上海法治报
www.shfzb.com.cn

网络“黑产链”犯罪的发展演化及刑法应对

□陈萍 曹艳梅

在大数据时代，利用互联网进行犯罪活动的网络黑色产业链（下文简称“黑产链”）日益猖獗，严重威胁国家网络安全、公民个人信息和财产的安全。网络“黑产链”犯罪对现行刑法理论和实践提出一定挑战，刑法应当如何回应才能有效规制此类行为，成为亟待解决的问题。

网络“黑产链”犯罪的类型透析

产业链是产业经济学中的一个概念，指各个产业部门之间基于一定的技术经济联系，而表现出的环环相扣的关联关系的形象描述。网络“黑产链”，也就是以盈利为目的、利用信息网络进行有组织、分工明确的犯罪活动的经济链。网络“黑产链”中的犯罪行为类型上具有多元性，对这些犯罪的类型进行细致区分，深入研究这些犯罪的属性和规律，有利于树立正确的刑法理念与应对策略。

从产业环节角度而言，产业链中大量存在着上下游关系和相互价值的交换，上游环节向下游环节输送产品或服务，下游环节向上游环节反馈信息。网络“黑产链”也可以区分为上游犯罪、中游犯罪和下游犯罪。上游犯罪主要由黑客技术实施者完成，他们基本具有较高的技术水平，是网络“黑产链”的基础环节，他们负责病毒制作、木马开发、代理，网站攻击，制作钓鱼网站，盗取用户数据库等；中游犯罪主要由团伙人员共同实施，由同一上游衍生出的中游犯罪团伙往往个数较多，而且可以进行层级细分，是“黑产链”的关键环节，中游团伙利用从上游购买的技术或信息实施具体的盗窃、诈骗、敲诈勒索等犯罪行为；下游犯罪则由中游犯罪团伙的周边组织负责进行，通过洗钱、销赃等行为，帮助中游团伙将其犯罪资产“变现”。

从犯罪手段角度来看，主要可以分为技术类犯罪、社会工程类犯罪和涉黄涉非类犯罪。技术类犯罪指利用网络和计算机存在的安全漏洞和缺陷，通过SQL注入、网络钓鱼、XSS（跨站脚本攻击）等方式侵入各种门户网站窃取数据和信息，并对网络、计算机及其他移动终端发起的各类攻击犯罪行为。社会工程类犯罪指通过QQ群、YY群等组织成百上千、甚至几万人的大规模团伙，利用受害者的信任、好奇心和贪婪等心理弱点，以冒充熟人或博取同情等社会工程学攻击方式进行网络盗窃、诈骗和敲诈勒索等犯罪。涉黄涉非类犯罪指利用网络的便捷性和难以追查性，使用大量C&C（命令与控制）架构控制“肉鸡”（被植入木马病毒的僵尸主机），构建起庞大的僵尸网络，进行如网络色情、网络赌博、贩卖枪支弹药和违禁品等的涉黄涉非违法犯罪活动。

“互联网+”引领了互联网产业发展的新方向，同时也为网络犯罪提供了可乘之机。从提供黑客技术“作案”工具，到信息数据的模式经销，再到“肉鸡”的精准定位，网络“黑产链”产业链上的每一环都有不同的牟利方式，组织严密规范、经济“效益”巨大，“互联网+”与犯罪组织的融合已经颇具规模，并在以越来越快的速度发展、膨胀，形成了高达数千亿元的产业链条。

网络“黑产链”犯罪的发展趋势

不断进化的“黑产链”正在像癌症一样，威胁着日渐勃兴的互联网世界。根据“We Are Social”和“Hootsuite”披露的最新数据，全球互联网用户数已经突破了40亿大关，证实全球有一半的人口“触网”。2018年，我国净增移动电话用户达到1.49亿户，总数达到15.7亿户，移动电话用户普及率达到112.2部/百人。然而，互联网的快速普及加大了网络犯罪分子的活动空间，网络犯罪的组织越来越多，手段越来越多，危害越来越大。


