提供侵入、非法控制计算机信息系统程序、工具罪的限缩解释

——以打击对象为切入

高艳东

【摘　　要】受从严打击网络犯罪刑事政策的影响，提供侵入、非法控制计算机信息系统程序、工具罪成为规制非法网络技术帮助行为的兜底性罪名之一，其打击对象从最初的“木马病毒”扩展到“外挂软件”“翻墙软件”“网络爬虫”等具有一定中立性的软件，打击范围的持续扩张使其呈现出口袋化趋势。该罪逐渐被滥用的原因在于，司法解释未对“侵入”“计算机信息系统安全保护措施”等专业名词做出合理解释，导致司法工作人员在理解“专门用于侵入、非法控制计算机信息系统的程序、工具”时存在偏差，混淆了“数据”“控制”等术语的技术判断与法律评价。为防止该罪的口袋化趋势，我们应从技术和法律两个层面解读其构成要素，为司法机关提供清晰的定罪标准。

【关 键 词】侵入；口袋罪；授权；计算机信息系统安全保护措施

【作者简介】高艳东，浙江大学光华法学院副教授。

【原文出处】《法学评论》（武汉），2023.6.121～132

【基金项目】本文系国家社科基金重大项目《网络时代的社会治理与刑法体系的理论创新》（项目编号：20&ZD199）的阶段性成果。

《刑法修正案（七）》于2009年设立了提供侵入、非法控制计算机信息系统程序、工具罪（以下简称“提供工具罪”），其适用经历了几个阶段性的演变。2009年至2013年，该罪主要打击制售盗号“木马病毒”行为，案件数量极少。2014年至2017年，该罪打击对象扩展到“翻墙软件”“网络爬虫”等有一定中立性的程序与工具，案件数量逐渐攀升。2017年之后，该罪打击对象扩展到有相对中立性的“外挂软件”，案件数量猛增。近年来，随着对网络犯罪“打早打小”刑事政策的落实，一些原本以非法经营罪、侵犯著作权罪、销售侵权复制品罪定罪的销售非法软件案件也经常被认定为“提供工具罪”。其中，部分案件属于多个罪名竞合而被动适用了“提供工具罪”，但也有很多案件直接被认定为“提供工具罪”并存在罪名适用争议。很多判决书在论证“专门用于侵入、非法控制计算机信息系统的程序、工具”时说理不充分，在解释“计算机信息系统安全保护措施”时含糊不清，让学界开始担心“提供工具罪”罪名适用的口袋化倾向。

一、问题提出

案例一：2018年，“明星蔡徐坤一条微博转发量过亿”事件引发社会对流量数据造假的关注。涉案刷量软件的开发者蔡某某因涉嫌破坏计算机信息系统罪被警方逮捕，最终以“提供工具罪”被法院判处有期徒刑五年。[①]该判决对于打击流量造假乱象具有积极意义，但判决结果却引发了争议：刷量软件是否属于“专门用于侵入计算机信息系统的程序”，使用软件的粉丝是否有“侵入”或“非法控制计算机信

息系统”的行为?

案例二:2018年9月,上海市宝山区法院审理了戴某提供VPN“翻墙”服务案,司法人员对于提供VPN“翻墙”服务的定性产生了分歧,存在无罪、非法经营罪、“提供工具罪”三种意见。[②]法院最终以“提供工具罪”判处戴某有期徒刑三年,缓刑三年。[③]虽然翻墙软件能避开国家网络管控措施,但这种管控措施是否属于“计算机信息系统安全保护措施”,即便翻墙软件避开了安全保护措施,是否非法获取了计算机信息系统数据或非法控制了计算机信息系统?这些理论问题,判决书都没有明确回应。

这些判例反映出司法实践中的常见问题:一是“‘专门’侵入、控制的程序、工具”(以下简称“专门工具”)和“‘可以’侵入、非法控制计算机信息系统的程序、工具”(以下简称“其他工具”)的界限不清;二是“侵入”“计算机信息系统安全保护措施”等专业名词的含义不清;三是工具使用者行为的定性对“提供工具罪”基本无影响,刷量软件、翻墙软件成为“提供工具罪”的打击对象,但软件使用者均不构成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。在类似案件中,法院认定的“专门工具”无法被用于侵入、非法控制计算机信息系统,逻辑上存在矛盾。2017年后,“提供工具罪”案件数量明显增加,但相关专业名词的含义并未清晰化,反而有被扩大化解释的趋势,导致该罪的打击范围不断扩大。法官在适用该罪名时常忽视涉案程序、工具的主要用途,混淆“专门工具”和“其他工具”,导致该罪被滥用。基于此,本文尝试提出防止“提供工具罪”被滥用的学理建议。

二、罪名适用现状与争议的类型化分析

笔者以北大法宝为数据库,以“提供工具罪”为案由,检索得到判决书748篇(上传日期截至2023年8月1日),历年审结案件数量如图1所示。

分析图1可知,自2015年起“提供工具罪”历年审结案件数量呈递增趋势,于2020年达到最高峰。需要说明,根据笔者在H市基层司法部门的调研,2021、2022年“提供工具罪”定罪数量仍居高不下,只是因该罪控辩双方争议较大导致判决书上网数量明显下降。

在748份判决书范围内,笔者以涉案软件、工具类型为关键字进行二次检索,得到各类软件、工具所涉案件数量与占比如下页表1所示。

表1中“其他”类型的程序、工具,部分属于已列明类别,但在判决书中无关键字;还有部分由于案件数量很少故不单独列明,如账号解封软件、会员破解软件、炒股分仓软件、黄牛抢票软件、爬虫软件等。

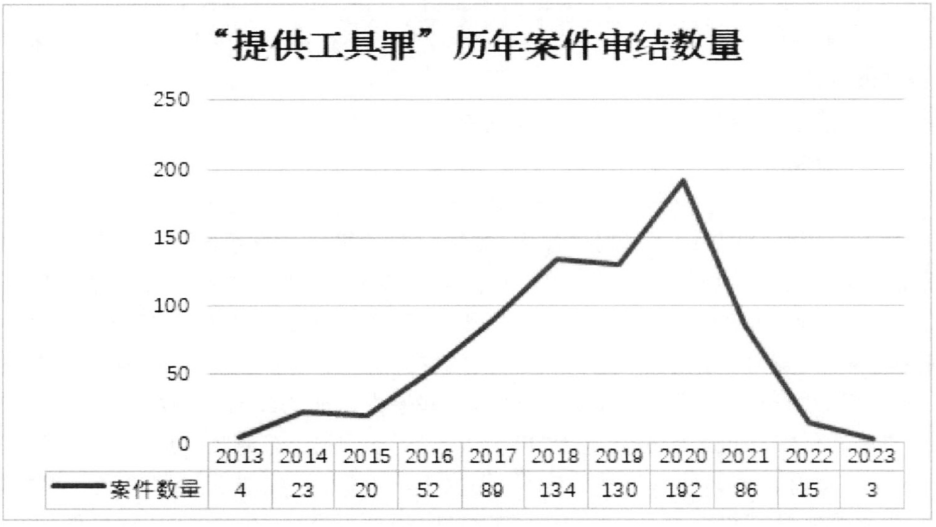

图1 “提供工具罪”判决情况

表1 “提供工具罪”各类程序、工具案件数量

	插件(外挂)	木马病毒	翻墙软件	钓鱼网站	撞库软件	手机轰炸软件	DDoS攻击软件	其他
案件数量	332	130	70	47	23	14	9	123
所占比例	44%	17%	10%	6%	3%	2%	1%	17%

