

网络黑灰产问题处置指南

(第 2 版)

反网络黑灰产联盟

2025 年 3 月

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

前言

随着互联网与信息科技的飞速发展，各类网络黑灰产问题层出不穷，逐步成为当前社会网络安全面临的一大挑战。所谓网络“黑灰产”，是指通过非法或不道德的手段，在网络空间进行的各种违法违规活动。其中，“黑产”指的是直接触犯国家法律的网络犯罪，具体而言，是指利用互联网技术实施网络攻击、窃取信息、勒索诈骗、盗窃钱财、推广黄赌毒等网络违法行为，以及为这些行为提供工具、资源、平台等准备和非法获利变现的渠道与环节。^①“灰产”则是游走在法律边缘，为“黑产”提供辅助的争议行为。网络黑灰产的持续滋长将导致包括扰乱市场秩序、侵犯公民个人信息等在内的各类社会负面问题的出现。从联盟工作情况看，绝大多数成员企业在业务开展的过程中都遭遇过此类问题的袭扰，甚至因此蒙受损失。网络黑灰产已经演变成为企业正常经营过程中的众多挑战之一。

鉴于此，在上海市徐汇区人民检察院、上海市公安局徐汇分局的指导下，由易玩（上海）网络科技有限公司，心动网络股份有限公司发起，反网络黑灰产联盟统筹汇编，阿里云、网易易盾、腾讯安全、腾讯游戏安全、天际友盟、极验GEETEST、百事通法务等多家主体共同参与制订了《网络黑灰产问题处置指南》（以下简称《指南》）。

本《指南》旨在围绕各类黑灰产问题，从概念简述、常见类型介绍、法律法规及政策解读、应对处置策略等方面为

^① 夏晓伦、董思睿：《图解黑色产业链该如何防范？》，
http://www.cac.gov.cn/2019-10/08/c_1572062776375154.htm，2023年10月。

企业提供合规性指引，为企业提供实际参考，帮助互联网企业更有效地应对和处置网络黑灰产问题，进而促进社会各方对网络黑灰产问题认知的提高，共同努力维护并构筑清朗健康的网络安全环境和秩序。

本指南由以下单位共同编写：

指导单位：

上海市徐汇区人民检察院

上海市公安局徐汇分局

发起单位：

易玩（上海）网络科技有限公司

心动网络股份有限公司

总编单位：

反网络黑灰产联盟工作小组

参与单位：（排名不分先后）

阿里云计算有限公司

上海政法学院刑事司法学院

杭州网易智企科技有限公司

武汉极意网络科技有限公司

腾讯云计算（北京）有限公司

北京天际友盟信息技术有限公司

上海百事通法务信息技术有限公司

目录

一、 DDoS 攻击	1
(一) DDoS 攻击的概念	1
(二) DDoS 攻击常见类型	1
(三) 法律法规及政策解读	3
(四) 事前防范措施	5
(五) 事中应对策略	8
(六) 事后处置方案	9
二、 游戏外挂	10
(一) 游戏外挂的概念	10
(二) 游戏外挂的类型	11
(三) 法律法规及政策解读	13
(四) 事前防范措施	15
(五) 事中应对策略	16
(六) 事后处置方案	17
三、 侵犯著作权	19
(一) 著作权的概念	19
(二) 侵犯著作权的常见场景	19
(三) 法律法规及政策解读	20
(四) 事前防范措施	24
(五) 事中应对策略	25
(六) 事后处置方案	27

四、 账号交易	29
(一) 账号交易的概念	29
(二) 非法账号交易的常见形式	29
(三) 法律法规及政策解读	30
(四) 事前防范措施	31
(五) 事中应对策略	33
(六) 事后处置方案	34
五、 违规信息内容	35
(一) 违规信息的概念	35
(二) 常见违规信息类型	35
(三) 常见的攻击方式	36
(四) 法律法规及政策解读	37
(五) 事前防范措施	39
(六) 事中应对策略	40
(七) 事后处置方案	41
六、 游戏欺诈	43
(一) 游戏欺诈的概念	43
(二) 游戏欺诈的高危场景	43
(三) 法律法规及政策解读	45
(四) 事前防范措施	48
(五) 事中应对策略	49
(六) 事后处置方案	52

七、 游戏私服	53
(一) 游戏私服的概念	53
(二) 游戏私服的常见表现形式	53
(三) 法律法规及政策解读	54
(四) 事前防范措施	55
(五) 事中应对策略	57
(六) 事后处置方案	58
八、 网络暴力	61
(一) 网络暴力相关概念	61
(二) 网络暴力的类型	61
(三) 法律法规及政策解读	63
(四) 事前防范措施	65
(五) 事中应对策略	68
(六) 事后处置方案	69

一、DDoS 攻击

（一）DDoS 攻击的概念

分布式拒绝服务（Distributed Denial of Service，简称 DDoS）是指将多台计算机联合起来作为攻击平台，通过远程连接，利用恶意程序对一个或多个目标发起 DDoS 攻击，消耗目标服务器性能或网络带宽，从而造成服务器无法正常地提供服务。

（二）DDoS 攻击常见类型

1. 畸形报文

主要包括 Frag Flood、Smurf、Stream Flood、Land Flood、IP 畸形报文、TCP 畸形报文、UDP 畸形报文等。畸形报文攻击指通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的报文时出现崩溃，从而达到拒绝服务的攻击目的。

2. 传输层 DDoS 攻击

传输层 DDoS 攻击主要包括 Syn Flood、Ack Flood、UDP Flood、ICMP Flood、RstFlood 等。以 Syn Flood 攻击为例，它利用了 TCP 协议的三次握手机制，当服务端接收到一个 Syn 请求时，服务端必须使用一个监听队列将该连接保存一定时间。因此，通过向服务端不停发送 Syn 请求，但不响应 Syn+Ack 报文，从而消耗服务端的资源。当监听队列被占满时，服务端将无法响应正常用户的请求，达到拒绝服务攻击的目的。

3. DNS DDoS 攻击

DNS DDoS 攻击主要包括 DNS Request Flood、DNS Response Flood、虚假源+真实源 DNS Query Flood、权威服务器攻击和 Local 服务器攻击等。以 DNS Query Flood 攻击为例，其本质上执行的是真实的 Query 请求，属于正常业务行为，但如果多台傀儡机同时发起海量的域名查询请求，服务端无法响应正常的 Query 请求，从而导致拒绝服务。

4. 连接型 DDoS 攻击

连接型 DDoS 攻击主要是指 TCP 慢速连接攻击、连接耗尽攻击、Loic、Hoic、Slowloris、Pyloris、Xoic 等慢速攻击。以 Slowloris 攻击为例，其攻击目标是 Web 服务器的并发上限。当 Web 服务器的连接并发数达到上限后，Web 服务即无法接收新的请求。Web 服务接收到新的 HTTP 请求时，建立新的连接来处理请求，并在处理完成后关闭这个连接。如果该连接一直处于连接状态，收到新的 HTTP 请求时则需要建立新的连接进行处理。而当所有连接都处于连接状态时，Web 将无法处理任何新的请求。Slowloris 攻击利用 HTTP 协议的特性来达到攻击目的。HTTP 请求以 \r\n\r\n 标识 Headers 的结束，如果 Web 服务端只收到 \r\n，则认为 HTTP Headers 部分没有结束，将保留该连接并等待后续的请求内容。

5. Web 应用层 DDoS 攻击

Web 应用层攻击主要是指 HTTP Get Flood、HTTP Post Flood、CC 等攻击。通常应用层攻击完全模拟用户请求，类

似于各种搜索引擎和爬虫一样，这些攻击行为和正常的业务并没有严格的边界，难以辨别。Web 服务中一些资源消耗较大的事务和页面。例如，Web 应用中的分页和分表，如果控制页面的参数过大，频繁的翻页将会占用较多的 Web 服务资源。尤其在高并发频繁调用的情况下，类似这样的事务就成了早期 CC 攻击的目标。由于现在的攻击大都是混合型的，因此模拟用户行为的频繁操作都可以被认为是 CC 攻击。例如，各种刷票软件对网站的访问，从某种程度上来说就是 CC 攻击。CC 攻击瞄准的是 Web 应用的后端业务，除了导致拒绝服务外，还会直接影响 Web 应用的功能和性能，包括 Web 响应时间、数据库服务、磁盘读写等。

（三）法律法规及政策解读

1. 直接攻击行为

根据刑法第二百八十六条【破坏计算机信息系统罪】

（1）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，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

（2）违反国家规定，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，后果严重的，依照前款的规定处罚。

（3）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，依照第一款的规定处罚。

（4）单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

2. 提供 DDoS 攻击流量、软件或专门开设 DDoS 攻击网站以非法牟利的服务者

（1）非法控制肉鸡

根据刑法第二百八十五条第二款【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】

违反国家规定，侵入前款规定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，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

（2）开设非法网站或为他人租用服务器

根据刑法第二百八十七条之二【帮助信息网络犯罪活动罪】

明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

（3）为他人提供 DDoS 攻击软件工具

根据刑法第二百八十五条第三款 **【提供侵入、非法控制计算机信息系统程序、工具罪】**

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，依照前款的规定处罚。

（四）事前防范措施

1. 缩小暴露面，隔离资源和无关业务

（1）配置安全组：尽量避免将非业务必需的服务端口暴露在公网上，从而避免与业务无关的请求和访问。通过配置安全组可以有效防止系统被扫描或者意外暴露。

（2）使用专有网络 VPC（Virtual Private Cloud）：通过专有网络 VPC 实现网络内部逻辑隔离，防止来自内网傀儡机的攻击。

2. 优化业务结构，设计弹性伸缩和灾备切换的系统

（1）科学评估业务架构性能：在业务部署前期或运营期间，技术团队应该对业务架构进行压力测试，以评估现有架构的业务吞吐处理能力，为 DDoS 防御提供详细的技术参数指导信息。

（2）弹性和冗余架构：通过负载均衡或异地多中心架构避免单点故障影响整体业务。如果您的业务在阿里云上，可以灵活地使用负载均衡服务 SLB（Server Load Balancer）

实现多台服务器的多点并发处理业务访问，将用户访问流量均衡分配到各个服务器上，降低单台服务器的压力，提升业务吞吐处理能力，这样可以有效缓解一定流量范围内的连接层 DDoS 攻击。

（3）优化 DNS 解析：通过智能解析的方式优化 DNS 解析，可以有效避免 DNS 流量攻击产生的风险。同时，建议您将业务托管至多家 DNS 服务商，并可以从以下方面考虑优化 DNS 解析：

- ① 屏蔽未经请求发送的 DNS 响应信息
- ② 丢弃快速重传数据包
 - a. 启用 TTL
 - b. 丢弃未知来源的 DNS 查询请求和响应数据
 - c. 丢弃未经请求或突发的 DNS 请求
- ③ 启动 DNS 客户端验证
 - a. 对响应信息进行缓存处理
 - b. 使用 ACL 的权限
 - c. 利用 ACL、BCP38 及 IP 信誉功能
- ④ 提供余量带宽