资料照片

一是技术门槛降低，黑客低龄化。由于各种病毒制作工具、黑客软件、黑客教程的泛滥，自动化程度越来越高，黑客群体的技术准入门槛变得越来越低。随着计算机技术的普及与制作工具的增多，入行者已呈现低龄化趋势，10到30岁的从业者占了非常高的比例。由于社会不同群体对黑客有着不同的理解，使得许多青少年对计算机产生兴趣后发现编写病毒、攻击网站，容易获得他人崇拜，最初出于炫耀目的而学习技术，逐步在网络游戏中偷取账号和设备，从“小打小闹”最终蜕化成“玩家大侠”。从炫耀技术的“行为艺术”到庞大产业链中的一环，黑客们具有明显的“趋利动机”。在整个产业链中掌握编程技术的病毒制造者只是少数人。丰厚的非法利润、较低的技术需求，吸引了大批人生观、价值观尚未稳定成型的中学生、大学生加入到产业链中。

二是跨行业跨平台，集团式运作。网络“黑产链”犯罪团伙已经发展为跨平台、跨行业的集团式经营运作，成为移动互联网时代的毒瘤。据不完全统计，目前中国网络黑色产业链的“从业者”已经超过了40万人，依托其进行网络诈骗产业的从业人数至少有160万人，“年产值”超过1100亿元。网络“黑产链”已经从过去的黑客攻击模式转化成为犯罪分子的敛财工具和商业竞争手段，呈现出明显的集团化趋势。通过盗取多个网站数据库，获取网民个人信息和银行卡资料，“拖库”“撞库”已成为“黑产链”人员的惯用招数。他们分工明确，工作领域互不交叉，互不实际接触，也互不知道对方的真实身份，却充分利用互联网多地合作进行犯罪活动。从暗扣话费、广告流量变现、手机应用分发，到木马刷量、勒索病毒、控制肉鸡挖矿，他们传递情报，相互配合，商讨犯罪手段和方法，提高作案能力，并利诱、教唆他人实施共同犯罪以非法牟取利益，导致网络犯罪的危害性更大、危险性更严重，类型和数量也越来越多。

三是活动由暗到明，手段公开化。网络病毒出现已有20多年的时间，已从最初炫耀技术的游戏演变成了犯罪工具，被用来偷盗网络账户、商业信息，甚至成为勒索的工具。近年来，网络犯罪所利用的“核心”已不只是病毒及木马，还包括利用程序漏洞、利用程序的保护机制进行的恶意攻击等技术及手段，从“暗偷”转变为“明抢”。目前很多网站已经公开进行木马交易。在网上，“木马”已成为公司化运作的产业，“木马”产品在网上以文字、贴图等形式公开进行广告，宣传自己诚信为本、服务周到，甚至定期会有打折促销活动，还有一些工作室推出客户专属定制服务，依据购买木马人员的需求，为其定做特定的木马。就连某知名网站上也公然进行病毒买卖，这种嚣张态势让人瞠目、震惊。近年来，黑客针对医药行业和游戏行业，尤其是走上信息化道路但自身防范力量比较弱的中小企业网站，实施病毒攻击，一些地方甚至形成了只有交“保护费”才能免遭病毒攻击尴尬的局面。国内某著名的网络游戏公司遭到长达10天的网络攻击，服务器全面瘫痪，其经营的网络游戏被迫停止，损失高达3460万元人民币。

在网络空间中，技术通过延伸人的交往、活动空间来直接改变人的社会属性。因此，伴随人类社会与人类行动向网络空间中的延续，人类社会的法律规则必然要延伸到网络空间之中。面对网络“黑产链”的犯罪活动，现实生活中的刑法规则更应如影随形。

网络“黑产链”犯罪的刑法应对

《2018年全球风险报告》中，网络安全被认为是除自然灾害以外，最大的风险。为遏制网络不法行为，全球网络安全成本已占到互联网建设总投资的15%。3月19日，公安部通报开展“净网2018”专项行动成果。行动期间，全国各级警方侦破网络犯罪案件57519起，抓获犯罪嫌疑人83668名。信息时代和大数据背景下，网络犯罪“异军突起”，确立信息网络时代网络犯罪评价的刑法规则，凸显其必要性和迫切性，刑法必须承担起全面维护网络安全和制裁网络犯罪的时代使命。网络技术日新月异，给刑事立法与刑事司法不断提出新的时代难题，需要及时进行审慎回应。