分析表1可知,外挂软件、木马病毒、翻墙软件所涉案件数量最多,是“提供工具罪”的主要打击对象。“提供工具罪”系帮助行为正犯化罪名,罪名成立与被帮助行为的定性息息相关,故笔者以被帮助行为是否构成犯罪及构成何罪为分类依据,将现有裁判文书中涉及的程序、工具分为“被帮助行为触犯《刑法》第285条”“被帮助行为构成其他犯罪”“被帮助行为不构成犯罪”三类,便于后续讨论。简要介绍如下:

(一)被帮助行为触犯《刑法》第285条

第一,木马病毒。木马病毒一般被用于盗窃他人账号、密码等身份认证信息,或控制他人计算机后实施敲诈,司法机关一般以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对使用木马病毒的行为进行定罪。由于木马病毒的侵入性较为明显,司法实践对其定性争议不大。

第二,撞库软件。由于撞库软件采用批量尝试登录这一简单机械化方式获取用户名与密码,其定性曾存在一定争议,有学者将其认定为“采用其他技术手段”非法获取计算机信息系统存储的数据,以非法获取计算机信息系统数据罪定罪。[④]2020年4月,最高人民检察院发布第十八批指导性案例,明确“撞库软件”为“专门工具”,为他人提供“撞库软件”的行为构成“提供工具罪”。自此,司法实践对撞库软件的定性形成了统一意见。

(二)被帮助行为构成其他犯罪

第一,钓鱼网站。我国刑事立法对于网络钓鱼缺乏针对性的规定,司法机关一般按照目的行为将其认定为诈骗罪、盗窃罪、侵犯公民个人信息罪、信用卡诈骗罪等,“东打一枪,西放一炮,没有形成一个明确且稳定的刑事规制体系”。[⑤]钓鱼网站也属于“其他技术手段”,但与“撞库软件”不同的是,对钓鱼网站的罪名适用存在分歧,对具有财产价值的数据应作为财产、个人信息还是数据进行保护,实践中存在较大争议。

第二,手机轰炸软件。现在网络上的手机轰炸软件均是由个人开发制作,以打击报复、敲诈勒索、软暴力催收欠款为目的,司法机关一般以寻衅滋事罪、敲诈勒索罪、破坏计算机信息系统罪、非法利用信息网络罪等罪名对其定罪。有学者认为手机轰炸软件具有“间接控制”计算机信息系统的功能,属于“专门工具”,可以构成非法控制计算机信息系统罪;但也有学者认为手机轰炸软件既有合法用途,也可用于非法用途,恶意呼叫使得被害人的手机在一定时间内无法正常使用,不代表对被害人的手机进行了非法控制,软件使用者不构成非法控制计算机信息系统罪,软件提供者也不构成“提供工具罪”。[⑥]总体而言,对手机轰炸软件的定性,司法实务和学界都存在较大争议。

第三,DDoS攻击软件。对以攻击计算机信息系统为目的、非法控制计算机信息系统的DDoS攻击行为,司法实践多数按照牵连犯处理,根据择一重罪处罚原则以破坏计算机信息系统罪定罪处罚;[⑦]但也有法院将其认定为非法控制计算机信息系统罪。[⑧]可见,对于DDoS软件的本质是“破坏性”还是“控制性”,实践中仍存在一定争议。

(三)被帮助行为不构成犯罪

第一,插件(外挂软件)。早期的外挂一般被用于网络游戏作弊,但随着移动智能设备的普及,外挂逐渐进入多个领域,如“微信抢红包”外挂、“美团众包抢单”外挂等。使用外挂一般不构成犯罪,而制售外挂的行为定性,在实践中存在“提供工具罪”、非法经营罪、破坏计算机信息系统罪、非法获取计算机信息系统数据罪、侵犯著作权罪、无罪(民事争议或行政处罚)等争议。由于外挂软件的运行方式多样,学者

多支持区别对待不同类型的外挂，但未形成普遍认同的分类标准，在罪名适用上也存在较大分歧。

第二，翻墙软件(VPN)。对提供翻墙软件是否构成犯罪有不同意见，在有罪论中也存在“提供工具罪”、非法经营罪、拒不履行信息网络安全管理义务罪等罪名争议。

综上，在三类程序、工具中，“被帮助行为构成《刑法》第285条”的木马病毒、撞库软件在罪名适用上无太大争议；而“被帮助行为构成其他犯罪”的钓鱼网站、手机轰炸软件、DDoS攻击软件及“被帮助行为不构成犯罪”的外挂软件、翻墙软件均存在很多争议，而这五种软件的案件数量合计占比在60%以上。因此，如何准确适用“提供工具罪”是亟须研究的问题。

三、罪名滥用现象梳理与原因分析

“提供工具罪”罪名适用争议的背后，是该罪的构成要件模糊导致口袋化。具体而言：一是“专门工具”与“其他工具”界限模糊，司法人员常错误解读司法解释中的技术名词，将“具有侵入功能”与“专门工具”画上等号；二是“专门工具”的认定标准过低，缺乏专门的鉴定机构与鉴定标准，混淆“破坏性程序”与“侵入性程序”；三是将“被帮助的犯罪行为”扩张到《刑法》第285条之外的犯罪，导致该罪适用范围扩张。

(一)“专门工具”与“其他工具”的界限不清

“提供工具罪”有“专门工具”和“其他工具”两个入罪路径：一是提供“‘专门’用于侵入、非法控制计算机信息系统的程序、工具”；二是“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”。可见，“专门工具”的入罪条件较少，无论他人是否实施犯罪行为，提供者均构成犯罪；而“其他工具”的入罪条件较多，需他人实施犯罪，且提供者对此明知。但是，实践中两者的界限模糊，导致该罪的入罪门槛降低。

