游戏公司刑事司法实务系列二
游戏公司高发涉计算机信息系统犯罪透视与应对

作者：王旭东 | 龙家乐

随着中国游戏产业的蓬勃发展，游戏行业以其规模庞大、技术密集、利益交织的特点，成为了国民经济的重要组成部分。但是，在行业繁荣的背后，围绕数据、流量、技术优势的灰色乃至黑色竞争也日益猖獗。从早期的“外挂”、“私服”，到“数据爬取”、“流量劫持”，再到“服务器攻击”、“数据库入侵”，各类涉计算机信息系统犯罪的行为随着技术手段的不断提升，已经给行业的健康发展造成了巨大的隐患和威胁。

本文旨在对游戏公司高发涉计算机信息系统犯罪的三大核心罪名：《刑法》第 285 条的【非法获取计算机信息系统数据、非法控制计算机信息系统罪】及【提供侵入、非法控制计算机信息系统程序、工具罪】，以及《刑法》第 286 条的【破坏计算机信息系统罪】进行剖析和解读，以法律规定为基础，结合司法实践案例和笔者亲身经历，深入探讨法律前沿与疑难问题，理清刑事证明中的关键和难题，为游戏公司提出一套系统、可操作的刑事合规与风险防范建议。

一. 核心罪名解析

游戏领域涉计算机系统犯罪，本质上是将计算机信息系统作为犯罪对象或工具，以实现不正当的商业目的。相关法律规定主要体现在《刑法》第 285 条和 286 条。

(一) 非法获取计算机信息系统数据、非法控制计算机信息系统罪

根据《刑法》第 285 条第 2 款的规定，违反国家规定，侵入前款规定(国家事务、国防建设、尖端科学技术领域的计算机信息系统)以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，构成此罪。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

在游戏领域，常见的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行为表现为：未经授权，通过技术手段爬取他人的用户数据、角色信息、交易记录以及游戏代码等；攻击竞争对手的服务器，窃取用户数据库，或者利用已获取的账号密码信息，尝试登录其他游戏平台(撞库)；通过外挂、木马病毒等方式，非法控制游戏客户端或者服务器端，修改游戏数据、改变游戏操作，扰乱游戏平衡等。

在实践过程中，上述行为一般存在较为复杂的竞合关系。如在笔者曾处理的某起相关案件中，犯罪嫌疑人派员以员工身份入职受害游戏公司，在受害公司内部植入木马程序，病毒通过内网蔓延，成功控制受害公司 20 余台电脑；犯罪嫌疑人控制相关电脑后，通过相关电脑上存储的游戏后台链接、账号和密码，登录游戏后台，浏览了用户信息、进行了禁言解除等操作；同时，犯罪嫌疑人还导出并复制了被控制电脑内存储的大客户信息表。上述案件中，既存在派员潜伏这种少见但极端的犯罪手法，也存在非法控制和非法获取的竞合，给相关犯罪的预防和办案带来了极大的困难。

(二) 提供侵入、非法控制计算机信息系统程序、工具罪

根据《刑法》第 285 条第 3 款的规定，提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、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，情节严重的，构成此罪。

该罪在游戏领域的典型表现形态就是外挂程序，具体表现为：开发、销售、传播能够修改游戏数据、盗取游戏资源、自动执行游戏操作的游戏外挂，或者开发针对游戏营销活动能够绕过游戏公司验证机制批量注册账号的“刷量工具”等。

(三) 破坏计算机信息系统罪

根据《刑法》第 286 条的规定，违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的；或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，后果严重的；或故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，均构成此罪。

该罪在游戏领域的典型表现主要是：DDoS 攻击，即通过分布式的拒绝服务攻击，向竞争对手的服务器发送海量无效请求，耗尽服务器资源，导致游戏卡顿或者服务器瘫痪；利用系统漏洞，侵入游戏服务器，恶意删除游戏数据或玩家存档信息；离职员工或外包开发者在编写的代码中植入恶意程序，使其在特定条件下被触发，进而导致游戏服务器崩溃或功能异常。

