2020

网络黑灰产犯罪研究报告

发布单位：百度时代网络技术(北京)有限公司
顾问单位：公安部第三研究所网络安全法律研究中心

前言

2020 年初，一场突如其来的疫情打破了大家和谐平静的生活，全国人民都经历了一场没有硝烟的战斗，网络随之成为人们获取信息和沟通的主要方式。时至今日，全民战疫仍是 2020 年最为突出的“关键词”。百度借助自身人工智能技术、大数据、搜索、信息服务方面的优势，积极支援一线的防疫控疫工作，帮助前线抗疫工作者提升效率、保障安全，为政府和研究机构提供科学的数据参考并陆续推出百度地图大数据、AI 测温、口罩人脸识别、AI 健康医生等众多应用，助力全国人民的抗疫之战。

疫情在进一步刺激互联网经济的同时，也对网络黑灰产犯罪产生了重要影响。疫情期间，大量企业和组织安排员工在家远程工作，网络安全因此受到了极大的威胁。黑灰产针对医疗、在线教育及在线办公、游戏三大行业的 DDoS 攻击和 Web 应用攻击均在 2020 年一季度呈现出高发态势。同时，网络内容生态的健康也受到黑灰产的严重侵害。仅在疫情形式严峻的季度，百度就清理与疫情相关的有害信息 20.7 万余条，重点处理了涉及散播恐慌性信息和失实谣言的有害信息、高价兜售医用防护用品的信息、宣传及贩卖野味的有害信息、假借售卖口罩之名实施诈骗等方面的有害信息。

当下，利用互联网新技术产生的新型网络犯罪形式层出不穷，网络黑灰产也呈现出了黑灰色产业链的发展趋势。黑灰产利用互联网平台实施网络犯罪，不仅扰乱市场正常经营秩序，威胁关键信息基础设施稳定运行，更加危害到用户的个人信息安全，影响互联网行业的健康发展。

《报告》以互联网企业常见的黑灰产类型为核心，深度揭示其现状、黑灰色产业链，并对其发展趋势进行分析，力求客观的呈现近年来互联网企业所遭遇的黑灰产行为，提出针对性的防治建议。

目录

一、网络黑灰产发展趋势

网络黑灰色产业，是指借助互联网技术和网络平台，进行有组织、有目的、有分工且规模化的网络违法犯罪。通常来讲，网络黑灰色产业链可分为上中下游：位于上游的黑灰产负责收集并提供各种资源，包括手机黑卡、公民个人信息、商业秘密、动态代理等；中游则负责开发定制大量黑灰产工具，以自动化的方式利用各类黑灰产资源实施各种网络违法犯罪活动；黑灰色产业链的下游负责将其活动“成果”进行交易变现，涉及众多黑灰色网络交易和支付渠道。

随着互联网的发展，盘踞在网络平台的黑灰产形态和规模也不断扩大。网络黑灰产一方面增加了企业运营的安防成本，恶化了竞争环境，导致劣币驱逐良币现象的发生；另一方面，也让普通网民的个人经济利益受到了极大的侵害，侵犯了公民的合法权益。疫情期间，不法分子利用广大人民群众增加上网时长、工作就业受影响的契机，实施了包括网络诈骗、传播违法内容、发起 DDoS 攻击、刷量等在内的多种违法犯罪行为。

1 生态化、多样化：黑灰产借势发展，攫取巨额利益

受疫情影响，广大网民的互联网使用率和使用时长增长明显。2020 年上半年，电商直播、短视频和网络购物等应用的用户规模增长最为显著，增长率分别 16.7%、5.8%和 5.5%。即时通信软件、搜索引擎、网络游戏和网络视频也保持增长，增长率在 1%-5%之间。同时，手机网络购物的用户规模增长已经超过 5%。[1]

与此同时，疫情期间的网络黑灰产呈现出更加频发的态势，不法分子开始实施网络诈骗、网络赌博、网络色情内容传播等各类犯罪行为。其中，仅网络诈骗黑生态的发展，较疫情前以金融类、网络赌博类、网赚类、冒充公检法人员等诈骗形式，快速衍生出包括买卖防疫物资诈骗、机票火车票退改签诈骗、贷款诈骗、网课缴费诈骗、网络游戏诈骗、刷单诈骗等与疫情相关的新型诈骗手法，危害了广大网民的切身利益。截至 2020 年上半年，全国公安机关共破获涉疫情诈骗犯罪 1.6 万起，抓获犯罪嫌疑人 7506 名。[2]

2 链条化、逐利化：以牟利为目的，分工不断细化

通常来讲，网络黑灰产定义为借助互联网技术、网络媒介，为黑客攻击、网络黄赌、网络诈骗、网络盗窃、网络水军等违法犯罪活动提供帮助，并从中非法牟利的犯罪产业。该定义方式更多的偏向与人民群众关系更加密切的网络犯罪业态。但是网络诈骗需要公民个人信息和非法话务中心的支持，网络水军需要账号批量注册黑灰产的协助，就连 DDoS 攻击也出现 SaaS 化的趋势，为下游犯罪提供支持与服务的上游黑灰产日益复杂，形成了一个巨大的网络犯罪生态。产业链的持续延伸导致其不断向集团化的方向发展。网络犯罪案件中，4 人以上团伙犯罪占到总案件量的 65%[3]，网络赌博、网络诈骗等产业链较长的犯罪团伙人员规模可达数百人。

网络犯罪集团内部既紧密又松散。紧密在于整个集团内部有统一组织者，有资金提供者，有数据提供者，有推广服务者，有话务员等，他们有的专门寻找各家平台的规则和技术漏洞，有的专门编写配套软件，有的专门负责发起网络攻击，有的专门负责拓展客户群，有的专门负责资金周转，彼此分工精细，任务明确，互相配合，各司其职。松散则在于集团成员之间以网上联系为主，彼此只了解对方的虚拟身份，不掌握彼此真实身份和所在地域，产业链上任何一个环节的团伙被打击，其他上下游团伙都能够迅速从其他渠道找到替补。

数据显示，利用互联网实施的犯罪，主要目的在于非法敛财，诈骗、盗窃这两类侵财型案件占了所有网络犯罪的 75%以上[4]。其他如非法吸收公众存款、开设

[1] 源自中国互联网络信息中心（CNNIC）发布的第 46 次《中国互联网络发展状况统计报告》
[2] 数据源自 2020 年 7 公安部新闻发布会通报来公安机关打击治理电信网络诈骗犯罪工作有关情况。
[3] 数据源自国家检察官学院浙江分院院长胡勇于 2019 年的“网络犯罪前沿问题高峰论坛”主题演讲。
[4] 数据源自国家检察官学院浙江分院院长胡勇于 2019 年的“网络犯罪前沿问题高峰论坛”主题演讲。

赌场、提供工具等也都是以敛财为目的，且与传统犯罪相比，涉案金额更大，受害人数更多，波及面更广。

3 国际化、低龄化：跨国、跨地域、年轻型犯罪比例上升

随着国内不断加大网络犯罪打击力度，网络犯罪国际化的趋势也愈加明显。网络犯罪本身不受空间限制，具有跨地域、跨时空的特点，只要能够连接网络，任何一台手机、电脑都可以成为犯罪工具。VPN 的发展和在我国境内的渗透，降低了黑灰产从业者翻墙与境外网络接触的门槛，黑灰产可利用国外一些知名度非常高的加密聊天软件进行违法犯罪交易。比如外网知名聊天软件 Telegram 中，就活跃着众多的黑灰产从业者，各种黑灰产群中交易不断。

近年来，“两高”、公安部、网信办等行业主管部门不断出台网络违法犯罪相关的法律政策和司法解释，并持续开展“净网”、“剑网”、“清朗”等专项行动，网络犯罪成员为逃避打击，逐渐与国外从事相关违法犯罪活动的人员加深合作，或者自己先潜逃境外再实施违法犯罪活动。网络黑灰产团伙的国际化程度不断加深，使得案件更加复杂化，证据采集难度加大，给司法机关侦办案件制造了一定困难。

除此以外，网络犯罪低龄化的发展趋势也不容忽视。《中国未成年人互联网运用报告》数据显示，我国 10 岁及以下未成年人开始接触互联网的人数比例达到 78%，未成年人首次触网年龄不断走低。与此同时，网络犯罪在犯罪主体上呈现橄榄型的年龄特点，属于典型的年轻型犯罪，年龄在 18-30 岁之间的占了网络犯罪主体的近八成。[5]

这主要是因为年轻人对互联网的了解和依赖度远比其他年龄段的人更深、更高，对互联网的应用、服务及各种技术的获取更加熟悉、便捷。同时，网络犯罪缺乏人与人的直接接触，极大降低了个人道德门槛和自我约束，心智尚未成熟的青少年极易在巨额利益的诱惑下铤而走险。

[5] 数据源自国家检察官学院浙江分院院长胡勇于 2019 年的“网络犯罪前沿问题高峰论坛”主题演讲。

二、互联网企业常见的黑灰产挑战

1 内容秩序威胁型黑灰产

随着我国互联网的快速发展，网络内容生态变得越来越多元化，人们已经逐渐养成了依靠网络获取信息的生活习惯。但是，在纷繁复杂的网络内容里也存在着大量的违法违规内容以及黑生态，尤其是疫情期间，各类违法内容呈现出高发态势，影响了网络生态内容的健康发展，威胁着网络平台和网民的利益。就威胁内容秩序的黑灰产而言，黑 SEO、网络诈骗、网络赌博、网络色情等最为常见。

1.1 黑 SEO

黑 SEO（Search Engine Optimization，搜素引擎优化）是一种为了提高 SERP（Search Engine Results Page，搜索引擎结果页）排名所使用的作弊技巧，手段多是钻搜索引擎算法漏洞或通过伪造优质内容的方式对网站进行修改。黑 SEO 本质是欺骗搜索引擎算法，让系统误认为经过其“优化”的网站是个“优质网站”。

1.1.1 黑灰产业态

黑 SEO 的手段主要可以分为：（1）关键词堆砌。通过对网站标题或是页面进行大量地关键词堆砌，包括使用长尾词、生僻词等手段，实现网站在搜索引擎中权重排名的提升，从而将用户诱导进入目标网站。(2)大规模站群。站群可以简单的理解为相互链接的众多网站，无论主题是否相关，所有的网站都链接在一起，构成了一个链接的网络系统。通过站群对网站进行权重的传递，欺骗搜索引擎获取靠前的排名。(3) URL 结构大量网址。通过对信息的堆积以及不合理的 URL 结构，黑 SEO 大量地发布目标网站的网址，欺骗搜索引擎对此类网址进行优先抓取。除此之外，隐藏文字、桥页、PR 劫持、垃圾链接和链接买卖等也属于黑 SEO 的常见手段。

黑 SEO 通过购买网站、黑客入侵等方式，将诈骗、赌博、淫秽色情内容等违法信息发布在众多网站上，再依靠不正当的手段确保这些载有违法信息的网站能够被普通网民搜索到，甚至出现在搜索结果靠前的显著位置。这些违法信息通常都含有电话号码、社交帐号、网址链接、下载链接等虚假内容。普通网民一旦添加联系方式或进入违法网站，就已经掉入了犯罪分子铺设的陷阱之中。

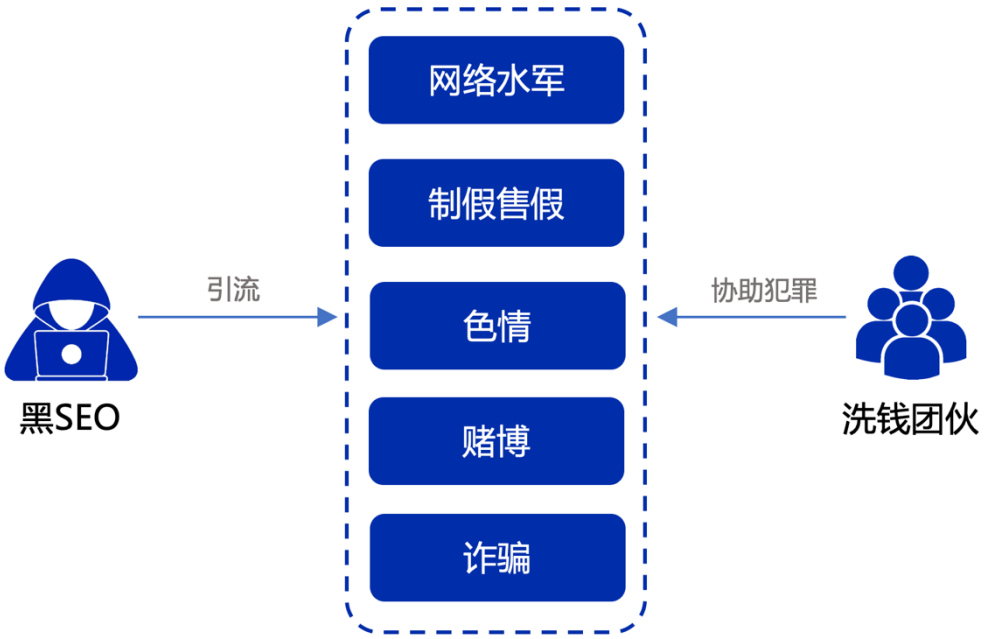

图 1 黑 SEO 产业业态

1.1.2 危害及防治建议

随着站内搜索的普及，黑 SEO 已从单纯影响搜索引擎逐渐发展为整个互联网行业的顽疾。黑灰产团伙通过多种手段为不法网站提供“刷排名服务”，干扰搜索结果质量，使黄赌毒、制假售假、诈骗等违法犯罪网站出现在搜索结果首页或联想词前列，威胁人民群众生命财产安全。黑 SEO 的经营主体作为事实上的内容发布者，完全不履行《广告法》《网络信息内容生态治理规定》等法律法规的责任义务，对发布内容、网站质量等不做任何把关，成为虚假信息传播的重要途径。