1. 司法解释扩大了“专门工具”的范围

第一，司法解释突破了立法机关对“专门工具”的界定。全国人大常委会法工委刑法室编写的论著将“专门工具”解释为“行为人所提供的程序、工具‘只能’用于实施非法侵入、非法控制计算机信息系统的用途。”[9]立法机关强调“只能用于侵入、控制”。而最高人民法院、最高人民检察院(以下简称“两高”)发布的《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》(以下简称《计算机司法解释》)第二条第(一)(二)项对于“专门工具”的解释仅要求“具有侵入、控制功能”，将“唯一功能”偷换成“可用功能”，扩张了“专门工具”的范围。

第二，司法解释未明确界定“侵入”的含义。《计算机司法解释》第二条第(一)(二)项均将“避开或者突破安全保护措施”“未经授权或者超越授权”作为认定“专门工具”的条件之一，而第(三)项却未规定前两项的认定标准，以“侵入”代之，将其与“非法控制”“非法获取数据”并列描述。《计算机司法解释》并未明确界定“侵入”的标准，其含义是“避开或者突破安全保护措施”“未经授权或者超越授权”之和，还是与“非法控制计算机信息系统”“非法获取计算机信息系统数据”并列，语义上存在模糊性。从系统解释的角度分析，按照非法侵入计算机信息系统罪的规定，若仅有“侵入”行为，则对象是国家事务、国防建设、尖端科学技术领域的计算机信息系统时才构成犯罪。据此可推论，若行为人提供只是具有“侵入”功能的程序、工具而非“‘只能用于’侵入的程序、工具”，则只能构成非法侵入计算机信息系统罪的帮助犯。显然，具有“侵入”功能不能当然推定其属于“专门工具”。在技术上，“专门工具”不一定具有“侵入”功能(如最高人民检察院在指导性案例中提及的“撞库软件”)。换言之，具有“侵入”功能不是“专门工具”的充分条件，也不是必要条件。但是，一些司法人员错误理解“侵入”的含义，将“具有侵入功能”与“专门工具”画等号，扩大了“专门工具”的范围。

2. 片面强调“数据”“控制”的技术判断或规范评价

认定“非法获取计算机信息系统数据”和“非法

控制计算机信息系统”时，片面强调技术判断或规范评价都会导致“专门工具”范围过大。

第一，司法机关片面强调“数据”的技术判断而忽视了其规范评价。法律保护数据是因为其技术属性具有成为保护客体的基础，但核心是数据承载了某种社会利益，技术的客观内容与法律的规范评价缺一不可。如学者所言，“法律应侧重于保护信息本身的合法财产利益，而不是通过保护信息系统的物理、有形属性来间接保护有价值的信息。”[10]《计算机司法解释》未解释“数据”，仅在第一条中明确身份认证信息属于数据，即用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。而司法机关认定的“数据”还包括储存在计算机信息系统上的用户身份信息，如身份证号码、联系方式、家庭住址、银行卡账号与密码等。身份认证信息代表系统操作权限，将“数据”解释为身份认证信息是一种规范评价；而用户身份信息代表用户个人的隐私权、财产权，将“数据”解释为一切存储在计算机中的信息是用技术判断的视角扩张了“数据”的范围。如学者指出，在技术层面上，数据是信息的载体，表现为二进制代码，很容易认定；而在法律层面上，数据承载着法益保护需要，较为抽象；不少司法人员倾向于只从技术角度理解数据，避而不谈非法获取数据行为侵犯了何种法益。[11]实践中，司法机关仅从技术层面理解“数据”概念，导致“数据”的范围扩大到使用翻墙软件获取的国外网站数据、使用游戏外挂软件获取的游戏数据、使用爬虫软件抓取的公开数据等，人为扩大了“数据”的范围，超越了《刑法》第285条的构成要件保护范围。

第二，司法机关过度强调“控制”的规范评价而忽视其技术判断。“非法控制”首先是技术判断，即窃取或限制系统管理员账户的部分系统控制权，如有学者的界定：“行为人使计算机信息系统处于非法控制状态下，按照行为人的意志运行，不正当地限制宿主的使用权限，侵犯权利人的合法权益。”[12]但是，在实践中，司法机关过度强调“控制”的规范评价，仅从侵害结果角度对行为进行规范评价，混淆了“控制”与“破坏”的界限。例如，在“全国首例黄牛抢购软件案”[13]中，该抢购软件具有模拟用户登录淘宝账号并进行批量下单的功能，同时能通过重新拨号更换IP地址，绕过淘宝对于同一IP地址频繁发送交易请求的限制。有学者认为，抢购软件会侵入淘宝的计算机信息系统并对其予以控制，应以非法控制计算机信息系统罪论处。[14]但是，黄牛抢购软件变换用户IP地址、高频发送交易请求的行为类似于DDoS攻击，所有操作指令均是从用户电脑上发出，且以普通用户身份而非管理员权限向系统发出交易请求，其目的是使计算机信息系统无法处理正常买家的交易请求，始终都未获得计算机系统的控制权限。将使用抢购软件的行为解释为“间接控制(计算机信息系统)”，就是从后果角度进行的主观规范评价，没有考虑到“控制”的技术判断，混同了“妨碍普通用户的使用权限”与“限制系统管理员的使用权限”。

(二)“专门工具”的认定标准过低

相比于“其他工具”，“专门工具”的鉴定标准、认定程序应更严格。但是，实践中以“专门工具”入罪的案件远多于“其他工具”，而其实体和程序认定均不规范。

1.在实体上过度扩张“侵入”的内涵

我国《刑法》没有明确规定“侵入”的含义，司法机关依据《计算机司法解释》第二条对“专门工具”的解释，将“侵入”理解为“避开或突破计算机信息系统的安全保护措施，未经授权或超越授权的访问行为”。但《计算机司法解释》没有定义“授权”“安全保护措施”“访问”，导致实践中过度扩张解释“侵入”。例如，在“张海波等复制IC卡案”[15]中，被告人张海波等从网上购买了IC卡加密复制器，将公司配发的IC卡原卡复制成小卡，使小卡与原卡一样具有刷卡吃饭、考勤打卡、门禁卡等功能，再出售小卡牟利。法院将复制后的小卡认定为“专门工具”，以“提供工具罪”判处被告人罚金5000元。司法机关滥用“侵入”，将使用小卡的行为认定为“侵入计算机信息系统”。

实际上，使用复制的小卡需要遵循作为公司安全保护措施的防护程序，类似于在POS机、自动取款机上“使用伪造的信用卡”，并未突破“安全保护措施”，和黑客攻击有本质区别，不能认定为侵入公司的计算机信息系统。