通过服务器性能测试，评估正常业务环境下所能承受的带宽和请求数。在购买带宽时确保有一定的余量带宽，可以避免遭受攻击时带宽大于正常使用量而影响正常用户的情况。

（4）关键内容通过 CDN 分发：通过在多个地理位置部

署多台服务器，并在边缘使用智能路由技术和缓存方式，以分散攻击时带宽，避免影响正常业务请求，同时降低网络延迟并提升访问速度。

3. 服务器安全加固，提升服务器性能

对服务器上的操作系统、软件服务进行安全加固，减少可被攻击的点，增大攻击方的攻击成本：

（1）确保服务器的系统文件是最新的版本，并及时更新系统补丁。

（2）对所有服务器主机进行检查，清楚访问者的来源。

（3）过滤不必要的服务和端口。例如，对于 WWW 服务器，只开放 80 端口，将其他所有端口关闭，或在防火墙上设置阻止策略。

（4）限制同时打开的 SYN 半连接数目，缩短 SYN 半连接的 timeout 时间，限制 SYN、ICMP 流量。

（5）仔细检查网络设备和服务器系统的日志。一旦出现漏洞或时间变更，则说明服务器可能遭到了攻击。

（6）限制在防火墙外进行网络文件共享。降低黑客截取系统文件的机会，若黑客以特洛伊木马替换它，文件传输功能将会陷入瘫痪。

（7）充分利用网络设备保护网络资源。在配置路由器时应考虑针对流控、包过滤、半连接超时、垃圾包丢弃、来源伪造的数据包丢弃、SYN 阈值、禁用 ICMP 和 UDP 广播的策略配置。

(8) 通过 iptable 之类的软件防火墙限制疑似恶意 IP 的 TCP 新建连接，限制疑似恶意 IP 的连接、传输速率。

4. 做好业务监控和应急响应

建立基础 DDoS 防护监控，一经监测到业务遭受 DDoS 攻击时接收告警信息，确保第一时间进行应急处理。此外，根据当前的技术业务架构和人员，提前建立应急技术预案，必要时可提前进行技术演练，以检验应急响应预案的合理性。

5. 提前为核心业务部署好高防

在核心业务或关键业务上线前，提高自身的网络安全防范意识，对数据包的真实 IP 进行隐藏处理，必要时可依据部署原生高防或 BGP 高防服务增强防御。如业务涉及全国地区，可选择边缘安全加速平台提升防护效果并保障业务访问效果。

(五) 事中应对策略

1. 证据收集与保全

在 DDoS 行为发生前，不法分子会通过各类通讯手段与被攻击方取得联系并进行勒索。注意收集有关勒索行为的证据，包括聊天内容的截图、社交账号、支付信息等。确保证据的完整性和安全性，以备将来维权使用。

2. 阻断勒索渠道

及时阻断不法分子与被攻击方间的沟通渠道是解决该问题一大有效方式。对涉及不法活动的社交媒体账号进行永久封停处理，能有效切断不法活动的中间环节，降低受到

DDoS 直接攻击或二次攻击的风险。

3. 依需安装 DDoS 高防服务

持续监测 DDoS 攻击的状态、原生高防或 BGP 高防水位，判断是否需要做相应的策略调整。对流量数据进行分析，识别 DDoS 攻击特征，针对性按需安装相对应的 DDoS 高防服务，保证核心业务仍能保持正常运行。

4. 合作与协调

与相关部门、行业组织、运营商及网络安全厂商合作，增强安全攻防对抗能力，形成协同合力，共同应对 DDoS 攻击问题。涉案严重时及时向相关执法部门报案。

（六）事后处置方案

1. 证据组织

通过技术手段追踪攻击来源，收集证据。其中证据包括：被攻击对象及简介、被攻击日期及时间段、攻击方名称、勒索金额、勒索用渠道及账号信息、勒索者提供的账户信息、被攻击时段的日志记录、攻击频次、聊天记录、服务器信息，详见表 1。

序号	材料明细
1	被攻击对象及简介
2	被攻击日期及时间段
3	攻击方名称
4	勒索金额
5	勒索用渠道及账号信息

6	勒索者提供的账户信息
7	被攻击时段的流量日志记录
8	攻击频次
9	聊天记录
10	服务器信息

表 1 遭遇 DDoS 攻击所需准备材料清单

2. 报案

被攻击方向司法机关诉讼或报案，提供相关证据和材料，确保案件受理的及时性和准确性。

3. 调查取证

协助配合司法机关各项办案流程。例如：提交对涉嫌犯罪的勒索者、攻击记录等进行调查取证的相关证据，参照附表 1。

4. 加强防范措施

总结经验教训，制定更加有效的防范措施。例如：实时流量监控、提前隐藏 IP 地址、必要时补充高防服务等，以避免类似的攻击勒索事件再次发生，保障业务安全稳定。^[1]

二、游戏外挂

（一）游戏外挂的概念

游戏外挂一般指通过修改游戏数据而为玩家谋取利益的作弊程序或软件。具体如，游戏外挂程序/软件利用技术手段影响游戏的内存数据、网络数据、文件数据和代码逻辑，改变游戏进程中相关的数值。

随着玩家游戏外挂需求的发展，市面上也出现不影响游戏数据的脚本，比如模拟按键类辅助和透视绘制类脚本等。

（二）游戏外挂的类型

1. 客户端破解

客户端破解版是指对游戏正版客户端修改数据资源和代码逻辑后重新生成的独立的游戏客户端，其实现方式主要包括数据资源静态分析和动态分析调试，客户端文件修改、替换等。客户端破解多用于帮助玩家获得游戏优势或者避免游戏付费等功能。

2. 脱机挂

脱机挂是指某些经过精心设计后的特定程序，利用数量可观的电脑主机（肉鸡或代理服务提供者）模拟正常的游戏客户端向游戏服务器端发送和接收数据包的过程。游戏行业发展初期，由于游戏服务端的数据校验和协议加密处理能力较差，脱机挂通过对游戏网络协议进行逆向分析，并生成独立的第三方客户端，从而让游戏厂商无法追溯损失。

3. 内存修改

内存修改类外挂是指利用内存修改工具，对游戏进程中的内存数据或者指定进程内存数据进行读写修改操作，常见的方法比如数值变化搜索、数据模糊搜索、反加密搜索等等。内存修改类外挂帮助玩家获取游戏竞争优势的同时，也可能引发玩家个人信息和账号安全受到泄露风险。

4. 加速外挂

变速类外挂一般是指利用外挂软件修改游戏内部计时器或者频率，从而控制人物的移动速度或攻击速度等。变速类外挂主要有两种实现方式，一种是通过 hook 时间 api 的形式篡改计算机的硬件时钟频率，使得游戏中的时间流逝速度发生改变，从而达到加速或者减速的效果；另一种是通过延迟数据包的发送时间来让游戏客户端误以为游戏服务器的响应时间变慢，从而达到减速的效果。

5. 定制外挂

定制外挂是指一些黑客或者外挂开发者，根据游戏玩家的需求和要求，利用自己的技术和经验，专门为某一款游戏开发并定制的外挂。定制外挂多以插件注入的形式，例如 Android 中的 so 和 iOS 中的 libdy，插件注入游戏进程以后，执行 HOOK 操作并实现外挂功能。

6. 协议抓包

协议抓包是指使用网络抓包工具，对游戏数据进行拦截和分析，以获取游戏协议、通信数据等信息，从而实现修改游戏数据和实现作弊的目的。协议抓包本质上是用于捕获和分析在计算机网络中传输的数据包，在游戏协议抓包的过程中，可以对数据包进行篡改、重发等操作，实现外挂功能。

7. 按键脚本

按键脚本在早期其实是为了方便玩家操作所开发的脚本辅助程序，而当前多被团伙工作室用于批量牟利性质，因此在某些游戏类型中其危害性不亚于修改类外挂。按键脚本

通过预先录制连续的按键操作、对游戏区域的图像色块或文字进行识别、对游戏的坐标内存进行搜索并识别等方式，实现自动按键点击的操作。

8. 窗口绘制

窗口绘制类外挂是指通过在游戏客户端窗口上绘制额外的图像或信息，从而实现提供额外的游戏信息的效果，比如显示其他玩家的位置、血量等。

9. AI 外挂

AI 外挂是基于机器学习和深度学习等技术，对游戏数据进行分析和处理，从而提供各种辅助功能，例如在射击类游戏中实现自瞄、自动设计、躲避等操作。与传统的外挂相比，AI 外挂不会通过修改游戏客户端或驱动程序的代码实现。

（三）法律法规及政策解读

1. 游戏外挂制售及传播行为

从既有的刑事裁判来看，司法机关适用的罪名经历了从非法经营罪，到侵犯著作权罪和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，再到提供侵入、非法控制计算机信息系统程序、工具罪的转变。

根据《中华人民共和国刑法》第二百八十五条第三款规定了提供侵入、非法控制计算机信息系统程序、工具罪，且明确了该罪的两行为方式，相关司法解释规定了情节严重的具体情形：

（1）提供能够用于非法获取支付结算、证券交易、期

货交易等网络金融服务身份认证信息的专门性程序、工具五十人次以上的；

（2）提供第1项以外的专门用于侵入、非法控制计算机信息系统的程序、工具二十人次以上的；

（3）明知他人实施非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的违法犯罪行为而为其提供程序、工具五十人次以上的；

（4）明知他人实施第3项以外的侵入、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、工具二十人次以上的；

（5）违法所得五千元以上或者造成经济损失一万元以上的；

（6）其他情节严重的情形。

2. 网络游戏厂商或企业侵权行为

根据《计算机软件保护条例》，有以下几条规定：

第十三条：禁止非法复制、传播、销售和使用他人已经注册登记或者未经授权的计算机软件。该条款明确禁止盗版行为，并且强调了著作权人对于自己创作的游戏软件享有合法权利。

第二十四条：禁止破坏技术保护措施，以获取不正当利益或者侵害他人合法权益。该条款旨在防范黑客攻击等风险，并且加强对于技术保护手段（如数字版权管理）的监管力度。

第二十五条：网络服务提供者应当采取必要措施，防范

恶意程序和电子病毒等危害信息系统安全行为；

第三十六条：违反本办法规定，构成犯罪的，依照刑事责任追究；情节较轻的，由公安机关处以警告、罚款等处罚。

（四）事前防范措施

1. 开展安全性评估

在游戏上线前，对游戏版本进行漏洞挖掘和风险评估，及时修复潜在漏洞及风险，并设置应急预案。

2. 加固数据资源

在游戏设计期内，注重加强对各项数据资源的保护：一是在客户端层加强代码、组件、资源加密和保护；二是在通信协议层强化数据加密；三是在服务端加强关键数据校验。

3. 保证文件完整性

定期检查客户端文件完整性，防止文件被篡改或替换。

4. 建立数据监测

建立完善的动态数据指标监测系统可以帮助发现异常游戏行为。这包括设置各种数值变化的阈值，一旦超过预设范围就触发报警机制，对异常游戏行为和外挂黑模块等及时制定反外挂策略，更高效对外挂用户进行检测打击。