受疫情影响，很多中小型企业都受到了较大冲击，开始寄希望于通过黑 SEO 降低获客成本。一些不法分子开始借机兜售其黑 SEO“服务”。整个疫情期间，网络赌博和网络诈骗多发高发，黑 SEO 在其中扮演着关键角色，已成为传播违法信息的重要“帮手”。

作为违法内容重要的信息发布渠道，对黑 SEO 进行治理才是事前预防，降低网络案件发生率的治本之策，具体可以从以下三方面入手：

一是完善平台算法和智能策略，对网站内容、关键词匹配度、网站源代码进行检测，及时清理被植入的网站后门、恶意代码以及恶意攻击行为。

二是在全行业建立风险网站数据库，对网站进行安全等级分类，对合法合规网站进行有效保护，并对高危网站主动进行屏蔽，限制其搜索展现结果。

三是建立用户反馈机制，主动接受来自广大网民对虚假网站的举报并对网站进行技术检测和人工排查，杜绝网络犯罪发生的可能。

1.1.3 百度治理实践

作为保护网站和防止黑 SEO 的手段之一，百度于 2017 年推出的“新站保护机制”对符合条件的网站进行保护，加快其网站收录，保护优质原创内容，为新网站提供良好的发展环境。同时，百度于 2018 年 5 月推出惊雷算法 2.0，针对“恶意制造作弊超链”和“恶意刷点击”的作弊行为进行了算法升级，持续监督、抵制以不正当手段获取流量的行为，营造健康的搜索生态。

由于现有的法律并无对黑 SEO 犯罪的直接规范，在打击过程中给公安机关造成了一定困难。百度对于此类黑 SEO 犯罪的打击主要包含两方面，一方面加强技术手段进行日常巡查和防控，通过百度网址安全中心（https://bsb.baidu.com/）接受广大网民对虚假网站的举报；另一方面，坚持以“打击全黑灰产链条”为出发点，借助对黑灰色产业链下游各类黑生态的打击，反推至上游的黑 SEO，以《刑法》规定的“帮助信息网络犯罪活动罪”对其进行打击。

图 2 百度网址安全中心

案例：百度联合重庆、杭州两地警方破获系列网络诈骗案

案情：疫情期间，重庆警方、杭州警方侦破了多起网络诈骗案件，并成功打掉了隐藏在案件背后的多条黑灰色产业链，抓获涉案犯罪嫌疑人 25 名，涉及诈骗资金达 120 余万元。经警方调查证实有犯罪分子通过在热门游戏中发布购买或出售装备的信息，引诱网民到虚假网站进行交易，进而实施诈骗。为了骗取网民信任，犯罪分子利用生僻关键字对虚假网站进行搜索结果优化，使用户在百度搜索犯罪分子提供的关键词时，会被诱骗至虚假网站。

链接：

https://baijiahao.baidu.com/s?id=1675871333163997143&wfr=spider&for=pc

1.2 网络诈骗

1.2.1 黑灰产业态

一般来讲，网络诈骗的黑灰产链条层级较多且分工明确。黑客利用非法的技术手段，盗取大量公民个人信息，并贩卖给话务组。技术支持团队负责制作木马程序、钓鱼网站等恶意程序，为话务组的诈骗提供后台保障。位于黑灰产顶层的策划团队指使话务组，通过网络、电话、短信等方式向不特定的受害人发送诈骗信息。当话务组通知洗钱组赃款到账后，银行卡商利用虚假身份信息，开通大量银行卡，提供给洗钱组。洗钱组通过网银将账户上的钱快速转移，由取款组在各地的 ATM 上将钱取出，汇入网络诈骗集团的账户中。

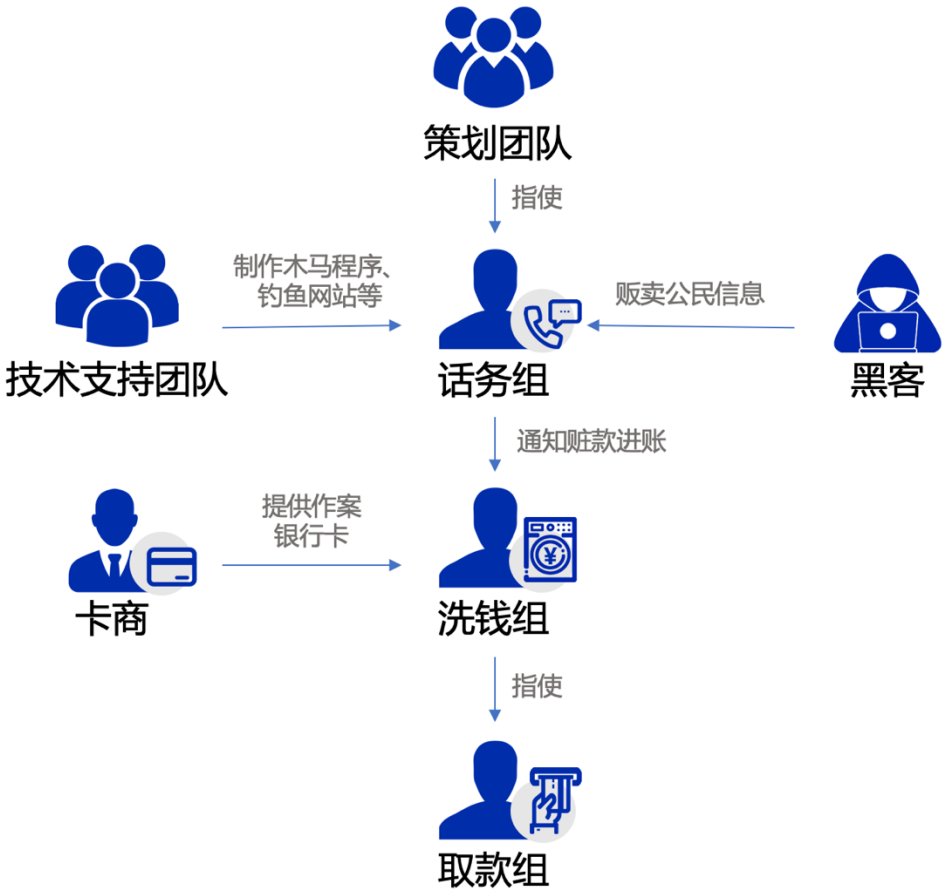

图 3 网络诈骗产业业态

1.2.2 危害及防治建议

当前，全国网络诈骗犯罪形势严峻复杂。上半年受疫情影响，国民生产生活加速向网上转移，犯罪分子借机以贷款、兼职刷单、冒充客服和虚假购物、虚假投资理财和网络赌博、冒充公检法机关等形式实施网络诈骗，威胁人民群众的利益。疫情期间也成为网络诈骗的高发期，公安部今年 7 月通报数据显示，截至 2020 年上半年，全国公安机关共破获网络诈骗案件 10.1 万起，抓获犯罪嫌疑人 9.2 万名。度小满金融发布的《2020 年上半年网络诈骗

分析报告》显示，网络诈骗团伙的目标人群集中在 21-40 岁，呈年轻化趋势。各类网络诈骗案件中，男性遭受网络诈骗占比达 70%，远超女性的 30%。网络诈骗人员的整体诈骗成功率在 20%以上，平均资损金额在 2900 元以上。

需要对虚假信息发布、个人信息窃取、贩卖作案工具等全链条进行综合治理。具体可以从三方面着手：

（1）断流。切断流量信息来源，网络平台应落实主体责任，加强内容审查力度，建立信息共享机制、完善用户反馈制度，形成平台合力，共同打击虚假信息发布。

（2）断料。加强个人信息保护，谨防因信息泄露和非法数据买卖被不法分子利用注册公司、开设对公账户、网络骗贷等，变成其牟利的工具。

（3）断卡。管制犯罪工具，着重对话务员、线路商、改号平台、贩卡商等环节进行重点打击。截至 2020 年 10 月 22 日，公安部“断卡”行动共抓获涉“两卡”违法犯罪嫌疑人 4600 余名，缴获电话卡、银行卡共计 6.5 万余张。

1.2.3 百度治理实践

疫情期间，百度内容巡查团队加大日常巡查力度，及时清理违规信息，维护用户的上网安全和切身利益。仅在 2 月疫情爆发的高峰期，百度通过多种排查、处置手段共清理疫情相关有害信息共计 147670 条，累计对 64437 条信息进行了巡查、处置和取证处理，其中涉及疫情的违法内容有 25291 条。百度刑事法务侦查部已经将 2000 多条违法犯罪线索向各地警方报送，配合公安机关破获涉疫情诈骗案 20 余起，涉案人员超过 160 人。

此外，百度于 2019 年发布“光明行动计划”，依托百度的人工智能技术与“搜索+信息流”双引擎生态，为政府部门与广大民众提供一手反诈防骗信息，精准打击网络诈骗犯罪。另外，为普及网络诈骗信息、增强警民互动，百度与中央电视台联合推出的“反诈骗互动平台”，依托智能小程序“全网追踪”，向用户提供防诈骗信息传递、举报、反预警等互动功能。

因网络诈骗的犯罪形式多样化、犯罪手法趋于集团化以及犯罪分子藏身海外等情况，给公安机关和网络平台进行打击制造了一定困难。对于此类案件的打击，百度借助于大数据优势为用户提供搜索保障，对搜索结果进行安全验证和风险提示，维护用户利益不受侵害。同时，通过每日的技术巡查、人工巡查和用户的举报信息，对平台内涉嫌网络诈骗的有害信息进行处理，并协助公安机关收集犯罪线索及犯罪证据，配合公安机关的刑事打击。对于网络诈骗，用户在百度搜索中直接输入想要查询的陌生号码时，搜索结果会出现认证结果，帮助用户识别陌生号码是否是诈骗、广告、还是官方客服。

图 4 百度安全号码认证平台

案例：《百度战疫：清理有害信息 14 万余条 联合警方破获口罩诈骗案》

案情：疫情出现以来，一些不法分子利用部分网民急于购买口罩的心理实施诈骗行为。对此，百度贴吧等产品已连续开展两次专项行动，对相关信息进行排查、挖掘和处理。对于其中涉嫌利用口罩实施诈骗行为的，百度已经联合各地警方进行了多起打击。截至 2 月 13 日，全国公安机关与百度开展合作共破案 21 起，查处嫌疑人 12 名。

链接：

https://baijiahao.baidu.com/s?id=1658859802849709769&wfr=spider&for=pc

1.3 涉黄涉赌等违法内容产业

1.3.1 现状及趋势

年初以来，人民群众的上网时长普遍增加，对网络内容的需求也随之加大。以网络赌博和网络色情为主的违法违规内容在此期间内也呈快速增长趋势，不仅内容形式更加多样化，而且传播方式也变得更加隐蔽，出现了弹幕、评论等传播形式。这类违法内容往往需要经过多层转化后才能接触到违法信息，给网络平台的审核造成了一定难度。

公安部在疫情期间专门发布《关于新冠肺炎疫情期间依法严厉打击跨境赌博和电信网络诈骗犯罪的通告》，重点围绕境外赌场和赌博网站两类犯罪主体进行严厉打击。据公安部通报，截至 2020 年 9 月底，全国公安机关共立各类跨境赌博案件 8800 余起，抓获犯罪嫌疑人 6 万余名，打掉涉赌平台 1700 余个、非法技术团队 730 余个、赌博推广平台 820 余个，打掉非法支付平台和地下钱庄 1400 余个，查明涉案资金上万亿元。

网络色情在 2020 年也呈现出新特点，出售自制淫秽视频内容的比例增加，并且呈现出“帮帮带”现象，即多名淫秽视频拍摄者互相是情侣、亲属或朋友关系。早期涉及网络色情案的犯罪分子文化程度相对比较低，但近年来情况发生了一定程度的转变，高学历涉案人员已经接近 4 成。而且，多数

犯罪分子都拥有优秀的互联网思维和营销能力，有的犯罪团伙甚至横跨境内外，利用最前沿的技术搭建了自己的黑灰色产业链生态体系。

网络违法内容产业不仅花样繁多，而且具有传播范围广、速度快和形式多样等特点，不仅危害了网络内容生态的健康发展，也时刻威胁着网民的个人利益。随着移动互联网的发展，网络赌博、网络色情等违法内容产业通过网络视频、直播软件、网络社交软件进行传播的趋势更加明显。同时，以制作、传播、买卖违法内容为目的的网络犯罪也已形成黑灰色产业链的发展趋势，上下游环节分工明确，衔接紧密。