如果不严格把握“侵入”的内涵，很多违法行为都可以被认定为“提供工具罪”。按照“张海波等复制IC卡案”判决的逻辑，行为人用猜数字的方式破解特斯拉汽车的电子密码锁，也会被认为侵入了汽车和电子锁的安全防护系统；伪造内置IC卡的二代身份证后刷身份证进火车站，会被认为侵入了身份证管理系统；伪造可以骗过ATM机的纸币，会被认为侵入了银行的安全防护系统。换言之，帮助他人偷开车锁、伪造身份证、伪造人民币都可能构成“提供工具罪”，这显然超出了刑法条文语义的最大射程。

2.在程序上缺乏鉴定“专门工具”的机构

《计算机司法解释》第十条规定，对于“专门工具”的认定难以把握的，可以委托省级以上负责计算机信息系统安全保护管理工作的部门检验。但在司法实践中，一些法官在被告人提出鉴定申请后，会以“没有必要委托有关部门检验”为由驳回。例如，在“杨童售卖DDoS攻击软件案”[16]中，法院未对涉案软件进行技术鉴定，未分析该程序避开了何种“安全保护措施”、如何对系统实施控制，仅因其产生了破坏性后果便认定为“专门程序”，其技术依据明显不足。

法院不愿进行司法鉴定有两个原因：一是合格鉴定机构缺失。“省级以上负责计算机信息系统安全保护管理工作的部门”具体是哪个部门，司法解释没有明确规定。二是鉴定能力不足。实践中法院委托的鉴定机构基本是以“电子证据”为鉴定内容，其主要业务是鉴定电子数据的真伪，如数据是否经过篡改、是否为原始数据，基本是一种静态、单向鉴定；而鉴定“专门工具”需要结合业务场景进行动态、双向鉴定。目前具备鉴定能力的专业机构极少，而传统鉴定机构的鉴定也多流于形式，其结论基本是将送检程序描述成具有破坏性或侵入性，法官再根据危害后果进行规范判断从而肯定其属于“专门工具”。

(三)将被帮助的犯罪行为扩张到《刑法》第285条之外的犯罪

《刑法》第285条明确限定了“提供工具罪”下游犯罪的范围，但司法机关常将下游犯罪扩张到诈骗、盗窃等非计算机犯罪，扩张本罪适用范围。

第一，择一重罪处罚导致罪名适用扩张。以“其他工具”为基础判定“提供工具罪”，需行为人明知他人实施侵入、非法控制计算机信息系统犯罪而为其提供程序、工具。虽然在字面上，法条未提及非法获取计算机信息系统数据罪，但从体系性解释的角度考虑，此处也应该包括非法获取计算机信息系统数据罪(下合称“侵入、获取、控制三罪”)。[17]择一重罪处罚导致罪名适用扩张是指，被帮助行为人同时构成“侵入、获取、控制三罪”和其他犯罪，按照牵连犯或想象竞合犯等择一重罪处罚时，最终以非计算机犯罪进行定罪的情形。在被帮助行为同时构成其他犯罪和“侵入、获取、控制三罪”时，择一重罪处罚并未扩张“提供工具罪”的适用范围，符合罪刑法定原则。但这种处理方式只能存在于以“其他工具”为基础判定构成“提供工具罪”的场合，否则将超出“‘专门工具’只能用于实施非法侵入、非法控制计算机信息系统的用途”的应有之意。

第二，宽松认定“专门工具”导致罪名适用扩张。以“专门工具”入罪，不要求被帮助的犯罪行为构成犯罪，也无须考虑被帮助行为构成何罪。许多涉案软件程序不具有非法获取数据或非法控制系统的功能，但司法人员为减少入罪障碍常直接将其认定为“专门工具”。如在“钟全喜出售赌资统计软件案”[18]中，被告人向他人出售统计软件，供他人在微信赌博群内统计赌资。经鉴定，该统计软件能够向微信主程序注入代码文件，在微信软件中增加赌博功能，法院认为被告人提供“专门工具”供他人用于微信赌博统计，构成“提供工具罪”。本案中，软件使用者利用微信与赌资统计软件开设线上赌场，构成开设赌场罪，不构成“侵入、获取、控制三罪”，若将该软

件认定为“其他工具”将导致无法入罪，故法院只能以“专门工具”入罪。但是，本案被告人的目的是通过反编译破解微信代码，绕过微信的插件安全识别措施，使得自己开发的赌博软件能够与微信主程序“捆绑”。该赌博软件与“脱机类外挂”相似，能够“伪装”成微信客户端程序访问微信服务器，但其获取的信息系赌客在线上赌博时产生的用户个人信息，不属于微信系统的数据。换言之，该赌博软件虽侵入了计算机信息系统，但未非法获取计算机信息系统数据，也未非法控制计算机信息系统。即便被告人在反编译过程中获得了软件代码，也只能认定为侵犯著作权罪，因为反编译在技术上不是侵入行为而不构成“提供工具罪”。因此，将类似统计软件认定为“专门工具”违反《计算机司法解释》的规定。

另外，上文提及的刷量软件、翻墙软件的罪名适用争议也体现了该罪扩张适用的现象。使用刷量软件的粉丝、使用翻墙软件浏览国外网站的用户不构成犯罪，两种软件只是单方面向境外计算机系统发送访问请求，不具备非法获取计算机信息系统数据或非法控制计算机信息系统的功能，甚至目标计算机信息系统(如国外网站)允许任何用户访问，将该两类软件认定为“专门工具”是为了入罪而无视“专门工具”的技术判断，导致“提供工具罪”的滥用。

四、“提供工具罪”滥用的应对路径

本文认为，解决“提供工具罪”滥用需从三个方向同时入手：一是划清“专门工具”与“其他工具”的界限，防止滥用“专门工具”而降低入罪门槛；二是明确“专门工具”认定标准中的专业名词，防止纯技术的简单判断或者唯后果论的规范评价；三是理清“提供工具罪”中的共犯关系，防止帮助行为正犯化型罪名的滥用。

(一)区分“专门工具”与“其他工具”的关键在于程序设计目的

司法实践混淆“专门工具”与“其他工具”界限的原因之一在于，将“行为”和“目的”混为一谈。“专门工具”是“只能”被用于侵入、非法控制计算机信息系统的程序、工具，而“其他工具”是“可以”被用于侵入计算机信息系统的程序、工具，两者的区别是程序、工具的设计目的——是否以非法获取数据、非法控制计算机信息系统为目标。