5. 强化授权保护

加强游戏授权保护，避免游戏被盗版和非法修改，减少游戏外挂行为的出现。比如可以采用数字签名技术来确保游戏源码的完整性和真实性；使用许可证验证机制来限制非法复制；以及利用反调试技术来阻止黑客对游戏进行逆向工程

分析。同时，还需定期更新安全策略，并积极参与打击网络犯罪活动，以降低外挂出现的可能性。

6. 设置处置手段

在游戏运营前预设处罚接口，这些接口包括：账号封禁、踢下线、禁模式等。同时，提升游戏的准入门槛，例如通过大数据模型甄别的小号或历史作弊号禁止进入、用户进行实名认证是预防外挂的有效措施。

（五）事中应对策略

1. 建立安全运营体系

通过建立包含作弊监控体系、实时检测体系、作弊处罚体系以及客观衡量游戏安全性的指标体系为一体的安全运营体系，加强对游戏外挂问题的追踪识别和打击处置。

2. 强化内外部舆情关注

游戏运营方除了要密切关注游戏安全系统数据外，也应加强对游戏社区和外部玩家讨论环境的关注，建立有效的监测系统，及时收集整理游戏外挂相关讨论信息，一旦确认信息属实，就应立即启动对抗流程，将相关信息纳入反外挂数据库，同时封禁散布游戏外挂信息的用户和组织。此外，还可以定期进行社区巡查，对违规行为进行严格处理，以维护游戏环境的公平性，营造良好的游戏生态。

3. 设置激励性检举机制

游戏运营方可在游戏内、游戏官网及其他官方社交渠道内设置一套有效的反外挂检举机制，鼓励玩家积极参与到反

外挂行动中，并对成功检举外挂用户的玩家给予奖励。这种机制不仅能增加玩家对游戏公平性的认同感，也有利于提高发现并处理外挂用户的效率。

4. 搭建闭环处罚体系

游戏运营方可通过搭建闭环处罚体系更精准地处置外挂用户。例如：建立自动化监测系统，实时监测并识别出外挂行为，系统迅速记录并进行初步分析；对于被系统标记及用户举报的账号进行人工复审；封禁被确定的外挂用户，并对其违规行为进行公示，情节严重可纳入黑名单防止再次注册；定期通过官方渠道发布反外挂措施和打击成果等。

5. 证据收集与保全

利用技术手段追踪外挂软件的来源，并获取部分有价值线索。包括：外挂制售方信息、外挂传播路径和交易信息等证据，确保证据的完整性和安全性，以备后续跟进法律途径使用。

（六）事后处置方案

1. 证据组织

对涉嫌外挂的网络平台、售卖主体进行调查取证，收集相关的违法证据，包括外挂用户账号信息、游戏日志、外挂软件截图等材料，以更顺利开展后续报案工作。详见表 2。

序号	材料明细
1	外挂用户账号信息（IP 属地、身份信息）
2	外挂用户游戏日志（游玩记录、截图/视频）

3	外挂用户异常数据分析
4	用户提供与外挂售卖方的聊天记录
5	外挂售卖方信息（账号、联系方式）
6	外挂软件信息（代码、开发者信息、使用说明）
7	交易信息（如截图、时间、方式、金额）
8	游戏产品相关的计算机软著证书
9	如委托第三方需提供授权书、营业执照
10	对企业造成经济损失的证明文件
11	对企业声誉、商誉等方面的影响证明

表 2 遭遇外挂问题所需材料清单

2. 报案

受害方向司法机关提起诉讼或报案，提供相关证据和材料，确保案件受理的及时性和准确性。

3. 调查取证和鉴定

协助配合司法机关各项办案流程。例如：对涉嫌制售外挂团伙的设备、身份、行为特征进行调查取证，提交相关证据材料，参照表 2。

4. 定期更新，加强防护

（1）定期更新维护游戏，及时发现并修复游戏中存在的漏洞和安全问题。同时，加强对已知外挂的分析，了解其工作原理，尽可能在设计中避免出现该类情况。

（2）对游戏中的关键数据内存地址进行常态化更新，

使外挂团伙难以找到正确的修改位置。

（3）严格管控第三方售卖平台。游戏运营方可与各大平台进行合作协同，在法律范围内要求下架相关外挂辅助工具^[2]。

三、侵犯著作权

（一）著作权的概念

著作权是指著作权人和与著作权有关的权利人对作品所享有的法定权利，包括复制权、发行权、表演权、展览权、放映权、广播权、信息网络传播权等，是指对原创文学、艺术和科学领域内具有独创性并能以一定形式表现的智力成果的独占权，包括文字、音乐、美术、计算机软件等形式的智力成果。

（二）侵犯著作权的常见场景

侵犯著作权不仅会损害享有著作权的企业的品牌价值和经济效益，同时也抑制了行业的创新发展，不利于促进社会主义文化和科学事业的发展与繁荣。因此，著作权的合法有效保护对相关行业的可持续发展非常重要。互联网侵犯著作权的场景主要有以下几种：

1. 盗版和非法复制

将受保护的游戏软件、电影、音乐、图书等作品进行未经授权的复制和传播，包括制作和分发盗版光盘、破解软件、非法下载等行为。

2. 网络传播和分享

在互联网上通过网站、社交媒体、P2P 网络等方式，分享和传播他人的受保护作品，如未经授权的在线电影和音乐分享、盗版软件下载等。

3. 模仿和抄袭

未经授权使用他人的创意、图形、音乐、文字等元素，进行游戏、艺术品、文学作品的模仿和抄袭。

4. 修改和派生

未经授权修改、编辑或创建衍生作品，如未授权的游戏修改、电影或小说的衍生创作等。

5. 侵犯软件和游戏源代码

未经授权访问、修改或复制游戏软件、应用程序或游戏源代码，包括盗取游戏设计和算法等。

6. 网络盗链和转载

未经授权将他人的文章、图片、音乐、视频等内容直接链接到自己的网站或平台，或未经授权转载他人的原创内容。

7. 未经授权的广告和商业使用

在未经授权的情况下，在游戏、网站、应用程序等中使用他人的原创作品进行广告和商业推广。

以上仅为一些常见侵犯著作权的场景，实际上，随着技术的不断发展和互联网的普及，新的侵权形式正不断涌现。

（三）法律法规及政策解读

1. 国际方面

（1）数字版权保护法律：许多国家都颁布了数字版权

保护法律，以适应数字化时代的挑战。这些法律规定了在互联网上传播、分享和使用作品的规则，确保版权所有者的权益得到保护，防止未经授权的复制和传播。

（2）数字版权管理系统（DRM）：DRM 是一种技术措施，用于管理数字内容的访问和使用，以保护著作权。它可以限制非法复制、打印和传播，从而防止盗版和侵权行为。

（3）数字千年版权法案（DMCA）：DMCA 是美国的一项法规，规定了网络服务提供商（如社交媒体平台、托管网站等）对著作权侵权行为的应对措施。根据该法案，网络服务提供商需要采取措施，移除用户上传的侵权内容，并为著作权所有者提供投诉途径。

（4）国际合作：侵犯著作权是跨境性问题，需要国际合作来解决。许多国家在国际层面积极合作，签署协议和条约，共同打击网络著作权侵权行为。

2. 国内方面

（1）《中华人民共和国著作权法》：该法律是中国著作权保护的基本法律法规，该法规定了著作权的范围、取得方式、权利保护、侵权行为等内容，是中国著作权保护的基本法律。从网络安全角度来看，它明确规定了网络上的作品享有与传统媒体作品相同的著作权保护。这意味着在网络环境下，对于未经授权的作品复制、传播和使用，著作权人可以依法维权，维护其版权合法权益。这种保护措施有助于减少网络盗版行为，同时促进网络安全的稳定发展。

（2）《信息网络传播权保护条例》：该条例主要针对网络著作权保护问题。它规定了网络服务提供者（ISP）对侵权内容的责任。网络服务提供者有义务采取合理措施防止侵权行为，及时删除侵权内容或断开链接。这种规定在一定程度上降低了侵权内容的传播和扩散，维护了网络安全的稳定。

（3）《计算机软件保护条例》：该法规主要保护计算机软件著作权。在网络环境下，计算机软件容易受到盗版和非法传播的威胁，从而影响网络安全。该法规规定了软件著作权的取得方式、权益保护和侵权行为的惩罚，为计算机软件的版权保护提供了法律依据。

（4）《中华人民共和国刑法》：刑法除了专门设立【侵犯著作权罪】，对六种具体侵犯著作权的行为进行了明确规定外，也对其他与侵犯著作权密切相关的侵权行为进行刑事处罚。包括非法获取计算机信息系统数据、非法控制计算机信息系统、提供侵入、非法控制计算机信息系统程序、工具、破坏计算机信息系统等罪名。此外，以窃取或其他非法手段获取商业秘密保护的核心资源，情节严重者会构成侵犯商业秘密罪。这些刑事处罚措施有效地震慑了侵权者，减少了网络著作权侵权行为，为网络安全提供了一定的保障。

① 第二百一十七条【侵犯著作权罪】以营利为目的，有下列侵犯著作权或者与著作权有关的权利的情形之一，违法所得数额较大或者有其他严重情节的，处三年以下有期徒刑

刑，并处或者单处罚金；违法所得数额巨大或者有其他特别严重情节的，处三年以上十年以下有期徒刑，并处罚金：（一）未经著作权人许可，复制发行、通过信息网络向公众传播其文字作品、音乐、美术、视听作品、计算机软件及法律、行政法规规定的其他作品的；（二）出版他人享有专有出版权的图书的；（三）未经录音录像制作者许可，复制发行、通过信息网络向公众传播其制作的录音录像的；（四）未经表演者许可，复制发行录有其表演的录音录像制品，或者通过信息网络向公众传播其表演的；（五）制作、出售假冒他人署名的美术作品的；（六）未经著作权人或者与著作权有关的权利人许可，故意避开或者破坏权利人为其作品、录音录像制品等采取的保护著作权或者与著作权有关的权利的技术措施的。

② 第二百八十七条之二【帮助信息网络犯罪活动罪】

明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，将被处三年以下有期徒刑或者拘役，并处或者单处罚金。

③ 第二百八十五条第三款【提供侵入、非法控制计算机信息系统程序、工具罪】

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，将依照

刑法规定处罚。

④ 第二百一十九条【侵犯商业秘密罪】

以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密的；披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。有上述侵犯商业秘密行为之一，情节严重的，处三年以下有期徒刑，并处或者单处罚金；情节特别严重的，处三年以上十年以下有期徒刑，并处罚金：