1.3.2 黑灰产业态

伴随着网络赌博运作模式的专业化、智能化、跨境化的发展趋势，网络赌博已经形成了包括赌博人员招聘、网络推广、赌博网站运营、洗钱等上下游在内的完整黑灰产链条，各环节分工明确、密切配合、而且多为跨国跨地域作案，给公安机关的打击造成了一定困难。

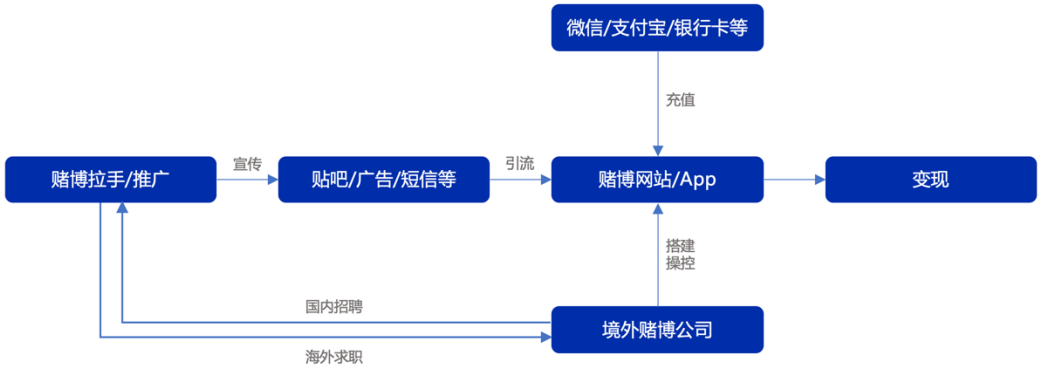

图 5 赌博产业业态

作为危害内容生态健康的最大威胁之一，网络色情借助于互联网新技术的发展和应用，也已呈现多元化的发展趋势。色情图片和视频、色情直播、自制淫秽视频、网络色情交易、淫秽物品买卖等网络黑灰产业链发展逐渐成熟的同时，也滋生出以色情内容为诱饵的网络诈骗和网络赌博等犯罪行为。

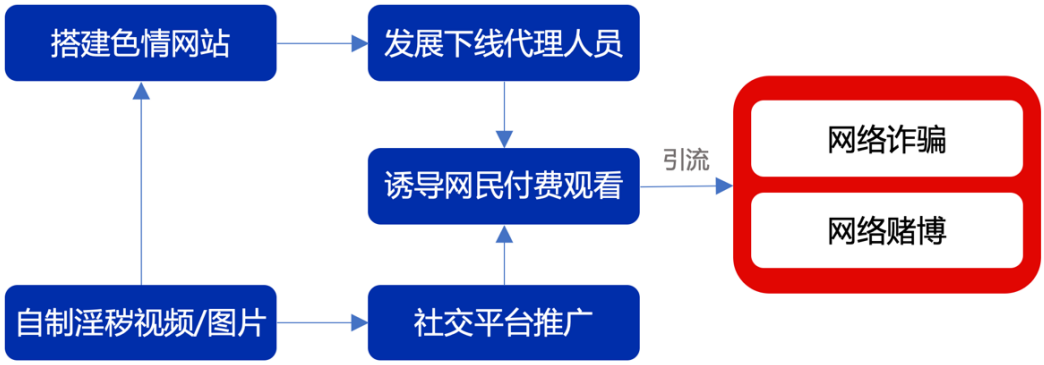

图 6 色情产业业态

1.3.3 危害及防治建议

随着互联网的普及，网络违法内容已经成为污染网络生态和人们精神世界的一大“毒瘤”，产生了极其不良的社会影响。2020 年 3 月 1 日实施的《网络信息内容生态治理规定》，明确了政府、企业、社会、网民等主体多元参与协同共治的治理模式，对网络内容的生产者、网络平台和网络内容服务的使用者做出了明确规定，更加强调网络平台应当履行信息内容管理主体责任，主要可以从以下四方面进行防控：

（1）健全用户注册制度。严格贯彻网络实名注册制度，确保账号到人。同时，积极落实未成年人防沉迷制度，保护青少年的身心健康。

（2）加强用户账号管理制度。保护用户个人信息的同时，开展账号风险分级管理，对涉嫌违规账号及时处理，避免侵害广大网民的利益。

（3）强化信息发布审核及管理。加大平台内容生态审查力度，扩大内容审核范围，建立内容风控二道防线，通过技术拦截和人工审核的方式维护平台内容生态的健康发展。

（4）黑灰色产业链信息处置制度。提高对网络黑灰产发展与趋势的警觉，建立平台级黑灰产监控体系和响应制度，发挥互联网企业的技术优势，积极配合公安机关的打击工作。

1.3.4 百度治理实践

2019 年，百度内容安全中心利用 AI 人工智能技术清理违法信息共计 530.7 亿余条。其中淫秽色情类信息是重点打击对象，占比为 49.25%，赌博类占比为 31.70%。其中，以杀猪盘为代表的赌博内容占比 45%，封禁了杀猪盘类违规账号 1.1 万余个。

借助人工智能技术，百度建立了“百度安全网络黑灰产监测与检测系统”，系统以保护网络安全，打击网络黑灰产为目的，运用图像识别、富媒体识别、NLP、分类/聚类、关联挖掘、机器学习方案等算法能力和技术创新手段进行黑灰产线索挖掘及分析，针对不同的产品形态，建立公司级的黑灰产态势平台，形成防、控、打、宣一体化联动机制，持续保持打击力度并为各地警方提供有效的案件打击支持。同时，百度也建立了完善的用户反馈机制，接受来自用户的举报，及时清理平台内的违规内容。

截至 2020 年 7 月，百度内容安全中心持续通过全方面手段打击清理百度全产品线的有害信息，其中利用人工智能技术挖掘打击淫秽色情类、赌博类等相关有害信息共 58.2 亿余条，通过人工巡查打击侵权类、淫秽色情类等相关有害信息 590 万余条。同时，打击医疗变体词 300 万个，拒绝不合规广告 1.56 亿条。百度各产品接收网民举报共计 426281 件，其中有关色情内容举报 150456 件，赌博类内容 52978 件，清理涉黄关键词 12232 组，引导组 4193 组，封禁相关账号 39621 个，关闭贴吧 1104 个，清理有害链接 14.46

亿条。

2 数据流量威胁型黑灰产

当今的互联网时代，数据和流量是构成网络行业生态的重要组成部分，是关乎到互联网企业发展和命运的关键要素，也是网络黑灰产关注和实施犯罪活动的高发领域。在这个“数据为王,流量至上”的时代，网络黑灰产通过流量劫持、恶意点击、刷单刷量、窃取数据等违法手段牟取不法利益，不仅危害了互联网企业和公民的合法权益，更是对国家经济发展造成了极为恶劣的影响。

2.1 恶意点击

2.1.1 概念

恶意点击是通过伪造点击量、播放量、下载量等各种流量假象，谋取不当利益的黑灰产。在数字化浪潮下，各行业都朝着线上发展，数字营销也成为广告行业的热点和趋势。由于数字营销供应链的复杂化与不透明，在面临 KPI 压力及企图最大化变现的情况下，部分供应商会选择流量作弊，雇佣黑灰产进行恶意点击已经成为常见手段。近年来，流量造假、恶意刷量等事件层出不穷，不仅吞噬着企业的利润，也极大扰乱了互联网行业的秩序。以广告刷量为代表的恶意点击行为，不仅严重破坏计算机系统的安全性，而且成为企业不正当竞争的手段之一，产生“劣币驱逐良币”的不良后果，扼杀互联网行业的生命力。

2.1.2 现状

目前，网络推广渠道结算的方式主要包括 CPM、CPA、CPC、CPT。CPM（Cost Per Mille）是通过计算每千人的曝光花费进行结算，CPA（Cost Per Action）是通过每个购买行为的平均花费进行结算，CPC（Cost Per Click）是通过每次点击的平均花费进行结算，CPT 是通过时间长短（每天）的花费进行结算。除了 CPT 之外，其他 3 种结算模式都直接与流量挂钩。因此，在以流量为主要衡量标准的结算模式中，推广渠道往往会虚增流量，以提高自身收入。目前，全国从事广告恶意点击的黑灰产人数超过 300 万，每年产生的广告刷量约占总流量的 30%，导致广告资源损失超过 200 亿元。

2.1.3 黑灰产业态

一般来讲，恶意点击的实施者主要是自身缺乏稳定流量又意图谋取暴利的非正规网站或平台。他们通过恶意点击增加其网站或平台流量，从而实现获得巨额广告佣金或流量采买费用的目的。还有少部分恶意点击行为来自同行业的竞争者，其目的是消耗竞争对手的预算，迫使其广告下线，以使自己的广告排名上升。此外，也有部分黑灰产以敲诈勒索为目的，对企业正常的推广活动进行破坏。

黑灰产进行恶意点击有两种路径，一种是机器点击，另一种是人肉刷量。

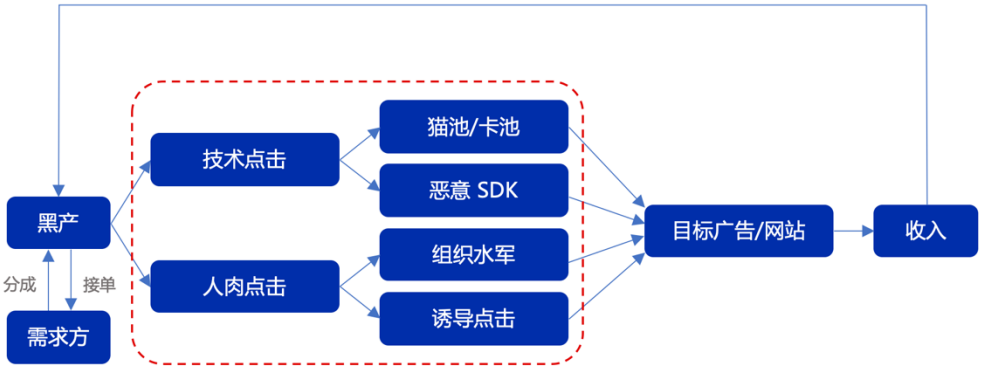

图 7 恶意点击产业业态

机器点击又可进一步细分为两大类，一类是猫池、卡池点击，一类是后台静默点击。猫池、卡池点击是黑灰产人员利用大量的非实名电话卡、物联网卡伪造大量用户并实施恶意点击。后台静默点击则是通过自制含有恶意 SDK 的手机软件安装包，对安装了该软件的手机进行后台控制，实施恶意点击行为。当用户在使用这些带有恶意 SDK 的 APP 时，其网络访问路径可能被劫持到特定渠道，或者悄悄访问网站、浏览文章或点击广告，用户在毫不知情的情况下被卷入刷量黑灰产等违法犯罪活动中。

随着各大平台对机器点击的围剿，恶意点击的方式逐渐由机器点击向人肉点击过度。人肉点击也可以分为两大类，一类是由水军头目组织普通网民点击，即刷量组织者通过微信群、QQ 群或者网赚平台，将刷量点击包装成网赚项目，普通网民在接受网赚任务后点击刷量组织者提供的广告链接。另一类是通过各种方法诱导普通网民点击，典型方式是将平台企业的广告弹窗设置成透明，浮动在色情图片的上方，再通过图片上的文字诱骗网民点击，网民误以为点击后能免费观看色情视频，其实却不能。但是，平台企业却会向黑灰产支付广告点击、浏览费用。

图 8 人肉点击和机器点击

图 9 恶意点击组织

2.1.4 危害及防治建议

恶意点击不仅给广告主带来经济损失,而且毒害了公平竞争的市场风气。为了躲避平台风控策略，黑灰产逐渐研发出以恶意 SDK 为代表的非法程序，手段的隐蔽性和危害性越来越高，严重威胁互联网企业和用户的系统安全。

首先，对于机器恶意点击行为，可以采取限制 IP、使用防范软件的方式进行屏蔽。单就商业类的恶意点击行为，如恶意点击广告等，可以通过设置消费限制、观察异常流量的方式进行处理。

其次，对于人肉恶意点击行为，由于其背后通常都是来自用户的真实点击行为，较难识别，可以对关键词的转化率、网站到达率、账号消费情况进行分析，对疑似的恶意点击行为第一时间进行人工复核与识别，避免利益受到损失。

2.1.5 百度治理实践

借助大数据系统和自动巡查引擎，结合百度积累的大量黑灰产数据，百度可以通过技术手段识别并防控恶意点击行为，如薅羊毛、恶意点击等网络黑灰产。同时，百度也不断提升自身的数据算法和运力，有效评估各渠道流量，对异常流量及时预警，从而严控并打击通过刷点击量等恶意手段提升网站搜索排序的作弊行为，以此保证用户的搜索体验以及客户利益，促进平台内容生态的良性发展。

为维护客户利益不受侵害，百度推出“商盾”恶意点击防御系统，通过对 IP、Cookie 等多维数据分析访客的点击行为，阻挡、过滤无效访客对客户推广信息的检索和点击。“商盾”允许用户通过手动展现屏蔽和策略展现屏蔽两种方式进行禁封 IP 等设置，阻挡和过滤无效点击，进而防止恶意点击行

为。

2.2 流量劫持

2.2.1 概念

流量是指用户访问网站、打开 APP、下载安装包等使用互联网的行为。对互联网公司而言，用户的相关行为意味着使用量和关注度，公司能够转化为商业价值。所谓流量劫持是指通过技术手段改变用户访问对象、访问路径或者改变用户获取的数据的违法行为。