1.“专门工具”不一定具有侵入功能

实践中常见的误解是：“专门工具”具有侵入功能，可以直接构成“提供工具罪”；而“其他工具”不具有侵入功能，若明知被用于实施计算机犯罪仍提供也可以构成“提供工具罪”。实际上，被用于非法获取计算机信息系统数据和非法控制计算机信息系统的程序、工具，不一定具有侵入功能。根据《刑法》第285条第二款规定，构成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有“侵入计算机信息系统”和“采用其他技术手段”两种方式。“其他技术手段”意味着使用“侵入”以外的方式非法获取计算机信息系统数据、非法控制计算机信息系统，常见的“其他技术手段”有撞库软件、[19]钓鱼网站、[20]接码平台[21]等。在“提供工具罪”语境下，撞库软件是专门用于非法获取计算机信息系统数据的“专门工具”；[22]钓鱼网站是可以被用于非法获取计算机信息系统数据的“其他工具”；[23]接码平台目前尚未涉及“提供工具罪”，对其一般按照帮助犯以帮助信息网络犯罪活动罪定罪。可见，区分“专门工具”和“其他工具”并非以是否具有侵入功能为依据，而是以实际用途为依据。

2.“专门工具”与“其他工具”的区别在于是否以“非法获取数据”“非法控制系统”为目的

“专门工具”与“其他工具”都可以被用于非法获取计算机信息系统数据、非法控制计算机信息系统，区分两者的依据是其功能设计是否以非法获取计算机信息系统数据、非法控制计算机信息系统为目的。例如，外挂软件的设计目的是节约操作时间、在竞争中作弊、获取额外操作功能等，而不是非法获取计算机信息系统数据、非法控制计算机信息系统。因此，外挂软件[24]属于“其他工具”，只有被用于实施“侵入、获取、控制三罪”时才可构成“提供工具罪”，

否则应按照侵犯著作权罪、非法经营罪等定罪。又如，钓鱼网站既可以用于获取用户的身份认证信息(即严格意义上的系统数据)，也可用于获取公民的个人信息(如身份证号码、手机号码)，只有被用于实施获取身份认证信息时才可构成“提供工具罪”。

结合限制中立帮助行为可罚性的理论，本文认为，判断提供程序、工具的行为是否可以构成“提供工具罪”，应从涉案程序的行政违法性、实际功能及设计目的三个层面进行判断(如图2所示)。

按图2的逻辑，在认定“专门工具”时，对于具有侵入功能的程序、工具，需判断其是否以“非法获取数据”或“非法控制系统”为设计目的；对于不具有侵入功能的程序、工具，还需判断其是否在“其他技术手段”的辐射范围内。具有侵入功能并不直接决定待证工具是“专门工具”还是“其他工具”，但会影响入罪路径与难度。《计算机司法解释》第二条第(一)(二)项将“避开或者突破安全保护措施”“未经授权或者超越授权”作为认定“专门工具”的条件之一，对应《刑法》第285条第2款中的“侵入计算机信息系统”；而第3款兜底性条款则为“其他技术手段”提供入罪空间。因此“非法获取数据”或“非法控制系统”是认定“专门工具”的必要条件，而“侵入(功能)”不是。将三者放在同等地位，是对司法解释的误解。

3.“非法获取数据”“非法控制系统”应受技术判断和规范评价两层限制

第一，在认定“非法获取数据”时，司法机关应更重视规范评价。对于“非法获取计算机信息系统数据”而言，“数据”在技术上指以二进制信息单元0、1的形式表示的信息载体，记录的信息包括声音、图像、符号、文字等。从技术角度理解“数据”，其范围是极为宽泛的，不能把以非法手段获取的数据都认定为“非法获取数据”。《计算机司法解释》第一条将“数据”的范围限缩为身份认证信息，无法适应实践中的复杂情况，因此需在此基础上从法律角度对“数据”的范围进行适当扩张。因此，界定“数据”的范围需要在技术判断的基础上进行规范评价，这就要考虑手段的非法性，即“非法获取数据”的“非法性”体现在所要获取的数据是合法手段无法获得的。例如，“钓鱼网站”获取用户身份认证信息属于“非法获取数据”，而“爬虫软件”抓取公开网页数据则不属于，以合法手段能够获得的数据不在“非法获取数据”的评价范围内。

第二，在认定“非法控制系统”时，司法机关应更重视技术判断。对于“非法控制计算机信息系统”而言，“控制”的词义是“使计算机系统执行管理员或用户发出的指令”。从技术判断的角度理解“非法控制”，应是使计算机系统执行“超出系统授权的指

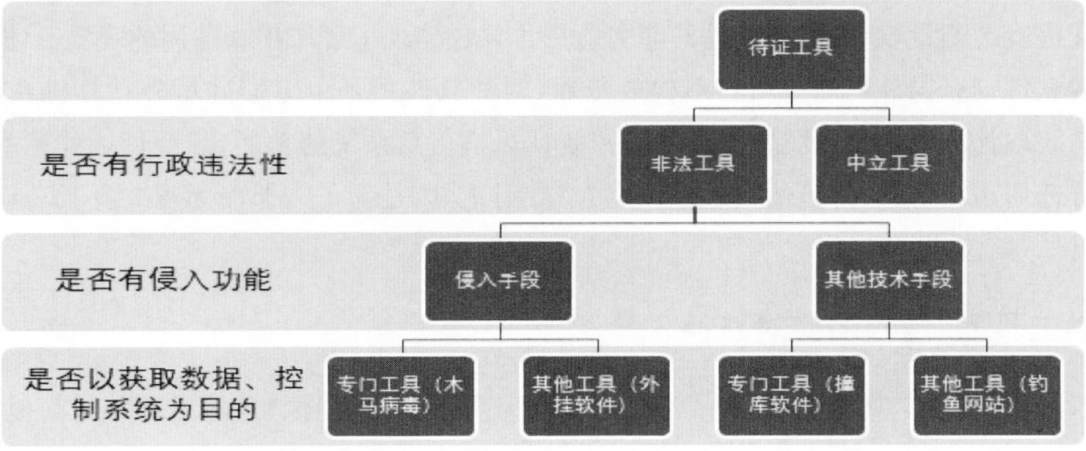

图2 “提供工具罪”认定逻辑结构

令”,而非所有“以非常规手段发送的指令”。破坏计算机信息系统的行为常“以非常规手段发送的指令”的方式实现,使系统无法正常运行。例如,手机轰炸软件通过恶意呼叫使得用户手机无法正常使用,属于破坏计算机信息系统的行为,而不能认定为非法控制计算机信息系统。“非法控制系统”的“非法性”体现在其发送给计算机执行的指令内容是未经授权或超出授权的,如木马病毒向计算机发送的“修改文件、格式化硬盘”的操作指令属于“非法控制系统”;相反,行为人私自开发第三方炒股分仓软件,通过股民账号向服务器发送的交易指令,没有超越系统的授权进行操作,就不属于“非法控制系统”。