二. 法律适用的前沿与疑难问题

在司法实践中，游戏产业的虚拟性、技术性和强交互性，使得传统刑法条文在适用时遇到了一定挑战，笔者将从以下几点就相关法律适用的前沿与疑难问题进行分析。

(一) “技术中立”与“犯罪故意”的辨析

在游戏公司涉计算机系统犯罪案件中，“技术无罪”通常是被告的主要辩护理由。如何将一个行为从“技术创新”或“不正当竞争”中剥离，并赋予其刑事犯罪的评价，是处理所有问题的起点。

上海市第二中级人民法院在(2023)沪 02 刑终 541 号案件中，确立了以“功能违法性+目的非法性”为核心的审查标准，对《刑法》第 285 条中的“专门程序”作了具体认定。该判决紧扣涉案程序是否具备侵入计算机信息系统的核心功能，进而判断其是否是以非法获取数据、非法控制系统为实质目的，兼顾对涉案程序的技术功能、实际用途与设计意图的审查。这解决了同类案件中“技术中立抗辩”的认定难题，明确若程序的核心功能是被用于非法用途且存在非法目的，即符合“专门程序、工具”的认定标准。

(二) 罪名界分与认定的实践难题

非法控制计算机信息系统罪要求“实现排他性或主导性操作”；而破坏计算机信息系统罪强调“造成系统不能正常运行”；非法获取计算机信息系统数据罪要求以“侵入或其他技术手段”为前提，且对计算机信息系统数据的认定有较为严格的要求。但在游戏场景中，部分行为既实现控制又造成破坏、既进行了侵入又获取了数据。

如在笔者曾处理的一起案件中，犯罪嫌疑人在被害人公司内网系统中种植了木马程序，控制了数十台被害人公司的电脑设备，但同时因为木马程序的介入造成了被害人公司数十台电脑设备无法正常使用；犯罪嫌疑人控制被害人公司电脑以后，在被害人公司电脑内获取了上千条玩家信息。在办案过程中，被害人公司主张种植木马控制电脑的行为同时导致电脑无法使用，属于手段行为与结果行为的牵连犯，应当择一重罪处罚，即优先适用法定刑更高的破坏计算机信息系统罪，但对于是否“造成系统不能正常运行”的判断，则要按照《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》的相关规定进行综合判断，从系统功能受损的角度来审度是否对计算机信息系统的功能进行删除、修改、增加、干扰等操作，导致系统无法按照设计目的正常运行，如系统崩溃、无法启动、运行过程中频繁死机、数据丢失或错误显示等，使系统失去或部分失去其应有的功能，无法为用户提供正常的服务或支持。[1]

另外，针对犯罪嫌疑人在被害人电脑内获取上千条玩家信息的行为，被害人主张该行为是控制系统后实施的一个新的行为，即非法获取计算机信息系统数据的行为，应该数罪并罚。但根据

[1] 《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 4 条第 1 款。

《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》的相关规定，若要构成非法获取计算机信息系统数据罪，嫌疑人获取的玩家信息必须符合“身份认证信息”。[2]在实践中，这类信息可能是指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。在该案中，嫌疑人获取的玩家信息组成非常复杂，并非单纯的“身份识别信息”；后经鉴定机构鉴定，最终认定为“身份识别信息”的仅几百余组，尚未构成“五百组以上”的“情节严重”标准。[3]