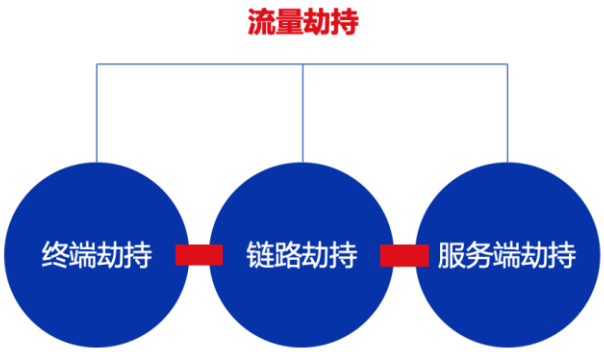

图 10 流量劫持分类

流量劫持的具体形式可以分为终端劫持、链路劫持、服务端劫持。

终端劫持指的是黑客通过攻击 DNS 服务器或者网民的 Wi-Fi 设备，使网民对特定网站的访问请求被错误解析到其他地址或者使请求失去响应，其效果就是对特定的网络不能反应或访问的是假网址。

链路劫持又称数据劫持,指的是运营商或者黑客针对传输过程中的数据，通过在用户至服务器之间植入恶意代码或者控制网络设备的手段，监听、篡改用户和服务器之间的数据，达到窃取用户重要数据（包括用户密码，用户身份数据等等）、修改用户访问页内容的目的。

服务端劫持指的是黑客对用户手机、PC 或者浏览器的劫持。常见的是，黑客在网站挂载木马程序，使用户无法正常退出该网站或者退出到假网站。假网站以仿冒的搜索引擎为主。

2.2.2 现状及趋势

中国互联网络信息中心（CNNIC）发布的第 46 次《中国互联网络发展状况统计报告》显示，截至 2020 年 6 月，我国网站数量已从 2018 年最高峰时的 544 万个下降至 468 万个，APP 数量也从 2018 年的 452 万下降至 359 万个。在此背景下，互联网企业之间围绕用户、流量的争夺日趋激烈，少数不

法分子铤而走险，企图依靠流量劫持等不正当手段攫取非法利益。在此过程中，大型平台互联网企业作为网民最主要的网络入口，已成为流量劫持行为的主要受害者安全。

2.2.3 黑灰产业态

流量劫持的实施者主要是能够进行流量变现的各种渠道商或者用户群体高度重叠的竞争对手，此外还有电信运营商、黑客等。

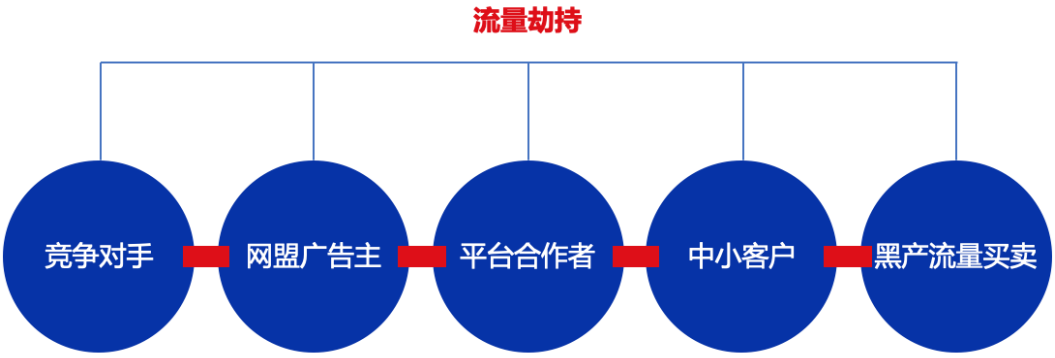

图 11 流量劫持实施者

近年来，流量见顶使各家互联网企业都感受到了前所未有的危机。作为应对之法，有的企业开拓下沉市场，有的企业进行多元经营，而有的则开始走歪门邪道。随着传统企业与互联网的融合不断加速，“流量劫持”作为很多互联网企业用来攻击竞争对手的不正当竞争手段，也被传统企业纷纷效仿。这种局面不仅损害了企业的切身利益，还损害了市场公平竞争机制，损害了消费者的系统安全和自主选择权。最高法院第 102 号指导案例黄某某破坏计算机信息系统案实际上就是这方面的典型代表，5W 网页导航雇佣黑客劫持了 2345 网页导航的流量，造成了恶劣后果。

除了来自外部的劫持，企业生态内部也可能出现流量劫持并造成巨额损失。互联网公司或多或少的都会通过各种渠道购买一定的用户流量，同时向渠道支付流量采购费用。有些流量渠道为了增加自身收入，通过技术方式将采购公司的自然流量劫持成渠道流量，给采购公司增加额外的流量采购费用。

同时，一些不法网站站长为了节省推广成本，也会与黑灰产团伙勾结，在自有的网站上挂载木马程序，强迫用户停留或者引导用户至某个特定页面，从而实施回退劫持的行为。此外，一些黑灰产还会实施无差别攻击。黑灰产先控制一定数量的设备，再根据客户需求将流量引导致特定的地方。这些黑灰产主要攻击的是 C 端用户，B 端企业是他们的客户。他们一般以千人 IP 为单位贩卖流量，根据用户的质量和数量价格不等，最高可以卖到 70 元/天。

2.2.4 危害及防治建议

国家互联网信息办公室于 2019 年发布的《网络信息内容生态治理规定》中明确规定了不得使用人工方式或者技术手段实施流量造假、流量劫持获取不正当商业利益的行为。打击流量劫持现象需要国家有关部门牵头进行综合治理，加强行业共治，强化企业尊重商业规则，从而对流量劫持进行整体的

防控与打击。同时，还需要针对不同的劫持方式开展多元化治理。

一是推动 HTTPS 普及。与明文传输协议 HTTP 不同，HTTPS 依靠证书来验证服务器的身份，并对用户和服务器之间的通信加密，因此能够有效抵御针对网站的流量劫持等攻击。另外，要尽量做到全站 HTTPS（即 Always On SSL），以此 保证用户机密信息和交易安全，防止被攻击和劫持。

二是 ICP 和 ISP 服务商合作共赢。从行业现状看，部分基础设施运营者在业绩压力下存在实施劫持的违法行为。对此，内容服务商和基础设施运营者需要找到一条合作共赢的出路，从服务器层面杜绝黑客行为。

三是加强用户终端的防护。用户端防护主要指的是硬件强化方面。手机发展至今，其算力已经足以支撑更强的防御策略，可以由工信、公安等部委牵头制定手机安防行业标准，将网络攻击预警与线索举报进行贯通，实现流量安防领域的早发现、早处置。

2.2.5 百度综合治理概述

一直以来，百度对于危害用户隐私和安全的恶意劫持行为都秉承“零容忍”的态度，并利用百度的人工智能和技术优势，先后推出包括“烽火反劫持计划”在内的系统防控机制，对可疑或问题站点进行干预处理，全力打击如回退劫持、跳转劫持等流量劫持行为，保护用户的搜索体验和网络安全。与此同时,百度也积极推动第三方网站站点改造 HTTPS 或者建议各网站自查，并保持与第三方资源提供者的充分沟通，保证网站统计、网站优化、推广广告等使用的第三方资源不存在恶意劫持的情况。此外，百度还通过搭建智能小程序，增强网站的安全性和可控性，降低被劫持的风险。

从 2009 年百度诉青岛联通“流量劫持”的“侵权第一案”，到 2015 年付宣豪、黄子超“DNS 劫持”的“入刑第一案”，从民事到刑事，百度不遗余力地推进案件的侦办。除了借助技术手段进行打击，百度于 2017 年组建互联网黑灰产打击团队，严厉打击窃取用户隐私、发布虚假信息、流量劫持、买卖公民信息等各类网络黑灰产并已协助公安机关破获上百起案件，涉案金额达数亿元人民币。

案例：百度联合警方破获“假百度”回退劫持案 犯罪分子均已获刑

简要案情：河南开封警方查明，犯罪团伙以“客服精灵”为旗号开展霸屏和回退劫持服务。其将违法代码上传至客户网站，网民通过搜索引擎进入相关网站后再点击浏览器的返回按钮,就会返回到一个假的百度页面。此时，网民无论点击哪个搜索结果或重新搜索任意关键词，都会进入到包含某些特定广告的页面，这其中甚至含有一些非法内容。同时，涉案犯罪团伙还从事在“假百度”里修改竞争对手网站客服信息以截取客户、抓取用户手机号码等个人信息的违法行为。2019 年 6 月 20 日，法院判决涉案公司 4 人犯破坏计算机信息系统罪，分别被判处有期徒刑 1 年 9 个月至 1 年 11 个月不等。

链接：http://3g.donews.com/News/donews_detail/3079832.html

2.3 网络水军

2.3.1 概念

网络水军是指在网络中针对特定内容发布特定信息的、被雇佣的网络写手。网络水军广泛活跃在电子商务网站、论坛、微博等社交网络平台，从事着批量发帖和顶帖引流等工作。他们伪装成普通网民或消费者，通过发布、回复和传播博文等手段对正常用户产生影响。

2.3.2 现状及趋势

网络水军已从单纯的大 V 引导和付费删帖，发展成为大 V 发文引导，批量发帖控评，压制不同意见的全方位舆论控制方式。有组织的水军行为和大规模的批量发帖不仅危害正常的网络内容秩序，而且这种编造虚假信息、诽谤攻击、大量刷帖控评、黑公关、非法推广等行为已经危害了互联网生态发展，扰乱了正常社会秩序，并涉嫌触犯《刑法》、《治安管理处罚法》等相关法律法规。

同时，网络水军已经从人肉水军向 AI 伪原创、批量发帖工具发展。批量发帖工具是一种在贴吧、论坛等平台大量发帖的工具，通常还附有转帖跟帖等诸多功能，因其能够在短时间内在论坛发出大量的贴文，该工具已成为黑灰产实施犯罪的重要途径和手段之一。

批量发帖工具的出现为网络水军提供了极大的便利，降低了黑灰产犯罪成本,却给各平台企业增加了内容巡查的难度和防范打击的困难。一般来说，此类工具操作简单且多数软件工具都支持多帐号自动登录，批量群发，自动顶帖等功能。

2.3.3 黑灰产业态

随着网络的发展，水军已经形成了有组织、有分工的黑灰产业链条模式，其黑灰产业链包括：链条上游的金主，主要包括广告商、委托人、爆料人等。他们通过“水军”炒作提高其投放广告的点击量；委托人、爆料人提供炒点，通过“水军”攻击炒作指定单位、人员、事件达到自身诉求。位于产业链下游的人员主要由“网络水军”业务的辅助实施者构成。其中包括专业推手、小型非法网站运营者和知名网站“内鬼”。专业推手往往是一些网络“大 V”“网红”等，借助自身在“粉丝”中的影响力，为炒作活动站脚助威；小型非法网站运营者、知名网站的“内鬼”（如编辑、版主）主要是接受“任务”，协助“网络水军”删除、置顶帖文等，从中谋取非法利益。

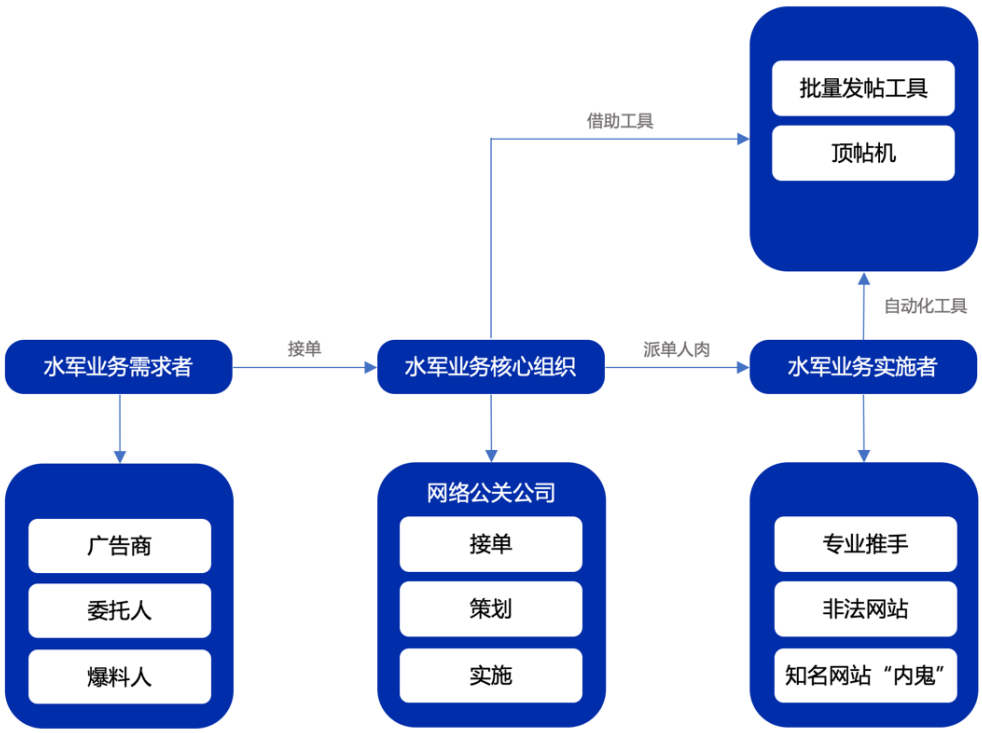

图 12 网络水军产业业态

2.3.4 危害及防治建议

因网络水军多是跨地区且利用网络化工具开展的多种违法行为，客观上增加了治理难度。要治理网络水军，需从多个方面入手。

首先，健全信息公开制度。要保证主流新闻媒体的权威性和公正性，提高媒介公信力，着重解决信息不对称的问题。健全信息公开和不实信息处理制度，完善权威信息发布平台和辟谣平台，让舆论回归事实和理性，维护良好网络环境。