从技术判断和规范评价两个角度综合理解“非法获取数据”“非法控制系统”,在遵循技术本质的同时结合行为的非法目的、结果判断“数据”和“控制”,避免了定义过窄,在满足司法实践需要的同时又防止了无序扩张罪名的口袋化危险。

(二)对“授权”“保护措施”做出法学定义

在司法实务中,法官一般将“侵入”理解为避开或突破计算机信息安全保护措施,未经授权或超越授权的访问行为。如何理解“访问”“授权”,是界定“侵入”的核心。有国外学者提出,对于“访问(access)”应做广义理解(即任何成功与计算机发生交互的行为),而对于“授权(authorization)”则要按照程序编码进行限制性解释。[25]我国学界并未深入讨论这几个术语,界定“侵入”的认定标准,需要先对“授权”和“保护措施”做出法学定义。

1.“授权”是程序编码设定的权限

第一,追本逐源,在计算机犯罪发源地,“授权”存在多种解释。美国《计算机欺诈和滥用法案》(下简称“CFAA”)规定了七种计算机犯罪,也以“未经授权或超越授权”为构罪要件,[26]实践中“授权”共出现了三种解释:(1)程序编码设定的权限(下简称“技术授权”),指计算机信息系统的权利人通过程序编码等技术手段对用户的身份进行识别,进而对用户的使用权限做出限制。例如,用户只有输入账号和密码、使用特定的客户端程序、互联网协议地址、访问设备才可以访问服务器,遵循这一认证逻辑就是授权访问,采用这一观点的代表案例有莫里斯案,[27]莫里斯开发了一款“蠕虫”程序并在网络上发布,旨在证明其发现了一项计算机信息系统的重大漏洞,导致美国境内大部分计算机信息系统瘫痪。(2)服务协议约定设立的权限(下简称“合意授权”),指计算机信息系统的权利人通过服务协议条款的方式与用户约定使用权限。例如,用户在注册账户时需同意软件开发者事先拟定的用户协议及隐私条款,注册成功后方可使用软件的相应功能,遵循这些协议要求才是授权访问,采用这一观点的代表案例有洛丽·德鲁案,[28]洛丽·德鲁的女儿与少女梅根·梅尔因一些原因交恶,洛丽为给女儿出气使用虚假身份在社交网站注册账号并与梅根“交往”,随后又煽动网友对梅根实施网络暴力,导致梅根自杀。(3)以代理规则为依据的代理人权限(下简称“代理授权”),即以民事代理中的规定来判断代理人在行使访问行为时是否未经授权或超越授权。例如,公司将其社交媒体账号交由其员工使用,并以命令等公司规定的方式限制员工的使用权限,员工违反公司规定就是超越授权访问,采用这一观点的代表案例有“赛佳德仓储中心公司诉赛福佳德自存仓储公司案”,[29]赛佳德公司买通了赛福佳德公司的地方部门经理埃里克·利兰及其他几个员工,让他们利用职务之便将赛福佳德公司电脑中的商业秘密通过邮件发送给赛佳德公司。

第二,我国《刑法》未对“未经授权、超越授权”做出定义,实践中未形成统一标准。一方面,判决书很少解释“未经授权、超越授权”。笔者以中国裁判文书网为数据库,检索2012年至2023年7月间案由为“提供工具罪”的裁判文书,800余篇文书中仅有20篇在判决主文部分提及“未经授权”,仅6篇文书在判决主文部分提及“超越授权”,仅5篇对“未经授权”进行简单解释。另一方面,契约型“合意授权”也成为定罪依据。如在“张某等转发定位数据案”中,被告人张某等注册了某定位公司的会员账号后,获取了

精准定位数据，再利用其编写的程序转发给他人以牟利。按照用户协议，一个账号只能给一个客户使用，客户不能以任何形式转发其获取的定位数据。对张某“合法获取数据、违约转发数据”的行为，法院认定构成非法获取计算机信息系统数据罪。[30]这就是采用契约型“合意授权”判断“超越授权”，把张某的违约行为作为犯罪处理。张某通过购买服务的方式合法获取了定位公司的数据后，超越用户协议的授权而转发数据牟利，侵犯了定位公司的数据权、商业秘密或知识产权，主要属于民事侵权行为。即便情节严重需要定罪，也属于侵犯著作权罪，而不属于“超越授权非法获取数据”。否则，大量违反用户协议的违约行为，都可能被作为犯罪处理。

第三，我国《刑法》应当采用“技术授权”的标准判断“侵入”。“合意授权”和“代理授权”均是民事行为的权利基础，属于民法的意思自治规范，以其作为刑事违法性的认定标准有违罪刑法定原则。美国法院已经注意到，滥用CFAA会使无数用户因整体上的无害行为而受到刑事制裁并承担民事责任。例如，滥用CFAA会过度打击只是违反服务协议的用户，如在社交网站上谎报年龄与性别；也可能打击仅违反了公司规定的员工，如公司为员工提供了限制访问权限的计算机，规定仅能用于公司商业目的，而员工使用公司计算机查看棒球比赛的比分。[31]因此，在“授权”的标准上，美国联邦法院在刑事案件中普遍以“技术授权”为依据，在洛丽·德鲁案之后就很少适用“合意授权”；[32]而“代理授权”一般适用于民事赔偿。[33]相较于美国法院，我国司法机关对“未经授权”和“超越授权”尚未形成统一判断标准，导致宽松地认定“侵入行为”。未来，我国司法机关在认定“侵入行为”时，应以“技术授权”作为判断标准，并在裁判文书中阐明“授权”的来源与内容，以明确区分违约、侵权与犯罪的界限。

2.“安全保护措施”仅限于系统安全和网络安全保护措施

第一，计算机犯罪语境下的“安全保护措施”是技术上的安全保护措施。“安全保护措施”在计算机领域没有统一定义。国际标准化委员会对“计算机安全”的定义是“为数据处理系统建立和采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。”在计算机领域，“安全保护措施”是一个包含硬件、软件、数据等多个层面的广义概念。有学者指出，要建立一个完整的网络信息安全系统，至少应包括三类措施：法律法规、规章制度和安全教育等外部措施、技术措施以及审计和管理措施。[34]可见，计算机领域的“安全保护措施”是一个含义多变的概念。对此可以看一下计算机发源地的做法，美国《计算机欺诈和滥用法案》并没有规定“保护措施”，而是以“受保护的(protected)计算机”指称犯罪对象。在实务中，连接到互联网的计算机均可认定为“受保护的计算机”，[35]而连接内部网络或不联网的计算机则不属于保护对象。本文认为，计算机犯罪语境下的“保护措施”首先应是在计算机信息系统连接公共网络时起保护作用的技术措施，法律法规等外部措施与审计、管理措施，因不直接作用于计算机信息系统的联网机制而应被排除在外。