(三) “情节严重”与“后果严重”的量化与质化标准

“情节严重”与“后果严重”是区分罪与非罪、罪轻与罪重的关键。

针对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罪，根据《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》的相关规定，“情节严重”主要体现在数量标准上，如获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上，或其他身份认证信息五百组以上；非法控制计算机信息系统二十台以上；违法所得五千元以上等。[4]在游戏行业的语境下，正如上文中提到的案例，对于获取游戏账号密码、虚拟财产信息等，如何折算为“身份认证信息”存在争议。实践中，往往结合信息的敏感性(如是否绑定支付工具)、获取数量、造成的经济损失(如账号内虚拟财产价值)等进行综合认定。另外，就非法控制而言，有些情形下虽未造成重大损失或控制的计算机系统单位价值不高，但数量足够的情况下，也足以认定为“情节严重”。[5]

针对破坏计算机信息系统罪而言，根据《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》的相关规定，“后果严重”的一般包括经济损失标准，如造成经济损失一万元以上，或造成商业信誉、形象严重损害；和系统影响标准，如造成十台以上计算机信息系统的主要软件或者硬件不能正常运行，或对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作等。[6]在游戏行业的语境下，一次成功的 DDoS 攻击可能导致游戏服务器瘫痪数小时，造成玩家流失、充值锐减、品牌声誉受损。这种“间接经济损失”和“商誉损失”难以精确计算，在案件办理过程中游戏公司需要通过玩家日志、充值流水比对、舆情监测报告等证据，作为“后果严重”的证据加以佐证。

三. 刑事证明的困境及解决方案

游戏行业的涉计算机系统犯罪具有高级性、易逝性和复杂性等特点，给相关的案件侦办和审理带来巨大的困难。正如笔者在《游戏公司刑事司法实务一》一文中所述，电子证据的收集与保全，需要遵

[2] 《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 1 条第 1 款第 2 项。
[3] 同前注 2。
[4] 《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 1 条第 1 款。
[5] 《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 1 条第 1 款第 3 项。
[6] 同前注 1。

循严格的法定程序，确保数据证据的合法性和完整性。在遇到相关侵害行为时，需要及时对公司的服务器数据进行封存和备份，防止数据被篡改和丢失，通过专业的技术手段，提取与案件相关的操作日志、玩家账号信息、虚拟财产交易记录等数据。在实际操作中，可聘请专业的电子数据鉴定机构，运用数据分析软件对大量的后台数据进行筛选、比对和可视化处理，以发现潜在的犯罪线索和证据链条。同时，日常取证中也要善于使用区块链取证工具。除此之外，针对游戏服务器日志数据，需要建立完善的日志管理系统，能够记录并追溯用户登录 IP、行为序列、异常操作、数据请求来源等。通过对攻击 IP、异常数据包特征、外挂行为模式的关联分析，可以构建完整的证据链。

除了上述证据固定问题外，游戏公司涉计算机系统犯罪还存在主观故意证明难题和因果关系与损失认定的难题。

(一) 犯罪主观故意的证明难题

在涉计算机系统犯罪案件中，如何证明被告人“明知”自己提供的程序是用于侵入、非法控制计算机系统的?如何证明攻击具有破坏的故意?司法实践中，主观故意往往通过客观行为来进行推定。如对于外挂提供者：其程序具有明显的规避安全检测的特征；其在销售和宣传中使用了“防封号”、“破解版”等词语；其主动、频繁地更新程序以对抗游戏官方的安全补丁，这些行为链条足以推定其“明知”。如对于数据爬取者：其使用了伪造 User-Agent、代理 IP 池、绕过验证码等技术手段；其爬取行为违反了网站的 Robots 协议；其爬取的数据明显超出了正常业务所需范围，这些都可以作为具有非法获取数据故意的证据。同时，同案犯的供述、下游购买者或使用者的证言，可以与客观证据相互印证，形成完整的证明体系。

(二) 因果关系与损失认定的难题

在破坏计算机信息系统罪中，如何证明 DDoS 攻击与服务器瘫痪之间的因果关系?如何量化因服务器瘫痪导致的玩家流失和收入损失?