其次，加强互联网企业管理。互联网运行企业应落实主体责任，落实网络实名制和人员审查制度，加强内容审核，严格依法依规提供互联网服务。互联网运行企业应当制定网络安全事件应急预案，在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

最后，互联网监管单位需形成合力。网信、公安、市场监管等部门要形成监管合力，建立长效监管合作机制，打造跨部门、跨地域的信息共享机制，形成无缝对接、有机衔接地打击“网络水军”的合作机制。要从根本上切断“网络水军”的资金来源，通过引导建立正确的互联网价值观消除其生存土壤。

2.3.5 百度综合治理概述

以维护网络内容生态的健康为目的，百度内容风控中心利用人工智能技术和人工巡查的方式，对平台内的网络内容进行全天候的巡查，及时清理各类违规信息。对于黑灰产使用的恶意发帖软件、恶意顶帖软件等行为，百度

也从技术手段进行封堵，对于违规操作的账号进行封禁，对此类黑灰产工具进行坚决打击。同时，百度也以挖掘和打击黑灰产业链条为目的，对此类网络犯罪行为进行整体打击。

截至 2020 年上半年，百度针对水军刷单、买卖公民信息等内容进行深入挖掘，清理拦截有害信息 588 万条，关闭贴吧 167 个。

2.4 非法获取、买卖个人信息

2.4.1 现状及趋势

随着网络的发展，人们已经习惯为了获取便利高效的服务，而不假思索的录入自己的姓名、电话、住址、银行卡号等隐私信息。手机 APP、恶意 SDK、可联网设备等都已经成为个人隐私泄露的重要渠道。

伴随人工智能技术的快速发展与应用，生物数据泄露的问题日益严峻。首先，人体的指纹、虹膜、面容、DNA 等个人生物信息的获取、采集、存储和应用越发便利和普及，众多手机 APP 通过收集个人生物信息作为用户登录和进行网络支付的密钥，如人脸识别、指纹识别等，这些信息一旦被不法分子利用，将对网民的个人利益造成危害。其次，恶意 SDK 和第三方应用违规盗取用户信息的趋势越加明显。部分 SDK 包中会加入一些恶意功能，轻者违规获取用户信息，重者则会威胁手机隐私安全、资金账户安全。

2.4.2 黑灰产业态

非法获取、买卖个人信息本身已成为众多网络黑灰产的上游，同时，其自身也在进一步细分化并已经形成了一条链条长、利益庞大的黑灰色产业链，这条产业链结构完整、分工细化，包含上、中、下游三部分犯罪环节。

上游：用户信息非法获取和通过违规手段获取大量用户信息，如恶意爬虫、病毒软件、APP 违规收集个人信息、恶意 SDK、山寨 APP 以及人为故意泄露等。

中游：违规买卖个人用户信息，中游环节负责对其进行处理与再加工，通过买卖、交换等形式形成规模化市场，对个人信息明码标价进行买卖。

下游：使用个人信息进行违法犯罪活动，不法分子通过购买得到数据，并利用这些数据进行精准诈骗和敲诈勒索等违法犯罪活动。

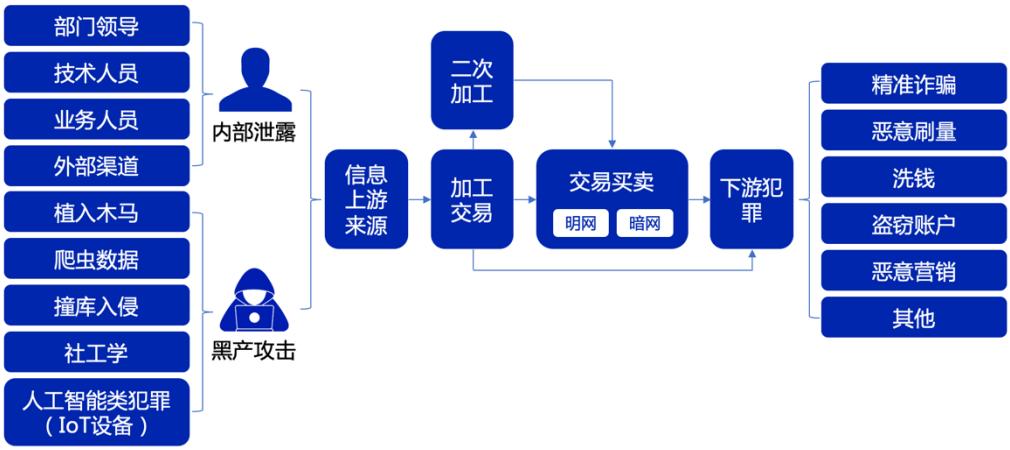

图 13 非法获取、买卖个人信息产业业态

同时，黑灰产从业者往往会利用一些社工库信息通过撞库等手段，获取更多的用户信息从而实施变现。除了诈骗盗号、发广告、刷量等直接变现之外，黑灰产还会将非法获取的个人信息数据打包成标准化的产品，对外出售或提供服务，与正规的数据行业别无二致。

2.4.3 危害及防治建议

个人隐私泄露和数据买卖轻则打扰民众的正常生活，如接到垃圾短信和骚扰电话等。重则可能带来人身财产损失。犯罪分子利用非法获取的信息实施盗号、虚假网贷、网络诈骗等新型的、非接触式犯罪。中国互联网络信息中心(CNNIC)发布的第 46 次《中国互联网络发展状况统计报告》显示，截至 2020 年 6 月，20.4%的网民表示遭遇过个人信息泄露，遭遇网络诈骗的网民比例为 17%。

国家网信办和网络平台一直都在普及网络安全知识，提示公民保护个人信息。除此之外，网民也应在提高个人隐私保护意识的同时，从以下几方面小事做起，保护自己的隐私不受侵害：（1）在公开网站平台填写信息时，避免用真名或实名拼音，非必要时不要在线填表，尽量用邮箱代替手机号码。（2）一定要仔细阅读涉及个人隐私内容（如通讯录、短信等）的权限获取申请。(3)在不必要的情况下记得关闭软件定位，以免泄露个人位置信息。(4)收集整理好含个人信息的票据，集中销毁。(5)及时注销，解除绑定长时间不使用的账户。不要在社交媒体随意公开自己及家人隐私信息。(6)不点击浏览不知名的网站、不随意下载来历不明的应用软件。

2.4.4 百度治理实践

基于 AI 能力的安全/隐私问题检测及动态分析平台，百度可以帮助企业高效、低成本地开展 APP 合规问题自查，确保企业隐私合规，降低隐私和数据泄露的风险。同时，百度 AI 检测技术提供隐私风险项检测、隐私专项检测、场景检测、权限过度收集与使用情况检测等产品服务，深度挖掘 APP 隐私合规风险产生的源头。

百度积极配合公安机关在线索提供、黑灰产溯源等层面展开大量工作，

为公安机关提供坚实的技术支持，成功协助公安机关破获多起非法获取公民个人信息案件，成功打击从黑灰产工具制作、多层级销售代理到黑灰产工具购买者的整个黑灰色产业链。同时，百度通过自动巡查、自主清理、用户举报等方式，持续对不良信息进行重点监控和打击。仅 2019 年，就累计清理下线“涉嫌窃取公民个人隐私”的恶意网站 46 万余个，网址 230 万余个。

3 技术威胁型黑灰产

技术威胁型黑灰产是指通过技术手段非法牟利的网络黑灰产，此类黑灰产主要隐藏在互联网的物理层、链路层、网络层和传输层，一般不在应用层呈现。技术型黑灰产可以通过技术手段直接实施犯罪，也可以作为技术提供者为网络犯罪的各环节提供支持。形态以恶意注册、DDoS 攻击、Web 应用攻击等最为常见。

随着疫情期间各行各业加速向线上转移，技术威胁型黑灰产攻击的受害范围更广、造成的潜在损失更大，技术型犯罪的发案数量也随之抬头。此外，随着 IOT 设备和物联网进入新的发展阶段，未来会有大量技术型黑产涌入此行业，这必然会给 IOT 设备厂商的安防能力带来极大挑战。

3.1 恶意注册

3.1.1 概念

恶意注册是指不以正常使用为目的，违反国家规定和平台注册规则，利用非法或虚假信息，批量注册平台账号的行为。恶意注册离不开 “卡商/号商”和“接码/打码平台”这两个角色的帮助。

3.1.2 现状及趋势

目前我国网络账号按照实名制原则进行管理，但各种互联网产品存在强实名制和弱实名制的差异。恶意注册由于使用的是非实名的手机号码或邮箱，身份绑定环节也多使用的是虚假的或者非法获取的公民信息，完全规避了实名制原则，造成账号的注册信息与实际使用人信息不对应。这样的行为不但突破了互联网行业的安全策略、增加了安全防护成本，而且给其他黑灰产提供了重要的作案工具。

面对这样的威胁，互联网公司普遍采取提高注册门槛的安全策略来应对，例如由弱实名制注册转为强实名注册、IP 限制、邀请好友辅助注册、人脸识别等。但恶意注册者又会对这些策略和措施不断地进行攻击和突破，如使用工具批量注册、外挂注册、批量养号等。双方呈现一种“道高一尺、魔高一丈”的状态。

3.1.3 黑灰产业态

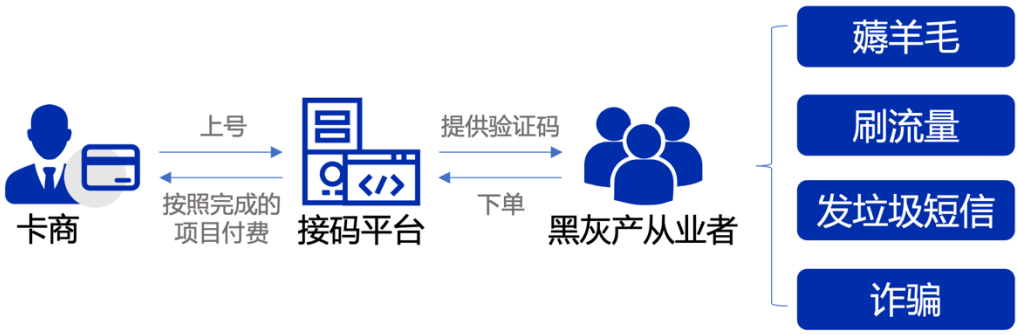

图 14 恶意注册产业业态

目前，恶意注册已经形成一个成熟的黑灰色产业链，为下游网络诈骗、薅羊毛、刷量等违法犯罪提供资源。例如在互联网广告生态中，黑产控制大量恶意注册的广告联盟账号来刷量，骗取广告费用；在内容生态中，控制大量普通账号在贴吧、论坛等产品中发布违法信息引流，从事高危活动。

3.1.4 危害及防治建议

恶意注册的危害波及范围极广，黑灰产利用虚假账号薅羊毛给企业造成经济损失的事情常有发生，多种下游犯罪也都需要依靠批量注册账号才能实施或实现盈利，如网络水军、恶意点击、数据刷量、网络欺诈、色情犯罪等等。

防治方面建议从四个环节入手，构建治理生态闭环。一是情报分析。开发定制版防控系统，迅速感知威胁情报并分析攻击来源和种类。二是深度溯源。建立公司级的黑灰产态势平台并搭建神经网络，实现对攻击深度溯源。三是电子取证。构建黑产打击生态闭环中的重要环节，以及时固化证据，以便司法追偿。四是司法打击。持续的高强度司法打击，提高法律震慑效果。

3.2 DDoS 攻击

3.2.1 概念

DDoS 攻击(Distributed Denial of Service，简称分布式拒绝服务攻击)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通信请求，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。一次完整的 DDoS 攻击体系由攻击者、主控端、代理端和攻击目标四部分组成。

