistic behavior prevention. Complying with the doctrine interpretation of

(下转第152页)

lower people's court finds that foreign-related arbitration agreement is invalid, it will require the latter to report to high people's courts. However, such a request for reporting is only applied against foreign-related cases, and its own procedure is very prolonged and inefficient. At the same time, in other cases including the nature of foreign-related affairs, there is a very unfriendly attitude towards the determination of arbitral consent, which is mainly manifested in the lack of agreement on arbitration agreement with the selection of two or more arbitration institutions. Such a harsh attitude of judicial review is not conducive to China's growth into a world-competitive place of arbitration. As one of the world's arbitration centers, it can bring a lot of benefits such as good reputation, foreign exchange income and a reduction in litigation rate in our country. Our country should adopt the dual measures of amending the corresponding defects of the Arbitration Law and improving the judicial attitude of the people's courts to achieve this goal, that is to abolish the legislative provisions of the prohibition of ad hoc arbitration, to allow to appeal to the higher-level people's courts for negative decisions on the issues of arbitral consent. At the same time, the people's courts in the judicial review of any case stop applying internal reporting procedures when they announce arbitral consent and so on.

Key words: arbitration; consent; judicial review; burden of proof

（责任编辑：倪建文）

(上接第138页)

normalized practice of Article 22 of the 'criminal law', 'in order to crime' should place emphasis on the correspondence between criminal purpose and preparatory act, 'the preparation of the instruments' must be limited to direct tool preparatory behavior, and 'creation of conditions' do not have specific patterns of preparatory using behavior. Under the basic guidance of the dualism of behavioral form of information network crime, a 'website' set up should include space types under 'three-network integration'; the issued 'information' evaluation should be interpreted in terms of 'time, nature and type'. Firstly, based on the time-dimension analysis of information release, the distribution is restricted to illegal information when the behavior is restricted. Secondly, in view of the substantive interpretation of the multiple types of publication, disguised information release act also provides a punishment basis. Finally, as for the nature judgment of the published information, it is necessary to avoid confusion with information types of release preparation act. While legislation trend towards preparation act of principal offender suffers a lot of criticism by the theoretical circle, crime of illegal use of information network as a type of network tool crime shall timely reverse the determination of discourse form and fact structure concerning an expansion of its transformation from preparation act to pure perpetrating act. In order to overcome uncertain infringement of legal interests resulting from the potential factors of network risk society, the establishment of a dual qualitative standard in behavioral form of information network crime, namely 'preparation act of principal offender' and 'pure perpetrating act', has reality feasibility, norm dredging and theoretical extension.

Key words: crime of illegal use of information network; network risk society; preparation act of principal offender; pure perpetrating act

（责任编辑：倪建文）