第二，“提供工具罪”语境下的“保护措施”不涉及硬件与环境安全、数据库安全与应用系统安全。一般认为，技术上的安全保护措施具体可分为五种类型：硬件与环境安全、操作系统安全、网络安全、数据库安全、应用系统安全。[36]

本文认为，《刑法》上的“保护措施”不包括硬件与环境安全、数据库安全、应用系统安全，理由如下：

首先，“硬件与环境安全”属于固定设备安全，没有现代计算机的特殊属性。无论是针对计算机信息系统实施的狭义计算机犯罪，还是通过网络实施的广义网络犯罪，均与虚拟网络世界有关，而硬件和环境安全主要是固定设备层面的。现代计算机的主要特征是联网，否则，传统汽车、冰箱、车床的操作系统，都会被认定为“计算机信息系统”。文件加密技术、硬件访问控制技术、防电磁泄漏技术、

防复制技术等具体措施，主要防止他人使用移动存储设备或外接设备非法获取计算机信息系统内存储的数据，与计算机信息系统是否联网无关，其同外部措施和管理措施一样，不是“计算机的安全保护措施”。

其次，按照我国《刑法》的归类，“数据库安全”属于破坏计算机信息系统罪的评价范围。“数据库安全”与“网络安全”的保护措施存在一定程度的重叠，如防火墙、高强度身份认证系统等，这些措施主要防止数据库中的数据被用户非法获取。而剔除重合部分，数据库安全的保护措施主要防止数据被非法用户删除、修改、增加。按照《刑法》第286条规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，应评价为破坏计算机信息系统罪，故意制作、传播计算机病毒等破坏性程序的也依照破坏计算机信息系统罪处理。因此在防止非法“获取”数据的保护措施已被“网络安全”涵盖的情况下，将“数据库安全”从“提供工具罪”语境下的“保护措施”中剔除，有利于实践分清“提供工具罪”和破坏计算机信息系统罪。

再次，“应用系统安全”属于“代理授权”或“合意授权”评价的内容。“应用系统安全”中的验证输出数据、审查日志、管理用户访问、责任分离等措施虽需通过技术手段实现，但本质是管理措施的延伸，主要防范系统内部网络的违规操作而非公共网络。其防护对象是系统管理人员和合法用户，防止用户的错误操作对系统自身造成破坏。例如，在“张某等转发定位数据案”中，张某经营的公司曾为该定位公司的分销商，其获取的数据来源于分销系统，该公司发现张某转发数据行为后更新了分销系统服务协议与用户协议，明确规定禁止转发数据，且终止张某公司的分销商资格，但张某编写程序突破系统的账号认证、位置识别、处置转发行为等保护措施，继续转发数据。该行为与“赛佳德仓储中心公司诉赛福佳德自存仓储公司案”中员工擅自转发公司的商业机密类似，即“获取”数据合规而“转发”数据违规，属于违反“代理授权”或“合意授权”的行为。因此突破“应用系统安全”的安全防护措施应属于民事违约或侵权而非刑事犯罪。

最后，“操作系统安全”的主要功能是控制系统的运行、管理计算机各种资源、防止计算机信息系统被他人非法控制；“网络安全”主要是阻止非法用户远程实施对计算机信息系统的非法访问、破坏或者拦截，防止计算机信息系统的数据被非法获取。因此，“操作系统安全”和“网络安全”符合“提供工具罪”中“保护措施”的定义，我国司法实践基本上也是按照这一思路认定“提供工具罪”。

综上所述，“提供工具罪”语境下“保护措施”的法学定义是“为保护计算机信息系统的操作系统安全与网络安全所采取的技术措施”。根据该定义，长城防火墙等国家网络安全监管措施属于政策层面的外部措施，公司对于员工IC卡的使用限制规定属于审计和管理措施，两者都不是为保护操作系统和网络安全而采取的技术措施。因此，使用翻墙软件、使用复制的IC卡不属于侵入计算机信息系统，提供翻墙服务、出售IC卡的行为也不构成“提供工具罪”。未来，我国应以司法解释的方式规定“保护措施”的具体类型，将法律法规、规章制度和安全教育等外部措施，以及审计和管理措施排除在外，让司法机关更清晰地理解“提供工具罪”的适用场景。

(三)以被帮助行为的性质限制罪名适用

帮助行为的正犯化，不代表正犯行为与帮助行为的完全“松绑”。“提供工具罪”的入罪与量刑有独立标准，但其定性不应完全脱离被帮助行为的性质。在被帮助行为构成“侵入、获取、控制三罪”时，提供工具者可以成立“提供工具罪”没有争议，而被帮助行为构成其他罪名或不构成犯罪时，应限制“提供工具罪”的适用。

1.被帮助行为人构成其他罪名分两种情形

在“提供工具罪”中，被帮助者以其他罪名定罪存在两种可能：一是被帮助者同时构成“侵入、获取、控制三罪”和其他犯罪，以择一重罪处罚的定罪规则

处理;二是不考虑被帮助行为人的行为性质,以行为人提供“专门工具”为依据入罪。

第一,被帮助者择一重罪处罚时只能以“其他工具”入罪,此时应以行为人“明知”他人实施了“侵入、获取、控制三罪”为构罪要件。以钓鱼网站为例,钓鱼网站是“其他工具”,既可以被用于获取账号、密码等身份认证信息;也可以被用于获取身份证号码、手机号码、银行卡密码等个人信息;亦可以被用于实施诈骗、盗窃、信用卡诈骗等犯罪。所以,只要在行为人明知他人实施“侵入、获取、控制三罪”仍为其提供钓鱼网站时才可以认定为“提供工具罪”。

第二,以行为人提供“专门工具”为依据入罪,应严格遵循“专门工具”的认定标准。一方面,“专门工具”以非法获取计算机信息系统数据和非法控制计算机信息系统为目的,在解释“非法获取数据”“非法控制系统”时应从技术和规范两个角度综合理解,严格区分“专门工具”与“其他工具”(对应《计算机司法解释》第二条第(一)(二)项中“获取计算机信息系统数据功能”“控制计算机信息系统功能”)。另一方面,“专门工具”有“具有侵入功能的程序、工具”和“其他技术手段”两类。“具有侵入功能的程序、工具”是具有避开或突破计算机信息系统安全保护措施、未经授权或者超越授权访问计算机信息系统功能的程序、工具(对应《计算机司法解释》第二条第(一)(二)项),“其他技术手段”的范围应参照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的规定(对应《计算机司法解释》第二条第(一)项)。