（四）事前防范措施

1. 开发数字版权管理系统（DRM）

开发和提供数字版权管理系统，用于对数字内容进行加密、授权和访问控制。通过 DRM 技术，可以限制非授权用户对受保护内容的复制、传播和使用，从而有效防范盗版行为。

2. 采用数字水印技术

采用数字水印技术对数字内容进行标记，不影响内容正常观看或使用，但能追踪侵权来源。一经发现侵权行为，可通过数字水印技术追溯侵权者，保护著作权人的权益。

3. 强化身份认证和访问控制

用户的内容发布平台或应用中，采用强化的身份认证和访问控制措施，确保只有授权用户可以访问和使用受保护的内容。这可以有效防止未授权用户的侵权行为。

4. 数据加密

数据加密是网络安全中常用的手段，可以保护敏感的版权内容不被未授权的用户访问。对于数字内容提供商和版权所有者的，加密是一种重要的保护措施。

5. 建立实时监测与安全分析

建立实时监测和安全分析系统，用于检测异常访问和下载行为。通过实时监测，可以及时发现和应对潜在的侵权行为，保护著作权人的内容免受盗版和侵权的威胁。

6. 建立维权机制

建立完善的维权机制，包括应对侵权问题的流程和策略、对员工及用户的安全教育和意识培训、建立投诉举报通道等。确保一旦发生侵权行为，能够第一时间采取合适的法律手段予以维权。

7. 定期开展安全评估

定期对内容或应用进行安全评估和漏洞扫描，发现和解决潜在的安全问题，防范潜在的侵权风险。

（五）事中应对策略

1. 监测发现

一是可以使用专门的版权检测工具，这些工具能够自动扫描互联网上的内容，识别可能侵犯著作权的作品；二是可以使用网络爬虫技术，定期抓取互联网上的内容，并与版权数据库进行对比，批量发现侵犯著作权的实物衍生品并制作侵权数据分析报告，这样可以发现未经授权使用他人作品的

网页和资源；三是可以通过威胁情报交换、新注册域名监测、威胁网站指纹特征以及搜索引擎探测等技术，建立一整套覆盖 Web 网站、App 商店、社交媒体、网盘存储、知识社区、暗网、AI 等渠道的数字风险监测系统。

2. 快速响应与处置

立即对发现的侵权行为进行快速响应和处置，分析侵权数据，制定维权重点和维权策略，及时采取措施阻止侵权行为的继续扩散，如向平台发起投诉、封锁非法链接、删除侵权内容、向侵权人发送律师函、警告函等，以减少侵权的影响。通过与覆盖全球的 VPS 提供商、域名注册商、网络提供商及各国 CERT、应用商店管理者、各社交媒体平台管理者的通力合作，对已确认的数字风险进行快速关停处置。

3. 证据收集与保全

收集有关侵权行为的证据，包括侵权内容的截图、侵权者的 IP 地址、访问记录等。同时，确保证据的完整性和安全性，以备将来维权使用。

4. 巧用调解资源

调解中心及时与侵权方联系以及及时制止侵权和预防侵权行为的再发生，代表权利人意愿与侵权方进行沟通和解或者沟通授权事项。

5. 技术溯源与定位

通过技术手段对侵权行为进行溯源与定位，追查侵权者的真实身份和所在位置，为后续的维权行动提供技术支持。

6. 合作与协调

与相关部门、权益保护组织和律师事务所等合作，形成协同合力，共同应对侵权行为。及时向相关执法部门报案，并与律师协商制定合理的维权策略。

7. 媒体宣传与舆论引导

通过媒体宣传和舆论引导，向公众传递著作权保护的重要性，唤起社会对侵权行为的谴责，增加维权事业的支持力度。

8. 制定防范措施

总结侵权行为的特征和方式，制定更加有效的防范措施，避免类似的侵权事件再次发生。

（六）事后处置方案

1. 证据组织

对涉嫌侵权的网络平台、网站、账号进行调查取证，收集相关的侵权证据，包括侵权内容的链接、发布者信息等材料，以便更顺利开展后续维权报案工作。详见表 3。

序号	材料明细
1	侵权作品的链接或截图
2	侵权者发布的内容截图或复制物证
3	侵权者发布渠道及方式
4	侵权者的身份信息（如 IP 地址、账号、身份证等）
5	交易信息（如时间、地点、方式、金额）

6	原始著作权作品及证明文件（原始备份）
7	原始作品的注册证书
8	著作权登记证书
9	著作权权属证明文件
10	司法鉴定报告（原作品与侵权作品技术比对）
11	对企业造成经济损失的证明文件
12	对企业声誉、商誉等方面的影响证明
13	如委托律师代理诉讼，需要提供法律授权委托书
14	向侵权者发出的侵权通知或警示的记录
15	如有证人目击侵权行为或可以提供有关证据的，需要提供其证言或声明

表 3 遭遇侵权事件所需准备材料清单

2. 诉讼及报案

版权持有人向侵权人所在地或者侵权行为实施地的司法机关或公安机关提起侵权诉讼或刑事报案，提供相关证据和材料，确保案件受理的及时性和准确性。

3. 调查取证

协助配合司法机关各项办案流程。例如：提交对涉嫌侵权的网络平台、网站、账号进行调查取证的相关侵权证据，参照表 3。

4. 加强防范措施

根据案件的经验教训，制定更加有效的防范措施，以避

免类似的侵权事件再次发生。^[3]

四、账号交易

（一）账号交易的概念

账号交易是一种在互联网世界中广泛存在的现象，它指的是个人或组织之间买卖或转让各种网站、应用和游戏等在线服务的账号。

游戏账号作为虚拟资产在现代网络游戏中扮演着重要角色。它不仅是玩家在游戏世界中的身份和载体，还具有一定的经济价值和交易活动。然而，虚拟资产的性质复杂，也随之带来了一些安全和法律风险。

（二）非法账号交易的常见形式

1. 黑市交易

在一些地下黑市或非法交易平台上，存在大量的游戏账号出售。这些账号往往是通过盗号、钓鱼或其他非法手段获取的，涉及个人信息泄露和身份盗用等安全问题。

2. 虚假宣传

一些不法分子通过虚假宣传手段，诱导玩家购买所谓的高级账号或优惠充值服务，但实际上这些账号可能是盗版或非法获取的，存在被封号风险。

3. 交易平台风险

一些非官方的游戏账号交易平台存在安全风险，这些平台未经授权，可能会泄露用户信息、存储交易记录等，导致用户信息被滥用或泄露。

4. 黑客攻击

有些账号交易者使用黑客手段入侵他人的游戏账号，窃取账号信息并进行非法转让或交易，给玩家造成损失。

5. 虚假退款

一些交易者通过虚假退款等手段骗取玩家账号，给玩家造成经济损失。

6. 资源代练

一些账号交易者提供代练服务，承诺帮助玩家提升游戏等级或收集资源，但可能存在窃取账号信息和财产的风险。

7. 非法交易货币

一些游戏账号交易涉及非法货币交易，这可能违反游戏平台的相关规定，并有可能导致账号被封号。

（三）法律法规及政策解读

1. 网络入侵

涉及侵入他人账号、虚拟货币钱包等虚拟资产的安全问题，可能违反《中华人民共和国网络安全法》等相关法律法规。

2. 虚假交易

（1）利用虚假手段获取他人虚拟资产，可能构成诈骗罪。

（2）《中华人民共和国著作权法》也有规定，因虚拟资产包括游戏账号中的游戏角色、装备等可能涉及著作权保护，该法律规定了著作权的取得、转让和侵权责任等规定，

保护著作权人的权益；

（3）在交易过程中可能涉及买卖合同等合同形式，《中华人民共和国民法典》规定了合同的成立、履行和违约等规定，保护买卖双方的权益。

3. 非法虚拟货币资产交易

《关于防止虚拟货币等资产用于非法活动的通知》是中国人民银行等七部委发布的文件，主要针对虚拟货币等资产的反洗钱监管，要求相关机构加强对虚拟货币等资产交易的监管，防止其被用于非法活动。

4. 青少年防沉迷管理

《关于加强网络游戏管理 防止沉迷通知》是国家新闻出版署、教育部等八部委发布的文件，主要针对未成年人沉迷网络游戏的问题，对游戏账号交易有一定影响。

（四）事前防范措施

1. 强化身份认证

采用多因素认证（MFA）技术，如短信验证码、手机令牌等，增强用户账号的身份认证过程，防止未经授权的访问。同时，加强游戏账号的身份验证措施，推广多因素认证，防止账号被盗用。鼓励用户进行实名认证，并进行合规的“了解你的客户”（Know Your Customer, KYC）过程，减少非法账号交易和欺诈行为。

2. 建立实时监测系统

建立实时监测系统，对账号交易行为进行实时监测，追

踪游戏账号和虚拟资产在各个交易平台上的交易情况，及时发现可疑交易并进行告警，如大额交易、频繁登录等。这可以通过威胁情报检测、网络爬虫、API 接口等方式实现，利用大数据分析技术，对监测平台采集的数据进行分析和挖掘；使用威胁情报数据建立模型和算法；利用人工智能和机器学习技术，建立智能风控系统，可以识别异常交易模式、异常账号转移行为等，帮助发现并拦截潜在的非法交易活动。

3. 建立安全事件响应机制

建立完善的安全事件响应机制，制定详细的安全事件响应预案，明确安全事件的分类和处理流程。预案中应包含不同级别安全事件的响应措施、责任人和联系方式等信息。一旦发现异常交易或账号被盗用等安全事件，立即采取行动进行调查。

建立自动化响应系统，对检测到的可疑交易和异常行为进行自动化处理。例如，自动封禁可疑账号、限制虚拟资产交易等。

4. 增强用户安全提示及教育

在关键操作环节，向用户发送安全提示和提醒，增加用户对交易安全的重视。同时，向用户提供有关虚拟账号交易安全的教育和培训，教育用户识别虚假交易、增强防范钓鱼攻击等安全意识。

5. 制定交易限制策略

制定合理的交易限制策略，防止账号被盗用或滥用。

6. 加强合规审核与合同约定

确保公司的交易活动符合当地相关法规，与用户签订明确的服务合同，并明示禁止非法交易。

7. 技术升级与漏洞修复

及时进行技术升级和漏洞修复，防止黑客利用安全漏洞进行攻击。

（五）事中应对策略

1. 快速冻结与恢复账号

对于可疑的账号交易，及时冻结相关账号和交易行为，以防止进一步损失。同时，对受影响的用户进行账号恢复和安全检查。

2. 数据分析与挖掘

通过数据分析和挖掘技术，发现隐藏的安全威胁和漏洞，及时采取措施进行修复。

3. 异常交易分析

对于大额、频繁、异地等异常交易进行分析，找出异常模式和行为特征，以提高检测效率和准确性。对游戏账号的登录地点进行检测，及时发现异地登录情况，防止账号被盗用或转移。

4. 技术溯源与取证

对于安全事件进行技术溯源和取证工作，确定攻击来源和手段，为后续追责和防范提供参考。

5. 用户通知与警示

对受影响的用户进行及时通知和警示，提醒其注意账号安全，避免受到更大损失。

（六）事后处置方案

1. 证据组织

对涉嫌违法犯罪的账号及相关信息进行调查取证，收集相关的犯罪证据，包括账号信息、交易信息等材料，以更顺利开展后续报案工作。详见表 4。

序号	材料明细
1	账号信息：包括账号名、ID、密码、实名制信息
2	交易信息：交易时间、地点、方式、金额
3	交易用户提供凭证：聊天记录、邮件、截图
4	支付凭证：支付凭证、交易记录
5	合同或协议（如签订）
6	账号恢复记录（如有恢复过被盗号的经历）
7	证人证词
8	律师意见及建议
9	其他证据：如交易记录、日志等。