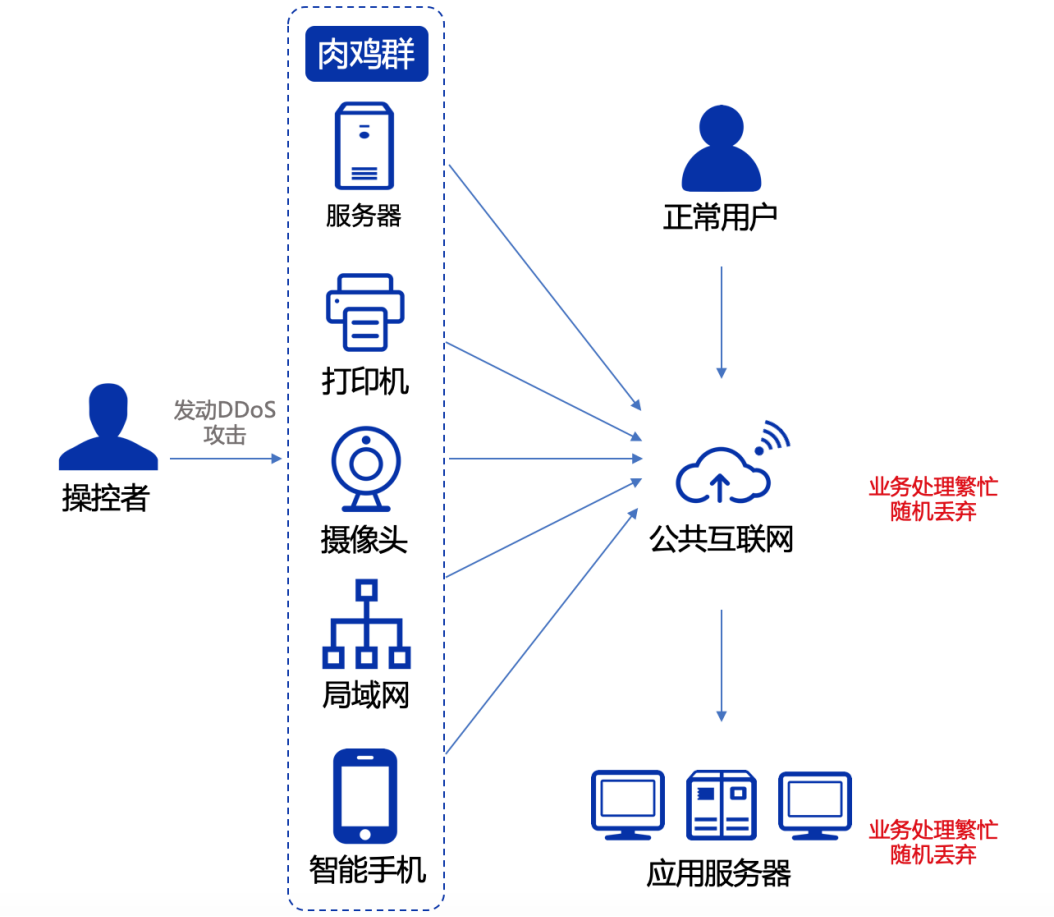

图 15 DDoS 攻击产业业态

3.2.2 现状及趋势

以前，DDoS攻击的主要承受者主要是自行搭建服务器的运营商和诸如美国Dyn之类的网络基础设施提供者。近年来随着云计算的兴起，云服务商也逐渐成为DDoS攻击主要的承受者。

2019年百度全网范围共监测到DDoS攻击36万余次，相对于2018年的46万余次有所减少。但今年开始，疫情造成线下的暂时失能，大量传统行业线下业务被逼上线，DDoS攻击次数随之攀升，2020年Q3单季度的攻击量已达约20万次，而去年同期仅有约7万次。百度2019年监测到的最大攻击峰值达793.84Gbps，2020年至今最大峰值为513.83Gbps。其中，在线教育、游戏、直播、云服务商等领域已成为DDoS攻击的主要目标。

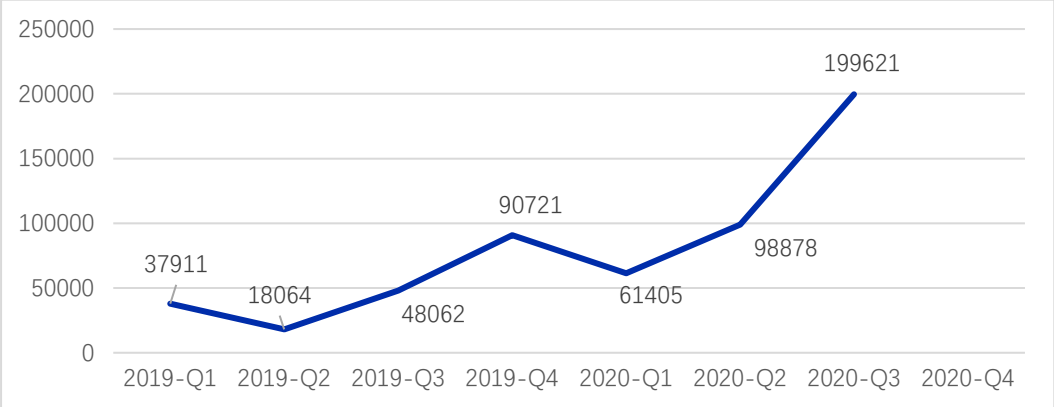

图 16 攻击事件趋势图

在攻击数量反弹的同时，DDoS攻击黑灰产在多个环节已逐渐标准化。发单人直接在“网页端DDoS攻击平台”下单，平台上包括用户注册、套餐付费、攻击发起等一系列操作，且在用户侧都可以完成，不需要其他人员参与。此外，DDoS攻击在分工上也由工具开发者向人员多维化发展，除发单人、担保商、黑客软件作者外，又增加了肉鸡商、接单人、资源提供者、接发单平台等多个维度。上述特征体现出DDoS攻击已经具备了SaaS化的趋势。

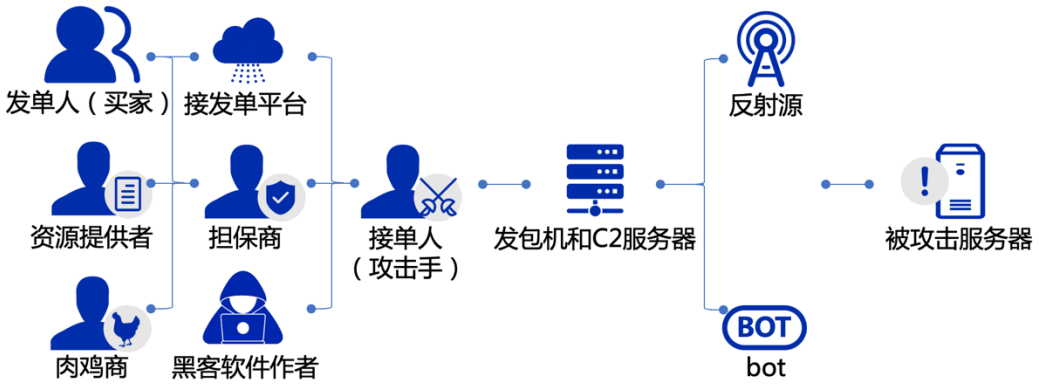

图 17 DDoS 攻击的分工

根据工信部数据，2017 年我国工业互联网直接产业规模为 5700 亿元，按每年 18%的复合增长率预计，工信部预计，2020 年我国工业互联网的直接产业规模有望突破 1 万亿规模。在自身向 SaaS 发展的同时，DDoS 的攻击目标也在发生变化，工业互联网、云平台已成为主要受害者。

目前，以云计算、人工智能、5G 技术等为代表的“新基建”产业迎来新机遇，未来这些领域随着云服务的普及或将成为 DDoS 攻击的重点目标。此外，疫情影响导致行业竞争的加剧，同业公司之间雇佣 DDoS 攻击的现象频发，而以赌博、淫秽色情等黑色产业之间的攻击尤甚。

3.2.3 黑灰产业态

当下，DDoS 黑灰产业态一般有以下三种：

（1）出售攻击软件和攻击流量

在网络上许多 DDoS 攻击工具可以直接免费下载。有特殊攻击需求的团伙可以从联系软件开发者定制特殊功能。软件开发者一般会根据攻击团伙的需求，开发定制化软件，并收取费用。一般数百元到千元不等。

除了攻击工具，发起 DDoS 攻击还需要具备一定的流量。攻击者会选择向流量平台商租用流量，流量供应商会把所掌握的流量管理权限有偿提供给攻击者实施网络攻击，一般按时按量收费。

（2）承接攻击业务

DDoS 黑灰产的高度成熟也催生出中介服务。最基础的模式是接单人员接到订单，再把订单分发给具备相应攻击资源和能力的攻击者。DDoS 攻击的报酬根据攻击难度、攻击时长、流量大小等要求的不同差异较大，从数百到数千元不等。中介则按比例从中抽成。

（3）敲诈勒索获利

在互联网上进行敲诈勒索，最常见的方式就是 DDoS 攻击。攻击者会把目标锁定在服务稳定性要求高、利润大的行业，如在线教育、游戏、金融、电商等。由于现在 DDoS 攻击成本越来越廉价，只需少量资金就可以租到一个规模庞大的僵尸网络，这直接导致 DDoS 攻击次数越来越高，逐年上升。

3.2.4 防治建议

业内防范DDoS攻击有如下4种主要的防御手段。

（1）持续更新系统。确保所有服务器采用最新系统，并打上安全补丁。计算机紧急响应协调中心发现，几乎每个受到DDoS攻击的系统都没有及时打上补丁。

（2）隐藏服务器IP。可以选择将所有的域名以及子域名都使用CDN来解析，这样可以隐藏服务器的真实IP，从而也不容易让服务器被DDOS攻击。不要把域名直接解析到服务器的真实IP地址，不能让服务器真实IP泄漏，服务器前端加CDN中转(免费的CDN一般能防止5G左右的DDoS)。

（3）实时监控，定期扫描。要定期扫描现有的网络主节点，清查可能存在的安全漏洞，对新出现的漏洞及时进行清理。

3.2.5 百度治理实践

百度对DDoS攻击的治理始终不遗余力。2018年初，百度安全智云盾便展开了针对网络协议漏洞进行DDoS攻击的“捕获行动”，截至目前已经发现了WS-DD、CoAP、ARMS、netAssistant服务和黑客自建反射源等5种新型DDoS攻击方式。2020年度前3季度分析出超过450W的威胁IP数据。

多年积累使百度拥有了成熟的实战经验，DDoS防护服务是百度安全面向用户推出的专业级DDoS防护服务。基于自主研发的天网防御系统，能有效防御各类攻击，包括（不限于）流量型、应用型、扫描窥探型、协议漏洞型、协议选项型等DDoS攻击（如SYN Flood、UDP Flood、DNS Query Flood、CC

等)。具备快速发现、区别牵引、有效缓解3个基础手段，针对被攻击的业务，结合风险及攻击持续情况，启用合适的防御资源进行清洗，挽回因网站或业务服务中断造成的诸多损失，确保源站稳定可靠。

得益于百度先进的DDoS攻击防御能力，百度安全智云盾团队在2020国庆前夕，有幸参加了公安部的护网行动，有效保障了国家各类网络资源的安全。

图 18 百度安全

3.3 Web 应用攻击

3.3.1 概念

Web应用攻击是指扫描探测器、WebShell上传与通信、跨站点请求伪造（CSRF)、SOL注入攻击、跨站脚本攻击（XSS攻击)、钓鱼网站等所有网络上存在的攻击合集，简称Web攻击。

3.3.2 现状及趋势

近年来，黑灰产对Web信息系统的攻击事件频发。不法分子利用Web系统的安全漏洞，实施网站篡改、数据窃取、执行指令、安装木马、传播病毒等破坏性行为，给企业安防造成了极大困难，威胁到企业自身的经济利益。

就目前的Web攻击种类而言，扫描器探测占比最大，是网络黑灰产常用的攻击手段，其次是WebShell上传与通信和SQL注入攻击。这三种应用攻击占全部Web应用攻击比例约77%。

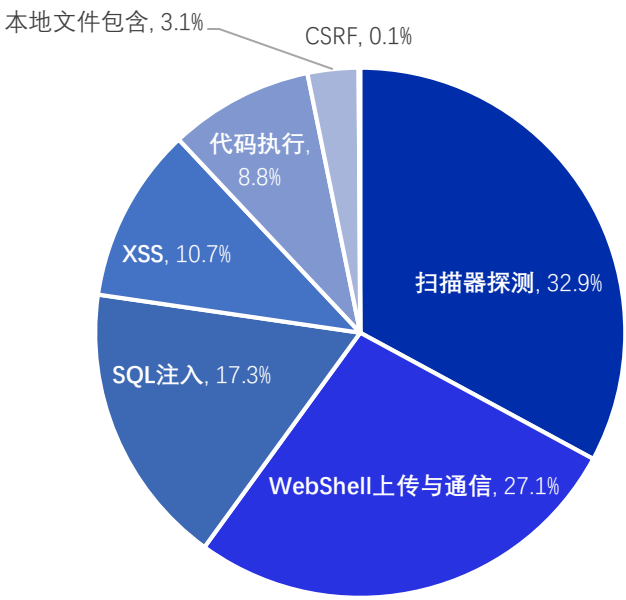

图 19 Web 攻击种类

从行业上看，互联网数据服务、新零售、互联网基础设施、互联网媒体服务、金融服务位列Top 5的受攻击行业。

3.3.3 黑灰产业态

随着大数据技术和流量产业的成熟，除了传统的网页和 APP，API 和小程序也作为新的流量入口迅速发展起来，Web 应用类型越发丰富，引发的数据泄露、流量作弊等网络犯罪也随之增加。