在司法实践中，可以通过技术关联来认定行为和损害结果之间的因果关系，如通过网络流量分析，精确锁定攻击流量来源、类型和攻击时间，并与服务器性能监控图表(CPU、内存、网络带宽使用率)进行时间点上的精确匹配，建立技术上的因果关联。

在经济损失的证明上，可以采取多维度的评估标准，除了直接经济损失和维修费用外，受害人还可以向法院提供直接营收损失的佐证，如系统被攻击期间与历史同期、相邻时间的流水对比；通过数据分析，评估攻击期间及之后一段时间内，活跃用户数、付费用户数的异常下降，并估算其生命周期价值(LTV)的损失；委托司法和审计机关进行鉴定和资产评估并出具经济损失鉴定意见的相关费用，也可以主张作为损失向法院提交。

四. 游戏公司相关风险防范建议

面对日益复杂和增加的涉计算机系统犯罪案件，游戏公司应当从被动防御和主动防控两个角度，构建全方位的刑事防控合规体系。

(一) 构建内部刑事合规制度

其一，制定清晰的制度红线。在公司内部的规章制度中，明确禁止以任何形式实施开发、使用及传播外挂，参与 DDoS 攻击，非法爬取数据等行为，同时明确违反后果为直接解除劳动合同并移交司法机关。

其二，建立员工培训与承诺机制。定期对全体员工，尤其是技术、运营、市场岗位的员工进行涉计算机犯罪的法律风险培训，并要求关键岗位员工签署《合规承诺书》，使其明确知晓行为边界。

其三，设立独立的举报渠道。建立独立、保密的内部举报渠道，鼓励员工举报内部违规行为，并对主动举报的员工予以保护。

(二) 强化技术防护与监测能力

其一，构建防御安全体系。构建防御安全体系，围绕网络边界、服务器主机到应用程序，搭建多层次的防护体系，具体包括部署 WAF(Web 应用防火墙)、DDoS 高防 IP、入侵检测系统(IDS/IPS)等。

其二，推行常态化安全性测试。定期委托第三方白帽黑客对旗下的游戏产品开展渗透测试，提前发现潜在的安全漏洞，并及时完成修复。

其三，搭建大数据风控与反外挂系统。可以依托 AI 和大数据算法，构建实时行为分析模型，对游戏内的异常行为(如移动轨迹异常、操作频率过高、资源超速获取)进行实时监测和自动处置，实现对外挂的精准识别和快速封禁。

(三) 规范第三方合作管理

首先，进行严格的供应商尽职调查。在与外包技术团队、营销公司、数据服务商合作前，对其进行一定的背景调查和合规审查。

其次，明确协议中的责任约定。在协议中明确约定，合作方不得从事任何涉及计算机犯罪的行为，并设置违约金条款和单方解约权，一旦发现违规行为，立即终止合作并追究其责任，以隔绝风险。

(四) 建立应急响应和司法协作机制

其一，制定应急预案与突发事件响应机制。预先制定针对 DDoS 攻击、数据泄露、外挂泛滥等突发事件的处置流程，进而最大限度降低突发事件对业务系统运行、用户权益及企业声誉造成的影响和损失。

其二，主动配合司法工作。在发现犯罪行为时，不应止于自行封禁，而是应第一时间通过公证或区块链固定证据，并主动向公安机关报案，积极配合调查。这不仅能打击犯罪行为，也能向行业和用户展示公司维护公平竞争环境的决心。

五. 结语

游戏行业的高速发展，伴随着涉计算机信息系统犯罪的技术迭代与形态演变，从外挂到 AI 辅助、从数据爬取到服务器攻击，既考验司法对新型犯罪的规制能力，也倒逼企业强化合规。未来，唯有企业筑牢合规防线、司法精准追责、行业协同规范，才能扭转“重创新轻合规”的惯性，守护游戏生态健康，为数字经济发展注入合规动力。

如您希望就相关问题进一步交流，请联系：

王旭东
+86 755 3391 7631
edward.wang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野