表 4 遭遇侵权事件所需准备材料清单

2. 报案

受害人向司法机关提起诉讼或报案，提供相关证据和材料，确保案件受理的及时性和准确性。

3. 调查取证和鉴定

协助配合司法机关各项办案流程。例如：提交相关的证据材料，如有需要可能需进行技术鉴定，参照附表 4。

4. 加强防护，增强意识

（1）分析安全事件中暴露的漏洞和弱点，及时进行修复和加固，以防止类似事件再次发生。

（2）及时向全体用户通知安全事件的发生，并提供安全警示和防范措施，提高用户的安全意识。^[4]

五、违规信息内容

（一）违规信息的概念

违规信息内容是指在产品自身内容及业务相关用户生成内容（UGC）场景中出现的违法违规信息，包括：涉黄、涉赌、涉暴及与业务安全相关的诈骗广告、侮辱谩骂或其他违法违规信息等内容。

（二）常见违规信息类型

1. 侮辱谩骂

在网络环境中，用户出于某种原因，对于其他特定用户或其他特定对象进行无理谩骂，攻击，侮辱等行为，往往带有互相诋毁，甚至会对其人格、地域、性别、种族等进行攻击；也时而发生用户对于特定事件的立场不同，引发其谩骂等攻击行为。

2. 色情低俗

色情低俗信息是指在网络环境中散布淫秽、色情内容。例如：发送以色情为目的的情色文字、情色视频、情色漫画

的内容，发送低俗类色情擦边、性暗示类信息内容，以此来达到吸引用户的目的。

3. 诈骗广告

在网络环境中，不法分子会通过各类社交渠道散布诈骗广告、冒充官方客服或与用户培养感情等方式实施诈骗犯罪。与传统的诈骗罪相比，此类诈骗犯罪具有手段多样化、行为隐蔽化、成本低廉化、传播广泛化、受众年轻化等特点。

4. 违法违规信息

这类信息包括但不限于危害国家安全、泄露国家秘密、颠覆国家政权、破坏国家统一、调侃英雄烈士、宣扬邪教迷信、散布谣言、网络赌博、贩卖毒品枪支、渲染传播暴力暴恐等内容。

（三）常见的攻击方式

网络黑灰产往往通过人工和自动化工具结合的方式大规模发布同质化的违规内容。同时会针对内容变形处理以躲避网络平台审核。常见的攻击类型有以下几种：

1. 文本

色情、赌博、广告等相关类型违规文本内容，以及其同音词、象形词、干扰词变种等。

2. 图片及视频

性器官、性行为、性分泌物、赌博、违禁品、血腥、暴力伤害等违规图像内容，以及图像中出现的违规文字内容。

3. 语音

娇喘呻吟声等涉黄音频、违禁音频以及其他在文本审核中常见的违规内容。

（四）法律法规及政策解读

1. 网络信息内容生产者

根据《互联网信息服务管理办法》第十五条 互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

- （1）反对宪法所确定的基本原则的；
- （2）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- （3）损害国家荣誉和利益的；
- （4）煽动民族仇恨、民族歧视，破坏民族团结的；
- （5）破坏国家宗教政策，宣扬邪教和封建迷信的；
- （6）散布谣言，扰乱社会秩序，破坏社会稳定的；
- （7）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- （8）侮辱或者诽谤他人，侵害他人合法权益的；
- （9）含有法律、行政法规禁止的其他内容的。

根据《互联网用户账号信息管理规定》第八条规定互联网用户注册、使用账号信息，不得有下列情形：

- （1）违反《网络信息内容生态治理规定》第六条、第七条规定；
- （2）假冒、仿冒、捏造政党、党政军机关、企事业单位

位、人民团体和社会组织的名称、标识等；

（3）假冒、仿冒、捏造国家（地区）、国际组织的名称、标识等；

（4）假冒、仿冒、捏造新闻网站、报刊社、广播电视机构、通讯社等新闻媒体的名称、标识等，或者擅自使用“新闻”、“报道”等具有新闻属性的名称、标识等；

（5）假冒、仿冒、恶意关联国家行政区域、机构所在地、标志性建筑物等重要空间的地理名称、标识等；

（6）以损害公共利益或者谋取不正当利益等为目的，故意夹带二维码、网址、邮箱、联系方式等，或者使用同音、谐音、相近的文字、数字、符号和字母等；

（7）含有名不副实、夸大其词等可能使公众受骗或者产生误解的内容；

（8）含有法律、行政法规和国家有关规定禁止的其他内容。

2. 网络信息内容服务平台责任

（1）网络信息内容服务平台应当履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培育积极健康、向上向善的网络文化。

（2）网络信息内容服务平台应当建立网络信息内容生态治理机制，制定本平台网络信息内容生态治理细则，健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业

链信息处置等制度。

网络信息内容服务平台应当设立网络信息内容生态治理负责人，配备与业务范围和服务规模相适应的专业人员，加强培训考核，提升从业人员素质。

（3）网络信息内容服务平台不得传播《互联网信息服务管理办法》第十五条规定的信息。

网络信息内容服务平台应当加强信息内容的管理，发现《互联网信息服务管理办法》第十五条信息的，应当依法立即采取处置措施，保存有关记录，并向有关主管部门报告。

（五）事前防范措施

1. 建立违规信息防控标准

为提升运营方对违规信息审查的效力，可制定新业务上线违规信息检测安全技术方案并接入红线标准，包括检测能力标准、处罚能力标准、人工审核能力标准以及产品功能形态标准等。这套标准也可作为企业内部自我审查和约束的基础，确保所有新上线的业务或产品都具备统一高效的检测机制，便于企业内部的安全部门进行统一指挥和部署。

2. 实施源头风险控制

由于网络黑灰产可以在短期内低成本生成各类违规内容变种，但用户的行为习惯和设备信息往往难以在短期内发生改变。因此，运营方可建立健全风险控制机制，包括但不限于：用户行为分析、设备信息跟踪、异常行为监测等，从违规信息源头进行风险控制，以便及时发现并处理潜在违规

行为。

3. 加强用户防诈骗教育

在产品内外官网论坛等适合场景设置防诈骗公告，滚动提示用户注意防范。通过积极引导提高用户的自我安全意识和防诈意识，帮助其了解相关法律法规，避免遭受欺诈行为的伤害。同时，鼓励玩家积极抵制破坏发言环境的行为。

4. 优化突发事件舆情管理

运营方应建立完善的重大或突发事件预警响应机制。当重大事件发生时，各团队和部门需具有快速制定相关标准并高效部署最新违规信息检测能力。同时还需要合理配置人工审核资源，并设立专项数据监测以保障网络发言环境的和谐稳定。

（六）事中应对策略

1. 建立违规信息监测机制

运营方应建立健全用户注册、账号管理、信息发布实时审核、跟帖评论审核、实时巡查、应急处置和网络谣言、黑灰产业链信息处置等制度，并采用智能 AI 审核系统，依托最新的深度学习算法，实现内容，行为，画像多维度协同，高效准确识别出文本、图片、视频、音频中的违规内容，并对敏感信息、色情低俗、消极谩骂、诈骗广告等多个类型违规信息进行自动分类识别。

2. 实时阻断与处罚

一旦检测到违规信息，运营方应立即采取措施进行实时

拦截，有效阻断违规信息曝光及传播。根据设立的相关处罚标准，对发布违规信息的账号予以禁言或封号处理，避免对正常用户造成干扰，净化网络空间环境。

3. 精细化场景安全标准

鉴于当前网络产品呈现 UGC 场景繁多、信息内容形态多样的特点，应细化用户昵称、消息、好友私聊、游戏社区、搜索等场景的安全标准，精准打击游戏内各场景的违规信息，可以有效降低误判漏判风险，提升用户体验。

4. 应急响应与监测系统

运营方应建立基础的违规信息处理防护监测系统。一类是对违规信息发布传播趋势进行监测；另一类是针对已检测到并作出处罚决定的违规信息进行监测。当监测预警发生时，运营人员需确保在第一时间进行处理，并快速触发整个运营机制的正向迭代，保障业务安全运营的效果。

5. 建立违规信息举报处理机制

运营方应建立健全违规信息举报机制，为用户提供各类在泛 UGC 场景中（如文字、图片、实时语音、音频消息、自定义内容）的规范举报服务。采用人机协同高效全面覆盖举报信息处理，并在游戏内外渠道向举报者反馈处理结果，实现举报-处理-反馈的用户服务闭环。

（七）事后处置方案

1. 证据组织

对发布违规信息并对用户或运营方造成巨大影响的用

户、平台进行调查取证，收集相关的违法证据，包括用户账号信息、违规信息内容等材料，以更顺利开展后续报案工作。详见表 5。

序号	材料明细
1	违规用户账号信息（IP 属地、身份信息）
2	违规信息内容（发布时间、次数、截图/视频）
3	违规信息内容分析
4	用户异常数据分析
5	正常用户提供与提供违规信息方的聊天记录
6	如有交易，提供交易信息（截图、金额、时间）
7	对用户/企业造成经济损失的证明文件
8	对用户造成声誉，其他方面的影响证明
9	对企业声誉、商誉等方面的影响证明

表 5 遭遇违规信息内容问题所需材料清单

2. 报案

受害方向司法机关提起诉讼或报案，提供相关证据和材料，确保案件受理的及时性和准确性。

3. 调查取证和鉴定

协助配合司法机关各项办案流程。例如：对涉嫌诈骗等犯罪行为进行调查取证，提交相关证据材料，参照附表 5。

4. 完善机制，增强防范

（1）建立违规信息追溯能力

由于自动化审核技术与审核人员对于新出现的违规信息与变种内容在认定标准与技术迭代上存在一定的滞后性，违规信息的完全实时筛查难度巨大，故建立针对存量信息的回溯追查能力是必要的。在运营过程中，历史存量信息一经发现恶意内容，应及时清除违规，消除影响，并更新检测标准，迭代自动化审核技术，同时对审核人员加强培训，对剩余存量信息进行统一回溯清理。

（2）增强人工巡查机制

针对产品内 UGC 场景，游戏外官网论坛，社区评论等，安全管理员应开展定期巡查，发现恶意违规信息及时处置，并实时反馈给运营团队，完善整体审核机制的正向反馈。^[5]

六、游戏欺诈

（一）游戏欺诈的概念

游戏欺诈指一系列黑灰产通过自动化脚本批量薅取游戏资源，损害玩家体验和平台收益的行为。

（二）游戏欺诈的高危场景

1. 批量注册

在一些特定的游戏模式下，会滋生大量小号，包括真实的玩家小号和黑灰产小号。目的不同，用途不同，但最终都会对用户体验、游戏生态、平台利益造成一定的负面影响。在某宝、某鱼等交易平台上，充斥着大量的游戏账号、点券等交易信息。这背后是黑灰产为了窃取更多游戏资产，使用自动化注册脚本创建并培育大量游戏账号，再利用云手机、