2. 被帮助者不构成犯罪时只能以“专门工具”入罪

当被帮助者不构成犯罪时,“明知‘侵入、获取、控制三罪’”这一要件无法成立,无法以“其他工具”入罪,只能以“专门工具”入罪。需要注意,在“被帮助者不构成犯罪”而以“专门工具”入罪时,也不能脱离共犯关系的钳制,即“被帮助者不构成犯罪”仅是诉讼法上的无罪而非实体法上的无罪。诉讼法上的无罪情形包括:(1)(有预备行为)未着手实施犯罪的;(2)情节轻微,未达入罪标准,不作为犯罪处理的;(3)查证成本过大或无法查证,现有证据无法证明其构成犯罪的;(4)符合《中华人民共和国刑事诉讼法》其他不起诉规定的(如相对不诉、合规不诉)。若被帮助者的行为在实体法上无罪,则不能以“提供工具罪”入罪。例如,提供作弊型外挂软件、翻墙软件,使用者(被帮助者)在实体法上无罪,对提供工具者只能寻找非法经营罪、侵犯著作权罪、拒不履行信息网络安全管理义务罪等其他入罪路径。

五、结语:刑法对技术应持宽容之心

在网络犯罪激增的当下,刑法应当“打早打小”但不能打中立技术。《刑法》第285条最初以保护国家事务、国防建设、尖端科学技术领域的计算机信息系统安全为目的。随着移动智能设备的普及,非法技术成为孕育网络犯罪的温床,立法者意识到对非法网络帮助行为有独立处罚的必要性,应为共犯行为设立独立罪名,“提供工具罪”应运而生。自本罪设立以来,非法技术更新迭代,网络犯罪手段也层出不穷,“提供工具罪”的打击范围也随之扩大,具有一定中立性的程序和工具逐渐成为打击对象。刑法应当推动技术的正当化使用,但不能过度干预技术,在技术高速进步与法律相对滞后的张力中,刑法不妨“让技术飞一会”。传统共犯理论难以应对日益严重的网络犯罪,司法者采用积极刑法观扩大刑法打击范围,对于治理网络空间乱象具有正面意义。但是,在传统刑法向预防刑法转变时,刑法应当为技术留下缓冲余地,在认定技术型网络犯罪时应当恪守罪刑法定原则,既要编织严密法网也要为技术发展提供空间。

注释:

①参见北京市丰台区人民法院(2019)京0106刑初1813号刑事判决书。

②参见梅礼匀:《提供给VPN“翻墙”服务的行为如何定性》,载《人民检察》2019年第6期。

③参见上海市宝山区人民法院(2018)沪0113刑初1606号刑事判决书。

④参见皮勇:《全国首例撞库打码案的法律适用分析》,载《中国检察官》2019年第6期。

⑤周华:《论网络犯罪及其刑法规制——以网络钓鱼为观察对象》,载《法制与社会》2010年第24期。

⑥参见杨毅:《操控恶意呼叫软件构成破坏计算机信息系统罪》,载《人民司法》2021年第5期。

⑦参见郑义嘉、陈芳:《非法控制他人计算机进行拒绝服务攻击行为之定性》,载《人民司法》2012年第4期。

⑧截至2023年7月30日,以破坏计算机信息系统罪对使用DDoS软件的行为进行定罪的判决有95起,以非法控制计算机信息系统罪进行定罪的判决有58起。

⑨全国人大常委会法工委刑法室编:《中华人民共和国刑法条文说明、立法理由及相关规定》,北京大学出版社2009年版,第592页。

⑩Orin S. Kerr, Cybercrime´s Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statute, New York University Law Review. Vol. 78, 2003, p. 1605.

⑪参见杨志琼:《非法获取计算机信息系统数据罪"口袋化"的实证分析及其处理路径》,载《法学评论》2018年第6期。

⑫李永升编:《刑法新增和修正罪名适用》,中国人民公安大学出版社2013年版,第252页。

⑬参见山西省太原市迎泽区人民法院(2017)晋0106刑初583号刑事判决书。

⑭参见周光权:《通过刑罚实现积极的一般预防——国内首起"黄牛"抢购软件案评析》,载《中国法律评论》2018年第2期。

⑮参见江苏省常州经济开发区人民法院(2021)苏0492刑初317号刑事判决书。

⑯参见浙江省苍南县人民法院(2017)浙0327刑初546号刑事判决书。

⑰参见喻海松:《〈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〉的理解与适用》,载《人民司法》2011年19期。

⑱参见安徽省含山县人民法院(2020)皖0522刑初21号刑事判决书。

⑲参见江苏省宿迁市中级人民法院(2020)苏13刑终23号刑事裁定书。

⑳参见江苏省苏州市吴江区人民法院(2021)苏0509刑初1065号刑事判决书。

㉑参见江苏省徐州市泉山区人民法院(2021)苏0311刑初441号刑事判决书。

㉒参见最高人民检察院第十八批指导性案例中的"叶源星案"。

㉓参见浙江省丽水市中级人民法院(2017)浙11刑终67号刑事判决书。

㉔并非所有外挂软件都具有侵入功能,此处仅指具有侵入功能的外挂软件。

㉕同前注⑩,Orin S.Kerr文。

㉖除了1030(a)(5)(A)(i)与(a)(7)款。

㉗See United States v. Morris, 928 F. 2d 504(1991).

㉘See United States v. Drew, 259 F. R. D. 449(2009).

㉙See Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121(2000).

㉚参见浙江省湖州市中级人民法院(2021)浙05刑终87号刑事裁定书。

㉛See David J. Schmitt, the Computer Fraud and Abuse Act Should Not Apply to The Misuse of Information Accessed with Permission, Creighton Law Review, Vol. 47, 2014, p. 423.

㉜洛丽·德鲁被指控违反CFAA规定,未经授权或超越授权访问计算机,非法获取信息。法院最终依据宪法上的明确性原则,判定以"违反服务协议条款"为由认定刑事违法性不当,撤销了对洛丽的指控。

㉝参见高仕银:《计算机网络犯罪规制中的"未经授权"与"超越授权"——中美比较研究》,载《时代法学》2020年第1期。

㉞参见赵瑞霞:《浅谈涉密计算机网络的安全防护措施》,载《网络安全技术与应用》2010年第5期。

㉟See Simmonds Equipment, LLC v. GGR Intern., Inc., 126 F. Supp. 3d 855(2015).

㊱参见耿珺:《计算机信息系统安全防护措施探讨》,载《信息与电脑(理论版)》2011年第12期。