黑灰产通过攻击各种 Web 应用的漏洞获得大量信息，如个人隐私、商业机密、知识产权等。黑客在窃取这些信息后，会售卖给不法分子用于各种下游犯罪。

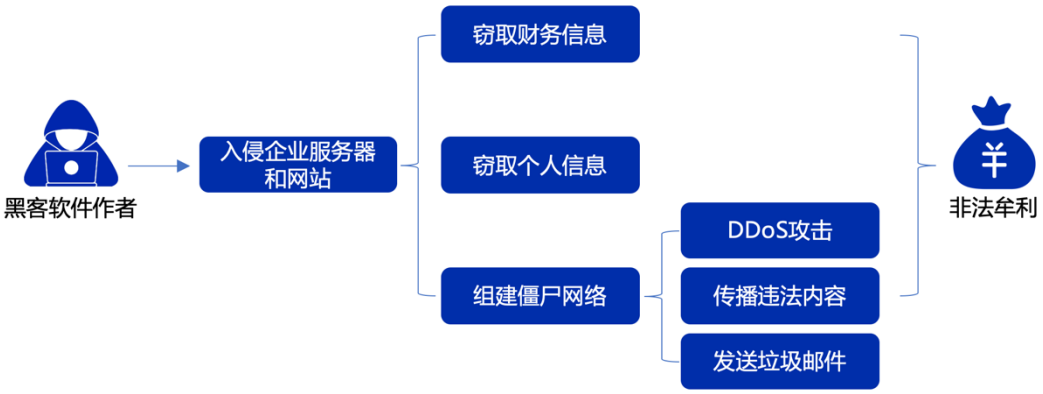

图 20 Web 应用攻击产业业态

3.3.4 危害及防治建议

企业遭受 Web 攻击，除对自身的安防系统和切身利益造成危害以外，黑灰产还会通过非法读取、篡改、删除数据库中的数据、盗取用户的各类敏感信息、通过修改数据库来修改网页上的内容、注入木马程序等手段来为帮助其他网络犯罪，成为黑灰产业链中重要的一环。

尽管 Web 攻击的种类繁多、表现形式也不一，但是他们的共性都是利用漏洞进行攻击。在日常的防控中，应重点提高以下三方面的能力：

（1）提高 Web 应用防火墙（WAF）安全等级和智能性，针对不同用户业务场景能够自动适应并调整防护策略。同时充分发挥云防火墙漏洞响应快、功能迭代快、处理快速的技术特点和优势，降低被攻击的风险。

（2）优化引擎解析 HTTP 协议能力，同时，敏感信息应使用 HTTPS 进行传输，确保安全性。

（3）多维度判断 IP 行为。随着黑产使用大规模代理 IP 池和秒拨 IP 等犯罪手段，传统的 IP 识别在抵御 Web 攻击已不再有效。通过使用多维度的 IP 身份识别与分析技术进行综合判断,能够有效提升 Web 攻击识别率，提高安防等级。

3.3.5 百度综合治理概述

百度“WEB 应用防火墙”由国内最顶级 Web 安全专家组成的技术团队，为不同行业、不同规模的网站提供云防护安全模式，彻底颠覆了过去单点部署 WAF 形式的被动防护，以网站替身的形式为网站拦截各种 SQL 注入、XSS 跨站、网站挂马、篡改、拖库等黑客攻击，并做到实时更新防护策略，第一时间防御各种 0day 漏洞，有效保护用户源站安全。

同时，为抵御 Web 应用攻击，百度安全云基于“全流量镜像技术”及“大数据处理技术”研发的"WEB 高级威胁检测系统",专注于识别 Web 应用攻击，能够深度挖掘黑客针对 Web 的拖库、远程命令执行、敏感文件泄露、Webshell 后门等攻击事件并发出准确的报警。该系统具有架构可横向扩展,报警准确，易于维护的特点，已被国内数十家企业用于日常的风控体系，助其实现自动化管理，节省安全运维成本。

3.4 涉物联网犯罪

3.4.1 概念

随着物联网发展和人工智能的应用技术的不断提高，犯罪分子攻破系统并窃取数据的渠道更多样化。其中，IoT 设备和应用会存有大量的个人数据、运营数据和企业数据，必须特别关注安全连接、设备强化、威胁监控和安全状况管理，以及保护云中后端数据的安全。

3.4.2 现状及趋势

物联网（IoT）的快速发展催生出了多种联网设备。2020 年全球活跃的物联网设备数量将达到 100 亿台，到 2025 年将达到 220 亿台。同时，物联网设备也将进一步智能化，甚至具备自己的意识。万物互联的背后是所有联网设备都可能存在安全漏洞，安全风险以及实际的攻击事件也随之增加。

目前，以智能摄像头、智能音箱、智能家居、智能售货机等为代表的 IoT 设备被黑灰产利用，已经成为网络犯罪的重要途径。监测数据显示，路由器、摄像头和智能电视是被攻击频率最高的三款 IoT 设备，占比分别为 45.47%、20.71%和 7.61%。未来，随着 5G 网络的发展，出现在人们身边的 IoT 还会更多，而 IoT 的安全问题也慢慢显露出来，黑灰产已经威胁到智能交通、无人驾驶等和人生命安全密切相关的场景。

3.4.3 黑灰产业态

目前，国内智能硬件的生产和研发都处于起步阶段，很多创业公司都参考国外标准的基础架构，然后快速实现产品使用流程、上线、众筹及发布，在整个阶段没有过多地考虑安全的问题，这给黑灰产造成了可乘之机。

IoT 攻击可以大致分为五类：欺骗、篡改、信息泄漏、拒绝服务和特权提升。

（1）欺骗类

黑灰产通过对IoT设备进行3种操作实施欺骗,即匿名操纵设备的状态、拦截或部分覆盖广播并欺骗发送方以及利用受限或具有特殊用途设备的漏洞。这些 IoT 设备通常具有密码或 PIN 码保护等通用的安全保护措施，或者依赖于网络共享密钥保护。当设备或网络的共享机密(PIN、密码、共享网络密钥)遭到泄漏时，攻击者可以控制设备或观察从设备发出的数据。

（2）篡改类

黑灰产篡改任何 IoT 设备，例如从利用电池放电漏洞或睡眠剥夺到通过冻结设备以减少熵来发起随机数生成器 (RNG) 攻击。如果非法程序可以使用密钥材料或持有密钥材料的加密设备，黑灰产通过部分或全部替换设备上运行的软件，以此让取而代之的软件运用设备的正版标识。

（3）信息泄漏类

黑灰产通过在未经授权的情况下窃听广播并获取信息，任意阻塞广播信号并拒绝信息分发；任意拦截或部分覆盖广播，并发送虚假信息。

（4）拒绝服务类

黑灰产通过控制大量的 IoT 设备发起 DDoS 攻击。

（5）特权提升类

执行特定功能的设备被黑灰产强制执行其他操作。例如，编程为半开放的阀门可能将受骗而完全开放。

3.4.4 危害及防治建议

攻击者一旦拥有 IoT 设备的控制权，就可以窃取数据、扰乱服务交付，或者利用计算机进行任何其他的网络犯罪。针对 IoT 基础设施的攻击会造成数据的泄露和操作的不可靠性，增加用户的个人隐私及信息泄露的风险。

现有 IoT 智能硬件安全防护技术大多集中于安全事件处理的某个阶段(例如事前预防、运行时监测阶段)，或仅针对具体问题(例如完整性验证、数据流异常检测),没有从全局视角对 IoT 智能硬件安全防护体系进行建模,缺乏涵盖智能硬件安全事件全过程的安全防护体系，并且 IoT 智能硬件自身的安防算力也存在不足。因此，未来的防治要针对 IoT 智能设备信息安全事件全生命周期过程的防护体系进行顶层设计。

3.4.5 百度综合治理概述

百度作为定位于人工智能行业的产业实践者，在对智能硬件攻击的防御方面，逐渐形成了自己的方法论，即施行两个维度保障和三个方向落地并举的顶层设计。

两个维度的保障，即研发上线保障、数据流通保障。三个方向落地，指安全方案落地、安全支持落地和安全标准落地。内在逻辑为安全方案、安全支持、安全标准均落地后，IoT 智能硬件和数据流通在设计、研发、测试和上线环节，均可有序展开、有章可循。

图 21 两个维度保障和三个方向落地

目前在小度和无人车中都已经应用上了百度云管端一体的安全解决方案，国内众多 IoT 厂商也不断与百度合作应用落地,如福特、长安、奇瑞、创维、康佳、暴风等。此外，百度在应对 IoT 黑灰产方面，对一些具体场景，比如音箱、摄像头等正在推行行业安全标准,逐一解决硬件和固件层面的威胁点，以期望未来基于 AI+IoT 的设备，上市之前都能够符合设备传输和 AI 的基础标准，从而提高设备的安全性，降低被攻击的可能。

4 暗网

4.1. 暗网的概念

普通网民日常通过百度等搜索引擎访问到的网络被称之为表层网络，即“明网”。暗网是指那些存储在分布于全球各个角落的服务器中、但不能通过超链接访问而需要通过特殊技术访问的资源。

图 22 暗网

4.2 现状及趋势

上世纪90年代，美国海军研究实验室（NRL）发起了一个关于情报传递的科研项目，这就是著名的“洋葱协议”（简称Tor）项目。目的是为了保护通讯网络安全、在网络中提供隐藏身份服务、避免被敌军跟踪信号，最早的暗网就此诞生。

项目后由一个 NGO 组织接管并完成了军转民，暗网由此得到迅猛发展。根据研究报告，如今暗网与整个明网相比，不管是信息量、访问量还是用户数量都不是一个数量级的。2014 年有报道披露每年有近 5000 万人次下载 Tor。

截至目前，关于暗网的站点数量并没有太精确的数量统计。2016 年，有媒体披露，当时暗网中的站点约 3 万个，并且大部分网站都是以英文做为其通用语言（约占 76%），接下来是德国(约占 4%)，中文(约占 3.7%)，而剩下的为其他国家语言网站。按此比例计算，2016 年中文的暗网站点就多达 1100 多个。2019 年，威胁情报公司 Recorded Future 试图通过匿名浏览器 Tor 映射.onion 网站的数

量，发现了 55428 个不同的 onion 域，较 2016 年几乎翻倍。

目前，我们监测到的暗网中文站点全部都是非法交易网站，而且从趋势特点看，暗网中文网站的交易近年来日趋活跃。我们研究发现，暗网中某些中文站点利用明网中知名品牌蹭热度。比如下图中的“暗网某宝网”，不但名称上、交易模式上都模仿明网中的某宝网，而且上面的非法交易的浏览量也很惊人。