软件多开、离线托管、公会许愿等手段自动完成资源升级，从而最终变现。

2. 账号登录忘记密码

在互联网生态中，75% 以上的用户都习惯在多个平台或网站中使用同一套账号密码进行登录。这种方式本身就存在极大风险，黑产可以通过社工库进行批量撞库的攻击；一旦成功，将会造成用户信息泄露甚至财产损失，给企业造成严重的负面影响。其中，“撞库”指黑产通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登录其他网站，得到一系列相应的可登录账号，从而高效获取有价值的游戏账号，并在交易平台上实施账号倒卖、虚拟财产转移等恶意操作，实现账号变现，谋取巨额不正当利益的行为。

3. 游戏预约

新游上线阶段，游戏厂商通常会在各大渠道和游戏中推出限时预约活动，在给玩家送来福利的同时，也引来了虚假邀请、刷积分、刷红包的羊毛党黑产，与真人玩家抢夺游戏资源。

黑产往往都是团体作战且分工明确，上游专门人员进行新游预约活动挖掘，利用社群等方式传播；中游通过一些自动化机器脚本在预约活动中薅取羊毛；下游则寻找平台漏洞进行快速变现。

4. 礼包领取

在游戏礼包领取、活动奖励领取场景，薅羊毛现象严重，

易被黑产通过批量注册小号、登录、签到做任务等方式薅走大量虚拟礼包和平台奖励。游戏欺诈往往通过生产大量账号积累游戏资源，再通过掠夺玩法进行定向转移，用低于官方商城的售价再交易给其他玩家，而谋取线下利益。

5. 恶意短信消耗

目前，大多游戏公司的短信接口缺乏安全工具保护，容易遭到机器脚本规模性的盗刷，造成短信费用损失。黑产通常会针对某一新模块上线或未设防护的网站，不断变换各接口参数，例如：手机号、IP（采用高匿代理）等去请求后台发送短信验证码，进行恶意刷短信。

恶意短信消耗一般不以直接获取利益为目的，而是以恶意刷取目标网站短信接口，消耗短信成本；或是获取价值用户信息，进行广告定向投放的形式对用户造成干扰，进而影响企业品牌形象，造成企业价值用户的流失。此外，大量访问请求使短信验证码发送，短信发送量急剧增长，游戏运营方也难以区分真实用户和黑产，不能够直接关闭接口，这往往会造成大量资源浪费与经济损失。

（三）法律法规及政策解读

1. 游戏欺诈直接攻击者

根据《中华人民共和国刑法》第二百六十七条，诈骗公私财物，数额较大或者有其他严重情节的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他特别严重情节的，处三年以上十年以下有期徒刑，并处

罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

2. 关键信息基础设施的运营者

（1）根据《中华人民共和国网络安全法》第十八条，关键信息基础设施的运营者应当履行网络安全保护义务，防止网络安全事件发生，保障网络安全。

（2）根据《中华人民共和国网络安全法》第三十一条，关键信息基础设施的运营者应当在网络安全事件发生后，立即启动应急预案，采取处置措施。

（3）根据《中华人民共和国网络安全法》第四十二条，关键信息基础设施的运营者应当建立网络安全监测、预警、通报和应急处置制度。

3. 个人信息处理者

（1）根据《中华人民共和国数据安全法》第三条，数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

（2）根据《中华人民共和国数据安全法》第四条，国家建立数据分类分级保护制度，对数据进行分类分级保护。

（3）根据《中华人民共和国数据安全法》第二十七条，国家保护个人信息和重要数据。个人信息处理者应当采取技术措施和其他必要措施，确保个人信息和重要数据的安全。

（4）根据《中华人民共和国个人信息保护法》第七条，个人信息处理者应当采取措施确保个人信息和重要数据的

安全。

（5）根据《中华人民共和国个人信息保护法》第十条，个人信息的处理应当遵循合法、正当、必要的原则，不得过度收集、使用个人信息。

（6）根据《中华人民共和国个人信息保护法》第十七条，个人信息处理者应当按照国家规定，建立健全个人信息安全管理制度，对个人信息进行分类管理。

4. 国际法律

（1）个人隐私泄露风险：根据欧盟《通用数据保护条例》（GDPR）第四条，个人数据泄露是指“由于违反安全政策而导致传输、储存、处理中的个人数据被意外或非法损毁、丢失、更改或未经同意而被公开或访问”。所以即使是黑灰产使用已经泄露的数据来进行撞库攻击，企业自身的安全防护工作没有能够避免未经授权的访问，也是违规的一种。

（2）信用评级风险：2019 年，信用评级公司穆迪（Moody's）对网络安全的业务影响进行了新的调整，将网络风险纳入其信用评级。穆迪根据企业违规而造成的业务影响将上市企业的评级从稳定降至负面。信用评级广泛影响到投资者在选择投资对象时所考虑的风险评估以及投资决定。

（3）虚假账号虚假流量风险：根据欧盟《数字服务法案》（DSA）将对从事数字中介服务的供应商进行监管，涉及：纯接入服务、缓存服务、托管服务、在线平台服务和在线引擎服务，特别是在欧盟境内拥有月均 4500 万活跃用户/接收

方的超大型网络平台（VLOPs）和超大型网络搜索引擎（VLOSEs）。DSA 将于 2024 年 2 月 7 日起适用，但对在线平台和在线搜索引擎的供应商，DSA 的一些专门规则将提前适用。违反 DSA 的行为，可能导致最高可达该主体前一财政年度全球营业额 6% 的罚款。

（四）事前防范措施

1. 开展系统风险评估

结合平台规则或游戏玩法设置，提前对可能存在的黑产欺诈行为进行风险评估，制定相应的解决方案，从规则设置层面降低游戏欺诈风险。同时，做好准备工作以更好应对上线可能遭遇的情况。

2. 进行安全工具建设

在账号注册、登录、找回密码、获取短信验证码等高危欺诈场景提前部署相关安全工具，加强人机防控策略，将“机器”的访问请求和“真实的人”的访问请求区别出来，及时识别并拦截“机器流量”。从技术手段来说，常见的有使用图形验证码，封禁高频率请求的 IP/会话、部署人机识别的 SDK 组件等等。

3. 进行存量用户风险评估

利用设备指纹的追踪定位技术，获取存量用户的风控判别结果。对用户的环境信息、行为数据、设备指纹进行多重分析验证，识别并处置黑产的可疑行为，加强业务风控能力。

4. 加强数据监测维度和频率

结合业务情况，加强数据监测维度和频率，以帮助运营方提升对黑产行为判断的精准度，更高效地处理可疑账号、可疑交易、可疑流水等相关问题。也能帮助运营方及时调整奖励、游戏玩法及设置，对可疑风险做更多维度的追踪，及时发现问题，做出响应。

5. 开展攻防演练

尝试从黑灰产视角出发对各业务场景进行攻防演练，结合演练结果和调研分析对黑灰产可能欺诈的风险点建设关联指标，并进行实时和离线监测，力求风险前置。

（五）事中应对策略

1. 异常发现

（1）设备环境校验：主要包含设备真实性校验和参数合法性校验，识别伪造设备参数的接口或者模拟器刷量请求。

（2）设备画像分析：对新进入的流量进行深入的设备维度风险分析，为每个设备生成唯一的设备标识，通过分析设备特征、运行环境、弱特征归因算法，我们可以对这些数据进行综合评估，识别潜在的风险和威胁。

（3）账号画像分析：对新进入的流量进行一系列账号维度的风险分析，以便更准确地识别出该账号历史行为潜在风险，并为每个流量输出相应的风险标签，为平台的安全策略提供支持。

（4）关联拓扑分析：将设备指纹、账号、ip、访问次数、风险标签等多维度指标进行关联分析，形成关联拓扑图，

扩展数据挖掘的深度及安全分析广度，及时发现黑账号、黑设备、黑 IP 的关联关系，对其进行打击。

2. 数据特征分析

（1）风险数据过滤：利用历史数据和第三方数据进行建模分析，以识别风险 IP、风险手机号和风险 openid 等信息，及时发现黑产请求，防止恶意攻击和欺诈活动。

（2）业务数据趋势：根据流量数据的常规数据表现、增长率去判定有无异常情况，可能包括增长率和比较历史数据。例如，如果某项业务数据增长速度与过去同期相比增长迅猛，这可能就是异常情况，根据数据趋势，可能需要执行一些规则，例如告警、发送电子邮件提醒或自动触发响应的处理方式。

3. 及时响应处理

（1）弹出验证码：通过应用计算机程序和人类行为轨迹特征，可以创建有效的人机分类模型，以识别并阻止黑产发起的恶意请求。同时，为了防止黑产绕过前端验证措施，也从以下几个方面考虑优化验证码的安全能力：从 js 混淆、蜜罐参数、验证形式等多种维度进行动态更新，提高黑产破解成本。

针对图片穷举破解和图片模型破解等黑产手段，建议保持每小时更新一批验证元素的频率并对图片、元素做视觉干扰处理，避免答案自动识别，业务安全防线被突破。

（2）本机号码认证：通过利用运营商网关流量校验技

术，确保其与当前业务体系所涉及的手机号码一致。这一策略旨在检测可能存在的身份伪造行为，并为实际用户提供一个安全、可靠的网络环境。

（3）其他验证：当发现异常行为时也可以通过触发短信或人脸识别验证，帮助被欺诈方对可能的非法行为进行识别，并保护我们的系统和数据免受潜在威胁。

（4）封禁处理：对明确为黑产行为的流量进行封禁处理，例如：封禁 IP，限制非法用户的权限、冻结其账户或将其从业务体系中剔除。

（5）自定义业务规则：制定一些自定义业务规则来适应不同的情况。这些规则可能涉及业务本身的操作流程、逻辑判断以及设备类型的切换等问题，针对这些问题做出对应通过、封禁、验证的处理。

（6）后续业务冻结：为了避免非法人员绕过身份验证机制进入业务体系，我们可以利用第三方工具为每个参与者添加标签，并通过跟踪这些标签对其行为进行限制。

4. 证据留存

对于已经识别出的黑灰产行为，我们应立即采取措施，确保数据得以保留。这包括记录恶意 IP 地址、已被非法控制的账户以及使用过的非法设备等关键信息。通过这种方式，我们可以在后续的数据分析过程中，深入挖掘出相关信息，从而为打击黑灰产提供有力的数据支持，为后续追责提供有力证据。

（六）事后处置方案

1. 证据组织

对涉嫌违法犯罪的账号及相关信息进行调查取证，收集相关的犯罪证据，包括软件信息、服务器信息等材料，以更顺利开展后续报案工作。详见表 6。

序号	材料明细
1	被欺诈对象信息及简介
2	被欺诈业务黑产盈利点说明
3	被欺诈业务链接及业务截图
4	欺诈方名称及相关信息
5	欺诈方控制账号信息及数量
6	造成业务损失金额的证明材料
7	欺诈方软件信息
8	欺诈方服务器信息
9	律师意见及建议