一方面，网络“黑产链”犯罪的惩治体系完善。网络因素的介入一定程度上，使得犯罪的构成要件要素（具体包括犯罪对象、犯罪行为、犯罪目的和犯罪结果等）、社会危害性和犯罪形态发生一些变异。面对网络空间中传统犯罪的变异态势，将部分预备行为提升、独立化为实行行为，将部分共犯行为加以正犯化，成为刑事立法无法回避的关键选择。伴随网络犯罪的日渐变异，我国网络犯罪罪名体系逐渐精细化和严密化，从1997年刑法“两点一面”式立法到《刑法修正案（九）》，经历多次转型和罪名扩充，尤其是《刑法修正案（九）》针对网络犯罪新增罪名、扩充罪状、降低入罪门槛、提升法定刑配置和增加单位犯罪主体，逐渐形成较为完整的网络犯罪罪名体系。

从产业分工的罪名设置角度而言，网络“黑产链”虽然已成规模，但从刑法视角来看，通常上中下游行为人之间的联系不足以构成共同犯罪，应当按照各自行为分别定罪量刑。上游犯罪人多涉及的罪名包括提供侵入、非法控制计算机信息系统的程序、工具罪，破坏计算机信息系统罪，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，侵犯公民个人信息罪等。对中游犯罪人按照其所实施的具体犯罪定罪，常见的罪名有盗窃罪、诈骗罪、敲诈勒索罪等；下游犯罪人可能涉及的常见罪名包括掩饰、隐瞒犯罪所得、犯罪所得收益罪，伪造、变造买卖身份证件罪等。不得不承认，现有立法中上游犯罪人容易触犯的罪名多为最高刑在三年有期徒刑以下的轻罪，这可能导致在量刑上过轻，使得上游犯罪人的行为造成的损害与其所受到的刑罚不相适应。

从网络犯罪的社会危害角度而言，目前刑法已经逐渐强化网络犯罪治理的空间思维，惩治重点转为以网络为工具和以网络为平台的犯罪，但仍多采取以手段行为为主的兜底式入罪立法方式。习近平总书记曾明确指出“没有网络安全，就没有国家安全”。随着信息网络应用的广泛与普及，网络犯罪的社会危害性将最终突破信息数据安全、网络金融安全的局限，越来越具有危害公共安全的性质。随着信息时代网络空间中新型法益的不断形成，现实已经开始要求刑法分则罪名体系再次进行调整以适应新的犯罪情势的需要。适时修改完善惩治网络犯罪的法律规定，形成惩治网络犯罪的高压态势，是网络时代刑法应对的题中之义。具体来说，需要将网络犯罪的部分罪种由妨害社会管理秩序罪的犯罪调整至危害公共安全罪的犯罪集群，或者在危害公共安全罪中专设有关网络犯罪的独立罪种。

另一方面，网络“黑产链”犯罪的预防体系更新。徒法不足以自治，惩治亦只是预防的一种终极方式，而且绝非最有效、最经济的方式。鉴于网络“黑产链”具有虚拟性、技术性、跨国性等特点，很容易成为刑事执法的痛点，甚至是盲区。因此，对网络“黑产链”的治理仍应当秉持“惩防结合、预防为主”的刑事理念。通过努力构建连接警方、金融机构、电子商务、运营商和安全厂商等多方平台的网络“安全产业链”，畅通协调机制，优化资源共享，从生产、销赃、获利的各个主要环节的源头和终端管理入手，多管齐下，共同治理，才能有效对抗网络“黑产链”，共同构建“网络安全共同体”。

从监管部门角度而言，公安机关网监、刑侦、经侦等部门要加强内部的技术、线索、警力等方面的协作配合，建成集发现、控制、侦查、打击、防范、管理于一体的网上技术体系，提高网上整体作战能力。要充分运用人工智能、大数据分析、人脸识别等新科技对活跃恶意网址和移动互联网应用，将网络威胁进行监测预警和分析处置，完善“依网管网、依网治网”的能力。

从社会协作角度而言，要加强相关管理部门、企业单位之间的信息共享和打防协作，如加强国务院信息化办公室、公安部、工信部、中科院等机构的有关部门，以及国家计算机网络应急技术中心、中国互联网协会网络与信息安全工作委员会和一些网络安全产品生产厂商等不同部门的协同作战；成立专门机构，收集相关数据，揭示网络“黑产链”的危害，扩大打击行为的社会影响力，研发应对网络病毒黑色产业链攻击的安全产品；加强网络法制宣传，通过政府网站设立网上咨询平台，为广大网络使用者提供在线法治教育服务，不断增强广大网民的法律意识和守法自觉性。

（作者单位：上海立信会计金融学院法学院；上海市黄浦区人民检察院）