图 23 暗网中的企业内部敏感数据交易

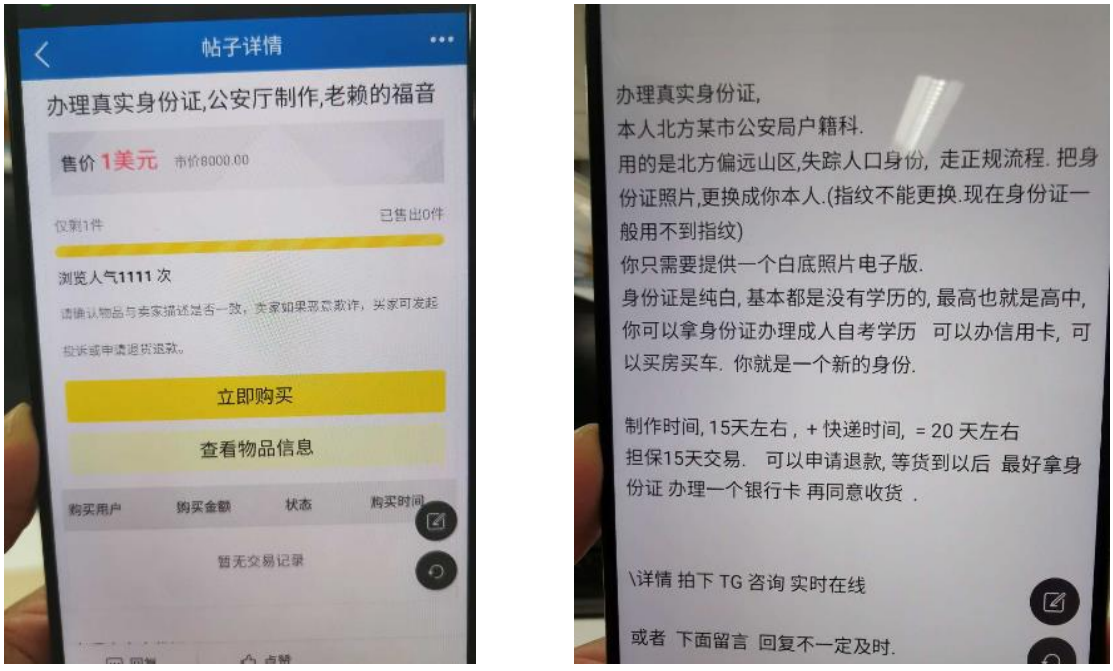

图 24 暗网中提供非法服务的交易

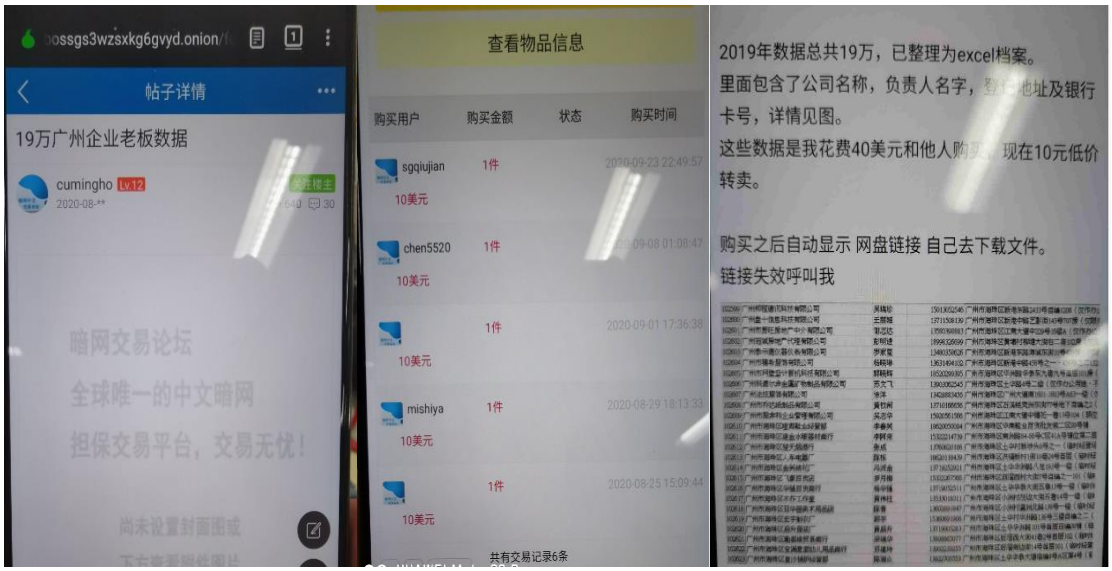

图 25 暗网中的个人隐私信息交易

黑灰产从业者近年来也有从明网转移到暗网的趋势，但这些黑灰产从业者也并非能在暗网中做到绝对隐蔽，其所使用的注册名称、昵称等信息都可能连带出其在明网中的蛛丝马迹。

4.3 黑灰产业态

暗网并不一定是直接犯罪，而是黑灰产寄生的平台。暗网中存在成百上千的交易论坛，承载了大量的非法信息。黑灰产生态在暗网与明网中的呈现形式、接洽过程、支付手段等方面有比较显著的差别。

序号	特点	明网	暗网
1	呈现形式	黑灰产隐匿在正常信息中，描述多用黑话、变体、谐音等方式掩饰，外行难以发现和理解。	整个论坛全部被黑灰产充斥，黑灰产公开的呈现。并按性质进行目录编排，方便访问者查找，部分站点针对一级目录还细分二级目录。描述均为通俗易懂并且具有诱惑性、教唆性的语言，可以轻易理解。
2	平台责任	由于黑灰产交易的非法性，网站运营者不介入双方交易，并且还有配合行政司法力量进行打黑的义务。	一般都免费注册，之后激活、留言、私聊等每一步进展都须先支付比特币给站点后方可进行。部分站点介入双方交易，接受投诉，保障交易、服务质量。
3	接洽	私下通过QQ或微信等社交工具转移阵地。	须充值比特币方可在网站中进行私聊。一般交易双方均不愿转移到社交工具上沟通。
4	支付方式	正常的支付方式均可交易，如网银、手机银行、第三方支付平台、第四方支付平台等。	仅通过比特币交易。
5	集中度	处于人找黑灰产的离散分布状态。 黑灰产分散在各个专业论坛、社交平台。	处于黑灰产找人的集中聚合状态。 一个交易网站可以集中全部黑灰产。

表 1 明网和暗网的区别

4.4 危害及防治建议

4.4.1 暗网的危害

卢森堡大学亚历克斯·比尤科夫(Alex Biryukov)教授的研究团队分析了 3050 个暗网站点，发现暗网上的毒品、色情、军火武器和伪造品犯罪相关

的内容约占 44%，服务类内容占 4%。暗网中一半内容充斥着违法犯罪交易，主要有以下几类危害。

（1）诈骗

暗网的特性吸引着各色人员不断涌入。其中，有大量诈骗分子利用匿名、不可追溯、交易不受法律保护等有利条件，以出售违禁品为诱饵实施诈骗。

（2）非法交易

暗网是非法交易的集中地，不乏隐私交易（如重点中学家长信息、开房记录）、犯罪方法交易（如黑 SEO、恶意点击、网络诈骗方法、各类薅羊毛方法）、非法服务交易（如监狱捞人、公职晋升）等。这些黑产在明网中均隐藏在正常信息中，描述多用黑话、变体、谐音等方式掩饰，外行难以发现和理解。但在暗网中，都被编排在暗网交易论坛的子目录中，组织有序、查阅非常便利，描述均为通俗易懂并且具有诱惑性、教唆性的语言，可以轻易理解。

（3）传统犯罪

传统犯罪在暗网中也占据了相当的比重。如贩卖军火武器、妇女儿童、人体器官、毒品，雇凶杀人以及恶意造谣颠覆政权等。

4.4.2 暗网的防治

（1）加强对“引诱者”的打击监管

为谋取非法利益，国内社交网络逐渐出现了一批介绍引诱普通网民进入暗网的教唆分子。这些不法分子属于比较早的进入暗网浏览者，并且掌握一些互联网翻墙技能和特殊软件。通过在国内社交网络公布一些暗网的截图来吸引广大网民，招募网民并传授进入暗网的方法，靠出售进入暗网所需方法、VPN 软件牟利或实施诈骗。此行为触犯了《中华人民共和国网络安全法》和《电信业务经营许可管理办法》规定，属于违法行为，情节严重的应按照《中华人民共和国刑法》的有关规定追究其刑事责任。因此，加大对教唆传授他人进入暗网分子的打击，可以有效的卡住进入暗网的源头。

此外，多数自制 VPN 也带有木马病毒等危害终端设备的风险（例如被控成为肉鸡、被盗取个人隐私等）。加强上网行为的政策宣传导向，降低个人的 VPN 使用率不仅有利于维护网民的通信安全，也能够降低暗网中的犯罪率。

（2）提升对暗网犯罪侦察的技术能力

目前，通过技术力量直接侦查到暗网中犯罪嫌疑人身份的难度较大，突破的关键仍为线索的积累和挖掘。提高涉暗网案件的破案率还需要进一步提升技术侦查能力。

在这方面，可以借鉴其他国家的一些做法。2015 年美国国防部发布了一款暗网搜索引擎，它可以深度“发现”谷歌等常规搜索引擎检索不到的信息，最初被用来监测暗网上的人口贩卖信息，后来又逐步用于监测其他犯罪活动。美国联邦调查局还使用网络检测工具“NIT”成功破解了“洋葱路由”的加密机制，可以一次性检索到 1300 个暗网 IP 地址，进而查找到所有使用这些地址的用户信息。

（3）加强国际合作

根据 2020 年卢森堡大学亚历克斯比尤科夫教授的研究成果，暗网站点中使用的语言多达 17 种，这说明暗网用户已呈现全球化态势。在取缔世界最大的暗网市场阿尔法湾犯罪团伙行动中，共有来自美国、荷兰、泰国、加拿大、英国、法国等国的数十个政府监管部门参与，这也是有史以来规模最大的国际网络犯罪打击行动。

暗网的服务器大多在境外，对国外服务器进行取证往往成为打击暗网犯罪的关键所在。如能达成国际合作协议，对于完成暗网犯罪的域外取证无疑具有十分重要的意义。

三、未来趋势预测

世界经济论坛（WEF）在《2020 全球风险报告》中指出，预计至2021 年，网络黑灰产的市场效益将比肩世界第三大经济体，网络犯罪将会是未来十年全球最引入注目的风险之一。网络黑灰产的多元化发展趋势，不仅破坏了互联网生态秩序，而且对人民的生活秩序和社会经济发展都带来了极大挑战。

1 细分领域自动化程度不断提高

随着各种配套的不断完善，网络黑灰产从业门槛也在不断降低。以接码平台、秒拨平台、跑分平台、售卖账号的发卡平台、专门用于违法内容推广的广告联盟等各类专业黑灰产平台不断产生和发展，拉低了网络犯罪的门槛和成本，加速了网络犯罪的蔓延趋势。任何人都可以从上游获取所需的物料，并借助自动化工具进行恶意注册、薅羊毛、恶意点击等网络犯罪，给网络平台的防范与打击造成了一定困难。未来，互联网黑灰产与网络新型犯罪发展呈现出的螺旋式伴生发展趋势将更加明显，两者衔接将更为紧密，互联网产业与黑灰产之间的技术对抗将更加激烈。

2 攻击对象向物联网和云平台迁移

疫情期间，为了保障社会正常运转、维持经济稳定，各行各业都出现了业务上云的趋势。云平台也随之成为网络黑灰产攻击的重点目标。漏洞利用、拒绝服务、暴力破解等网络攻击严重威胁企业云业务的安全。这种新型的云端攻击和云端黑产，极易引发数据泄露、API 安全漏洞、DDoS 攻击等网络犯罪行为。未来，加强云安全和云防护等级，也将是企业发展的核心问题之一。

现阶段，大量物联网设备应用在工业领域，涉及自动驾驶、智能网关、摄像头、门禁、打印机等多种设备类型。物联网设备接入方式灵活、分布位置广泛的特点增加了设备的安全隐患，也给网络黑灰产带来了可乘之机。同时，因物联网传统安防手段存在一定漏洞以及网络黑灰产攻击形式的技术升级，未来在物联网领域的攻防战，将以深度学习、大数据挖掘和推荐算法等人工智能安全技术手段为核心。

3 黑灰产犯罪进入 AI 时代

随着人工智能技术的发展和应用普及，黑灰产也借助人工智能技术，利用深度学习等手段不断升级其犯罪方式，扩展其犯罪领域，已经出现人脸仿造、AI 换脸、AI 机器人拨打诈骗电话等借助人工智能技术实施的新型网络犯罪活动。未来，随着人工智能商业化和应用种类的增加，AI 安全将成为各行各业不容忽视的关键问题。

四、打击防治建议

近年来黑灰产技术手段越来越高，形式也越来越多样化，并且还存在向云端转移的趋势。日趋链条化、逐利化、生态化的网络黑灰产，损害了广大互联网用户的利益，恶化了网络空间的内容生态，已成为危害公民权益和数字经济发展的毒瘤，依法严厉打击网络黑灰产势在必行。

为了维护网络清朗空间，保护公众合法权益，网络平台应当切实担起社会责任。同时，网络黑灰产治理是一项复杂的系统工程，不可能毕其功于一役，亦不能由某一家或某几家网络平台承担，而是需要主管部门、企业、社会组织及公众各司其责，共同参与。随着网络的发展，互联网平台与黑灰产之间的对抗也将随之加强，道魔之战也会更为激烈。

1 部门联动，司法与行政联手打击黑灰产生态

对于网络黑灰产的打击，不应仅局限在单个案件的打击，而是以打击整条黑灰色产业链及其生存土壤为目的，彻底摧毁黑灰产生态。常见的网络黑生态具有产业链利益关系复杂，发展迅速、犯罪跨平台、跨地域且资金流向分散、打击工作存证取证难等特点，单纯的司法打击难以起到根治效果。

与刑事司法的滞后不同，行政执法在应对黑灰产的灵活性和模糊地带方面有其明显的优势。因此，在不断加强刑事执法打击的同时，需要更加灵活地运用行政法规开展行业和生态治理。只有制定和完善相关法律，明确违法行为的界限，才可以使网络行为有法可依，使网络黑灰产无处遁形，从而真正做到源头治理，维护网络社会秩序。

2 共治共享，政府与企业共同应对黑灰产挑战

打击网络黑灰产不能各自为政，多方协作才能有合力效应。在主要由政府职能部门（监管执法部门）、互联网平台、网络安全技术企业三方组成的网络生态治理体系中，互联网平台应充分发挥自身优势，可以将大数据分析、人工智能、机器学习等新技术运用于安全体系，力求对安全事件做到事前侦知预警、事中察知阻断和事后溯源修复，提高对网络黑灰产的威慑力和杀伤力。同时，为支持互联网平台打击网络黑灰产，有关部门应当从监管执法、立法司法等角度，赋予互联网平台相关监管职责和治理主体地位，激发平台更大治理潜能动能，包括让平台在对商户、用户等主体的监管上更有自主性，对信息数据控制和网络安全维护承担更多职责。职能部门对平台应实施包容审慎监管，在数据信息共享、信用互通、职能协调等方面与平台深度合作，推动政府、平台、企业商户、用户形成合力，构建依法打击网络黑灰产最有力链条，营造安全有序、风清气正的良好网络生态。

3 群策群力，面向青少年强化黑灰产宣传教育

防治防范网络黑灰产离不开人民群众的理解与支持。中青年和青少年即是网络黑灰产犯罪的主要受害者也是主要参与者。政府与企业需要共同加强对社会各界人士、广大网民群体和青少年群体关于网络黑灰产和违法犯罪的宣传教育，使其充分了解网络黑灰产的社会危害性，及时掌握网络犯罪最新作案手法，维护人民群众的切身利益。在谨防自身上当受骗的同时，坚决做到抵制网络违法内容、坚决做到不为网络黑灰产提供帮助。只有人人都具备了反黑灰产意识，才可能形成群防群控机制，将网络黑灰产扼杀在萌芽状态。

百家号

微信公众号