表 6 遭遇游戏欺诈所需准备材料清单

2. 报案

被欺诈者向司法机关提起诉讼或报案，提供相关证据和材料，确保案件受理的及时性和准确性。

3. 调查取证和鉴定

协助配合司法机关各项办案流程。对涉嫌欺诈团伙的设备、身份、行为特征进行调查取证，提交相关欺诈证据材料，

参照表 6。

4. 整改漏洞，加强防护

（1）根据本次事件分析沉淀，针对被利用的技术漏洞进行修复和加固，总结经验教训，以避免类似的欺诈事件再次发生。

（2）针对不同的欺诈方式制定更加有效的防范措施，持续加强业务风控的技术和手段。^[6]

七、游戏私服

（一）游戏私服的概念

游戏私服是指未经游戏开发商或版权方授权而私自搭建的游戏服务器。这些私服通常通过逆向工程、破解或盗用正版游戏的源代码或资源，提供与官方服务器类似或修改后的游戏体验。玩家在这些服务器上进行游戏时，使用的并非官方发行的客户端或服务器端程序，导致可能出现侵犯著作权、数据安全和经济纠纷等问题。

（二）游戏私服的常见表现形式

1. “盗版”私服

主要表现为复制正版游戏的内容，行为人未经权利人的授权非法获取游戏“源代码”后设立网络服务器，之后向玩家提供和“官服”类似的游戏注册、充值等服务从而实现营利。

2. “改版”私服

在上述复制正版游戏的基础上，对游戏内容进行非法修

改，如调整游戏规则、开放未正式发布的内容或增强装备属性等，以吸引特定玩家群体。

3. “高仿”私服

该类私服通过逆向工程和代码分析，自行编写代码进而开发游戏程序。但是行为人在其开发的游戏程序中大量使用与权利人游戏画面、内容、地图、玩法等相似或相同的元素，试图在功能和体验上尽可能模仿官方服务器，甚至模仿正版游戏的更新节奏和内容，以欺骗玩家。

（三）法律法规及政策解读

1. 游戏私服制售方

制售私服的行为通常包括未经授权复制、修改、运行游戏服务器，并向玩家提供这些非法服务器的访问权限。此外，制售私服可能还包括通过私服出售虚拟物品、装备、货币等行为。

（1）侵犯著作权

《中华人民共和国刑法》第二百一十七条，未经著作权人许可，复制发行其作品，构成侵犯著作权罪。情节严重的，可以判处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，可以判处三年以上七年以下有期徒刑，并处罚金。

《中华人民共和国著作权法》第四十八条，未经著作权人许可，复制、发行、表演、放映、广播、汇编、传播其作品，属于侵犯著作权的行为。侵权人可以被要求停止侵权行

为，消除影响，公开赔礼道歉，并赔偿损失。如果侵权行为严重，赔偿金额可以按照实际损失或非法所得的数额来计算，并可能处以罚款。

2. 游戏私服传播方

（1）侵犯信息网络传播权

《信息网络传播权保护条例》第三条，信息网络传播权是指通过信息网络向公众提供作品的权利。私服通过互联网向玩家提供未经授权的游戏内容，侵犯了著作权人的信息网络传播权。

《信息网络传播权保护条例》第十八条，版权人可以要求侵权者停止侵权行为，删除侵权内容，并赔偿损失。严重的侵权行为可能导致侵权人被起诉，并处以赔偿和法律责任。

（2）危害网络安全

根据《中华人民共和国网络安全法》第二十七条，任何个人和组织不得从事危害网络安全的活动。私服的搭建和运营可能会被视为危害网络安全的活动，特别是如果私服涉及非法窃取或利用他人的网络资源。

根据《中华人民共和国网络安全法》第六十三条，违反本法第二十七条规定的个人和组织，可以被责令改正，并处以罚款。情节严重的，还可能被责令停业整顿、关闭网站、吊销相关许可证等行政处罚。如果涉及犯罪行为，还可以依法追究刑事责任。

（四）事前防范措施

1. 客户端安全保护

加强游戏客户端和服务端的安全防护，防止逆向工程和非法入侵。定期更新游戏的加密和认证机制，提高私服搭建的技术难度。

2. 版权收集及留存

游戏版权方应确认好自有版权，将文件数据做好水印，对于历史服务器版本和数据做好留存记录。

3. 建立实时监控系统

建立实时监控系统，对潜在的私服活动进行 7*24 小时监控。一旦发现可疑活动，立即启动快速响应机制，组织技术团队全面侦查。

4. 企业内部人员的风险防控

（1）对其游戏软、硬件等核心商业秘密采取保密措施，限制接触人员，防止单个员工掌握全部游戏代码；

（2）在游戏源代码中埋伏特殊、错误或无效的代码或标记，以便举证；

（3）与接触源代码、游戏核心设计的员工签订严格的保密协议，并根据情况增减保密内容；

（4）对于游戏核心人员应签订完善的竞业禁止协议，约定不超过两年的合理竞业禁止期限，避免核心员工加入其他竞争游戏公司而造成对本公司游戏产品的重大冲击和破坏。

5. 数据收集与分析

利用网络爬虫技术，搜集互联网上与游戏私服相关的论坛、社交媒体、聊天室等平台的数据。通过 API 收集游戏内部的日志数据，包括异常登录、交易行为等，实时掌握私服相关动态信息，提高风险意识，便于提前安全部署。

6. 用户教育与社区管理

教育用户识别私服风险，鼓励其通过官方渠道举报可疑的私服活动。加强对游戏社区的管理，对违规言论和行为进行监控和处罚。

（五）事中应对策略

1. 加强安全防护

通常私服是通过盗取游戏源代码或利用游戏漏洞搭建的，因此技术团队应尽快查明原因进行漏洞修补。同时，增强游戏的防作弊系统和加密技术，防止数据泄露或被破解。

2. 取证与证据保全

对收集分析到的证据进行取证、固定和留存，包括但不限于私服玩家注册信息、交易记录、游戏数据、运营情况等。

3. 发布公告并引导用户

通过游戏官网网站、游戏内公告、社交媒体进一步发布相关声明，提醒用户注意私服的安全风险并明确私服是非法的，正确引导用户使用官方渠道。

4. 舆情监控与公关应对

实时监控网络舆情，密切关注公众意见与情绪变化。若私服事件引发负面舆论，及时公关应对，避免事件升级。同

时，可以联动媒体发布报道或专访，塑造企业正面形象。

（六）事后处置方案

1. 证据组织

对涉嫌私服的网络平台、售卖主体进行调查取证，收集相关的违法证据，包括私服服务器信息、私服运营情况等材料，以更顺利开展后续报案工作。详见表 7。

序号	材料明细
1	私服访问方式及信息（网址、域名、客户端下载链接）
2	私服服务器情况（服务器位置、托管信息）
3	私服用户数据（用户名、IP 地址、游玩记录）
4	被抄袭的原服务器版本文件
5	知识产权证明（商标、专利、著作权）
6	私服售卖方信息（账号、联系方式）
7	交易信息（如截图、时间、方式、金额）
8	用户举报记录
9	对企业造成经济损失的证明文件
10	对企业声誉、商誉等方面的影响证明
11	第三方技术鉴定报告

表 7 遭遇私服问题所需材料清单

2. 阿里云游戏私服处理方案

若发现该私服服务器为阿里云产品，可在阿里云举报中心（<https://report.aliyun.com/>）发起知识产权侵权举

报，需提供材料如下：

（1）权利人/投诉人主体信息和相关证明材料

① 个人投诉：权利人/投诉人的真实姓名、联系电话及邮箱、身份证或护照（外国公民）的照片或扫描件等。

② 企业投诉：权利人/投诉人的企业名称、联系人、联系电话及邮箱、营业执照等。

③ 代他人投诉：除上述要求的投诉人和权利人双方的主体身份信息和证明材料外，还需提供权利人签名或盖章的授权委托书的照片或扫描件。

（2）投诉内容

① 被举报内容侵犯的权利类型（如：商标权、著作权、专利权等）；

② 阿里云为被举报对象提供的产品或服务内容（如：域名注册服务、服务器租赁服务等）；

③ 被举报侵权的内容所在的网络地址、域名、IP 地址、APP 或其他能够准确定位到侵权内容的信息。

（3）构成侵权的初步证明材料

① 商标权权属证明材料：商标注册证等。

② 著作权权属证明材料：包括但不限于著作权版权登记证、软件著作权登记证、出版物征订发行委托书、著作权授权合同、经权威机构签发的作品创作时间戳、公映许可证等。

③ 专利权权属证明材料：包括但不限于专利证书、专

利登记簿等。

④ 被举报内容构成侵权的证明材料：请告知您认为被举报网站构成侵权的事实及详细理由，包括但不限于被举报方的侵权内容截图（包括但不限于权利人与被举报方双方内容的对比，并明确具体的侵权范围）等。

（4）权利人/投诉人的保证声明

您保证您的投诉材料的真实性、准确性及完整性，并保证承担和赔偿如因投诉材料不真实、不准确、不完整或因阿里云根据您的投诉而采取相关措施给被举报方、阿里云和/或其他主体造成的任何损失（包括但不限于阿里云因向被举报方或其他主体赔偿而产生的损失及阿里云名誉、商誉损害等）。

3. 侵权投诉或法律行动

受害方若发现私服使用阿里云产品可进行侵权投诉。也可以通过法律途径追究其责任，向司法机关提起法律诉讼或刑事追责，提供相关证据和材料，确保案件受理的及时性和准确性。

4. 调查取证和鉴定

协助配合司法机关各项办案流程。例如：对涉嫌搭建私服、传播私服者的设备、身份、行为特征进行调查取证，提交相关证据材料，参照表 7。

5. 定期更新，加强防护

（1）定期发布安全补丁，及时修复漏洞，避免被不法

分子利用进行私服搭建。

（2）加强对代码、数据和服务器的安全保护，定期审查及测试，尽可能避免类似问题再发生。

（3）严格管控第三方售卖平台。游戏运营方可与各大平台进行协同合作，在法律范围内要求下架相关私服售卖渠道。^[7]

八、网络暴力

（一）网络暴力相关概念

网络暴力，也被称为“网络欺凌”或“网络攻击”，是指个体或群体通过互联网平台对他人进行的恶意言语攻击、骚扰、羞辱、谩骂、诽谤、造谣、曝光隐私或其他方式的有害行为。在《关于依法惩治网络暴力违法犯罪的指导意见》中，将网络暴力行为界定为“在信息网络上针对个人肆意发布谩骂侮辱、造谣诽谤等信息，贬损他人人格，损害他人名誉，扰乱网络秩序，造成他人社会性死亡，甚至精神失常、自杀等严重后果的行为”。

根据《网络暴力信息治理规定》第三十二条，明确定义网络暴力信息是指通过网络以文本、图像、音频、视频等形式对个人集中发布的，含有侮辱谩骂、造谣诽谤、煽动仇恨、威逼胁迫、侵犯隐私，以及影响身心健康的指责嘲讽、贬低歧视等内容的违法和不良信息。

（二）网络暴力的类型

1. 语言攻击

(1) 侮辱与谩骂：在社交媒体、论坛、评论区等公开场合，对某人进行恶意的侮辱、谩骂或嘲讽，使用粗俗、下流或极具攻击性的语言，意图贬低或羞辱对方。

(2) 恶意评论：在他人的发布内容下恶意评论，包含不实指控、贬低人格的言论，甚至可能涉及种族、性别、宗教歧视等。

2. 网络围攻

(1) 集体攻击：一群人组织或自发地在网络平台上集中对某个个体或群体进行攻击，使受害者陷入舆论漩涡，感受到巨大的心理压力。

(2) 网络水军：雇佣大量虚假账户或机器人对某人进行集体攻击，发布恶意评论或虚假信息，制造虚假的网络舆论。

3. 人肉搜索

(1) 隐私泄露：通过非法手段获取他人的个人信息，如家庭住址、联系方式、身份证号码等，并在网络上公开，导致受害者隐私严重受损。

(2) 网络暴力升级：将获取的隐私信息散播给更广泛的受众，引发更多人参与攻击或骚扰，甚至导致线下骚扰或威胁。

4. 网络骚扰

(1) 重复骚扰：持续不断地通过私信、邮件、留言等方式发送威胁性、性骚扰或不受欢迎的消息，意图干扰或恐

吓受害者。

(2) 社交媒体侵扰：通过假冒账户、盗用个人资料或照片在社交媒体上冒充受害者发布不当内容，或用其他方式侵扰其社交生活。

5. 网络诽谤

(1) 虚假信息传播：通过捏造或夸大事实，发布虚假的信息来攻击某人的声誉，可能会引发公众的误解或不实的舆论。

(2) 恶意抹黑：有组织地散布虚假的、贬低性的信息或舆论，损害某人或企业的社会形象或商业信誉。

(三) 法律法规及政策解读

1. 《中华人民共和国刑法》

第二百四十六条：以暴力或者其他方法公然侮辱他人或者捏造事实诽谤他人，情节严重的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利。

2. 《中华人民共和国治安管理处罚法》

第四十二条：有下列行为之一的，处五日以下拘留或者五百元以下罚款；情节较重的，处五日以上十日以下拘留，可以并处五百元以下罚款：

(1) 写恐吓信或者以其他方法威胁他人人身安全的；

(2) 公然侮辱他人或者捏造事实诽谤他人的；

(3) 捏造事实诬告陷害他人，企图使他人受到刑事追究或者受到治安管理处罚的；

(4) 对证人及其近亲属进行威胁、侮辱、殴打或者打击报复的；

(5) 多次发送淫秽、侮辱、恐吓或者其他信息，干扰他人正常生活的。

3. 《中华人民共和国民法典》

第一千一百九十四条：网络用户、网络服务提供者利用网络侵害他人民事权益的，应当承担侵权责任。法律另有规定的，依照其规定。

第一千一百九十五条：网络用户利用网络服务实施侵权行为的，权利人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。通知应当包括构成侵权的初步证据及权利人的真实身份信息。

第一千一百九十七条：网络服务提供者知道或者应当知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。

4. 《中华人民共和国网络安全法》

第十二条：国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社

会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

5. 《网络暴力信息治理规定》

第三十条：违反本规定的，依照《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国治安管理处罚法》、《互联网信息服务管理办法》等法律、行政法规的规定予以处罚。

法律、行政法规没有规定的，由网信、公安、文化和旅游、广播电视等有关部门依据职责给予警告、通报批评，责令限期改正，可以并处一万元以上十万元以下罚款；涉及危害公民生命健康安全且有严重后果的，并处十万元以上二十万元以下罚款。

对组织、煽动制作、复制、发布、传播网络暴力信息或者利用网络暴力事件实施恶意营销炒作等行为的组织和个人，应当依法从重处罚。

第三十一条：违反本规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

（四）事前防范措施

1. 建立网络暴力行为数据库

利用网络爬虫和 API 调取历史数据，包括社交媒体、论坛、评论区等可能存在网络暴力的场所。收集用户报告和历史案例。同时，在国家网信部门和国务院有关部门指导下细化网络暴力信息分类标准规则，建立健全网络暴力信息特征库和典型案例样本库。

2. 建立实时监控系统

建立实时监控系统，对社交平台、公共论坛和评论区等进行文本监控扫描，识别敏感词汇和侮辱性语言。利用自然语言处理技术进行语义分析，区分正常对话和攻击性语言。分析用户行为模式，识别攻击行为是否是有组织的集体行动。利用机器学习模型对实时数据流进行分析，以快速识别潜在的网络暴力。

3. 建立实时预警系统

建立实时预警系统，综合事件类别、针对主体、参与人数、信息内容、发布频次、环节场景、举报投诉等因素，及时发现预警网络暴力信息风险。一旦监测发现存在网络暴力信息风险的，应当及时回应社会关切，引导用户文明互动、理性表达，并对异常账号及时采取真实身份信息动态核验、弹窗提示、违规警示、限制流量等措施；发现相关信息内容浏览、搜索、评论、举报量显著增长等情形的，还应当及时向有关部门报告。

4. 部署平台防护

在平台层面实施技术防护措施，如敏感词过滤、自动内容审核等。开发智能内容审核系统，结合人工审核，加强对网络暴力信息的识别监测和处理效率。

5. 制定网络舆情预案

企业制定详细的网络舆情应对预案，包括但不限于：舆情监控、应急响应、内部沟通与外部危机公关等内容。定期进行舆情风险评估，确定潜在威胁，尤其是敏感时期应加大监控力度。

6. 加强社区及用户管理

制定明确的社区准则和行为规范，对违规行为进行处罚。教育用户识别和抵制网络暴力，鼓励用户积极举报不当行为。

建立健全用户账号信用管理体系，将涉网络暴力信息违法违规情形记入用户信用记录，依法依规降低账号信用等级或列入黑名单，并据以限制账号功能或停止提供相关服务。

7. 加强用户教育

提醒用户应注意以下几点，树立好网络安全意识：

（1）不在社交媒体上公开过多个人信息，如家庭住址、工作单位、联系方式等。

（2）定期检查和更新隐私设置，确保个人信息不被轻易泄露。

（3）在发布内容时，仔细斟酌所分享的信息是否可能引发争议或被恶意利用。

（4）对于涉及他人的内容，在发布前要获得他人的同意，以免引起不必要的麻烦。

8. 法律与政策支持

熟悉与网络暴力相关的法律法规，如《中华人民共和国网络安全法》《中华人民共和国民法典》等。确保平台政策符合相关法律法规，为受害者提供法律支持。宣传网络暴力的法律后果，提高公众对网络暴力严重性的认识。

9. 合作与信息共享

与其他社交平台、网络安全机构和行业协会合作，共享网络暴力的情报和最佳实践。参与或建立网络暴力防范的组织，共同应对网络暴力问题。

10. 用户保护机制

提供用户保护工具，如匿名举报、屏蔽和过滤功能，帮助用户避免不必要的网络暴力。另外，提前建立心理支持和咨询服务，帮助受害者应对网络暴力带来的影响。

（五）事中应对策略

1. 内容审核与干预

加强内容审核机制，对含有攻击性语言的内容进行及时干预。对于审核确认的网络暴力内容，立即采取删除、屏蔽、关闭评论、警告、停止提供相关服务等处置措施。

2. 证据留存与法律行动

发现涉网络暴力违法信息的，或者在其服务的醒目位置、易引起用户关注的重点环节发现涉网络暴力不良信息的，应

当立即停止传输，采取删除、屏蔽、断开链接等处置措施，保存有关记录，向有关部门报告。发现涉嫌违法犯罪的，应当及时向公安机关报案，并提供相关线索，依法配合开展侦查、调查和处置等工作。

3. 用户支持与保护

建立健全网络暴力信息防护功能，提供便利用户设置屏蔽陌生用户或者特定用户、本人发布信息可见范围、禁止转载或者评论本人发布信息等网络暴力信息防护选项。完善私信规则，提供便利用户设置仅接收好友私信或者拒绝接收所有私信等网络暴力信息防护选项，鼓励提供智能屏蔽私信或者自定义私信屏蔽词等功能。

应当及时保存信息内容、浏览评论转发数量等数据。企业应向用户提供网络暴力信息快捷取证等功能，依法依规为用户维权提供便利。

4. 危机公关与公众沟通

通过公关和危机沟通策略，向公众传达网络暴力事件的处理进展和结果。通过透明和及时地沟通，减少误解和谣言的传播。

（六）事后处置方案

1. 证据组织

立即收集和保全与网络暴力事件相关的所有证据，包括截图、视频、聊天记录、用户资料等，以更顺利开展后续报案工作。详见表 8。

序号	材料明细
1	涉网络暴力内容信息（截图、视频、聊天记录）
2	与事件相关的链接和网页内容
3	发布网络暴力信息的用户信息
4	对受害方造成经济/精神损失的证明材料
5	对受害方造成经济/精神损失的因果证明文件
6	对企业声誉、商誉等方面的影响证明
7	报案书面情况说明（事件经过、暴力内容、造成伤害）
8	其他证人证言

表 8 遭遇网络暴力问题所需材料清单

2. 报案

受害方向司法机关提起诉讼或报案，提供相关证据和材料，确保案件受理的及时性和准确性，并根据公安机关要求提供其他相关证据材料。

3. 调查取证和鉴定

协助配合司法机关各项办案流程。例如：对发布网络暴力信息的用户及内容进行调查取证，提交相关证据材料，参照附表 8。

4. 平台责任履行

要求涉及的网络平台履行责任，对违法内容进行删除，对违规账号进行封禁。与平台合作，加强对网络暴力行为的监控和预防。

5. 受害者保护

为受害者提供必要的心理辅导和情感支持，帮助他们恢复心理健康。如果需要，为受害者提供法律援助，包括但不限于起诉、索赔等。

6. 技术防护措施加强

加强技术防护措施，如改进内容过滤系统，提高自动检测网络暴力的准确性。更新安全策略，提高对网络暴力行为的响应速度和处理效率。^[8]

特别鸣谢

- [1] 第一章《DDoS 攻击》核心内容由阿里云计算有限公司、腾讯安全提供。
- [2] 第二章《游戏外挂》核心内容由网易易盾、腾讯游戏安全提供。
- [3] 第三章《侵犯著作权》核心内容由天际友盟、百事通法务提供。
- [4] 第四章《账号交易》核心内容由天际友盟提供。
- [5] 第五章《违规信息内容》核心内容由腾讯游戏安全、网易易盾提供。
- [6] 第六章《游戏欺诈》核心内容由极验 GEETEST 提供。
- [7] 第七章《游戏私服》核心内容由百事通法务、天际友盟、阿里云计算有限公司提供。
- [8] 第八章《网络暴力》核心内容由网易易盾、天际友盟、百事通法务提供。
- [9] 上海政法学院刑事司法学院参与本指南的修改与完善。