暗网犯罪刑事治理研究

谢 玲

[摘 要] 近年来,受Tor软件服务、加密数字货币支付、Tumbler和PGP软件技术支持,网络犯罪出现了由可见表网向隐秘暗网空间转移的趋势,并形成较为固定的常见高发暗网犯罪类型,一些新型暗网犯罪也在加密空间中寻求生存空间。面对通信匿名和交易加密的暗网犯罪为犯罪防控带来的全新挑战,须从实案角度厘清暗网犯罪常见高发类型与新兴类型的发生机制、发展动向、调查难点和司法施用障碍,从侦查方法和刑法适用角度提出解决思路与应对策略,同时加强网络安全技术攻防、互联网信息源头管控、涉网犯罪国际刑事司法合作、虚拟数字货币金融管制等多领域多维度综合性措施,为国家打击、治理暗网犯罪的立法与实践提供参考。

[关键词] 暗网;网络犯罪;匿名特性;Tor浏览器;加密数字货币;刑事犯罪

[作者简介] 谢玲,西南政法大学刑事侦查学院讲师,博士后,重庆 401120

[中图分类号] D914;G203 [文献标识码] A [文章编号] 1004-4434(2020)05-0013-12
DOI:10.16524/j.45-1002.2020.05.002

一、网络空间分层视域下的犯罪问题

互联网向全球用户展开的是一个巨大的、无限传送的信息、数字和符号的世界。近年来,随着人们对互联网世界认知的加深,犯罪人也与之产生了更多的新的接触方式,对于新型网络犯罪的研究和讨论开始从可见的网络区段向隐秘的网络深层延展。如果对网络空间进行分层,可以按照访问的自由限度分为表网、深网及暗网三层。在这三层网络空间中承载着相应的网络犯罪现象,呈现出各自的发生特点。

(一)表网、深网及暗网空间环境下的网络犯罪

第一层网络空间称为“表网”(Clearnet),又称“可见网络”。它是指已经被编入索引,利用百度、谷歌、雅虎等互联网标准搜索引擎和网络浏览器能够直接访问的页面和内容,主要以通过超链接方式关联起来的网页构成,是人们日常上网普遍接触的网络层次,也是所有类型的网络犯罪主要发生的传统领域。

第二层网络空间称为“深网”(Deepnet),是指托管在互联网开放部分但因其具有内容访问限制而未被搜索引擎索引和收录,无法通过超链接访问的网页、站点。例如公司内部使用的网站、网上银行个人账户、大学和研究机构的数据库和图书馆目录就属于深网的范畴[1]。深网必须借助于动态网页技术等特殊手段才能获得访问。有研究根据全球图书馆数据生成、拷贝和使用的储量进行估算,认为深网的规模约为可见网络的400倍[2]。由于深网建立和存储了企事业单位人员基本信息、客户信息等内部管理和相关业务数据库,因而成为电信网络诈骗的上游犯罪、公民个人信息盗窃灰色产业链的网络空间之一。例如,实案中聘请的网络安全维护人员在为单位提供网络安全服务期间故意将单位数据库回流至个人电脑、窃取重要信息并对外出售;单位网络管理人员滥用后台权限、非法获取数据库信息并贩卖给他人以谋取非法利益;黑客以技术手段突破网络安全管理防火墙、攻击数据库代码漏洞以窃取数据、信息。由于犯罪人使用表网买卖上述非法获取的公民个人信息,存在被举报、监控和刑事追诉的可能性,为降低被查处风险,当前大量非法信息的网上交易已转入更深层的暗网空间进行。

[基金项目] 重庆市教委科学技术研究计划项目“电信网络诈骗犯罪资讯调查研究”(KJQN202000311);西南政法大学生物安全风险防控和治理体系建设专项研究课题“城市生物恐怖袭击AHP潜在攻击风险模型及防控策略研究”(JS-ZTG-JAQG-005)

第三层网络空间称为“暗网”(darknet)。暗网被认为是由深网延续的一部分特殊加密子集,是指利用多级加密网络提供的匿名通信构建的网络平台,其加密性和匿名性特征决定了它不被互联网标准搜索引擎收录、查询,并能保护所有通信用户的IP地址、通信内容、通信过程免受监视和流量分析。当前所发现的暗网虽只占互联网的0.1%,但由于暗网为用户提供的匿名、匿踪保护,使其成为网络犯罪人在数字信息世界中的“避风港”,暗网中充满了创建者和使用者故意隐藏的内容,存在大量的非法和反社会信息。

(二)网络犯罪的最新迁移趋势及发生原因

依据犯罪现象发生和存续的空间领域,可以将网络犯罪分为表网犯罪、深网犯罪和暗网犯罪。从寄生于第一层表网空间的传统型网络犯罪发展到隐藏于第三层暗网空间的新型网络犯罪,体现了一种空间形态犯罪迁移的趋势,这意味着传统犯罪赖以生存的外界情势发生深刻变化从而导致犯罪发生空间条件的转移。2013年是证明网络犯罪发生迁移的一个重要标志性时间节点。多年来,暗网的存在并未引起执法部门和社会大众的注意,大多数人熟悉并使用的是表网的站点、社区和平台。2013年10月,美国联邦调查局关闭了第一个暗网毒品市场“丝绸之路”(Silk Road),逮捕了网站运营者罗斯·威廉·乌布利希,自此暗网才正式进入全球公众视野。“丝绸之路”在短短两年的运行中,从事毒品、计算机黑客服务、非法金融、假币贩卖和恐怖分子通联,赚取了超过12亿美元的比特币。从“丝绸之路”的“经营范围”可以看出,除了“丝绸之路”内部明确禁止的武器交易、儿童色情和人体器官交易,其他重要类型的网络犯罪形式都能在该暗网站点中得以实现,只是网络犯罪现象从一个空间向另一个空间发生了转移,犯罪人在表网中从事的网络犯罪行为均能在暗网环境中得到对应。

网络犯罪场域发生空间转换,一方面来自于表网空间强大的执法压力,表网犯罪执法活动包括常规措施与专项行动的开展,如近年来铺开的系列“净网行动”、打击境外电信网络诈骗犯罪的“长城行动”,对网络犯罪的表网生存空间形成了强烈挤压,以致不法行为受到压制的犯罪人更倾向于在新的犯罪生态系统中活动;另一方面是寻找到暗网这一更适宜犯罪的存续和增长的新的网络空间。暗网的隐秘和匿名化特征有别于表网,能够促进犯罪人犯罪目的的实现,同时最大限度地减少被发现和被追诉的危险,并且这一特征“优势”所造成的刑事犯罪调查大面积受阻的结果不断被负强化,形成了对于网络犯罪人同时使用具有通信和交易隐藏功能的Tor系统与比特币等加密数字货币的不良示范和“引导”,适宜于暗网环境下使用的犯罪技术、手段由此衍生出新的形式。这将导致深网衍生出的暗网空间犯罪在未来呈指数级增长。

二、暗网匿名特性对网络犯罪的支持作用

暗网的在线匿名性和隐秘交易是将传统的互联网犯罪人带入暗网从事犯罪活动的最重要因素,也是网络犯罪由表网向暗网转型的关键。利用Tor软件服务将用户的IP地址模糊化以逃避流量分析,使用加密数字货币支付系统与Tumbler技术处理非法交易,采取PGP软件加密信息是暗网中用来隐藏犯罪人活动,保证用户匿名性的主要技术方法。上述技术主要通过设定暗网配置模式、浏览者进入途径、数据传输规则与买卖双方交易方式的内容和程序来实现。

(一)以Tor软件服务隐藏用户身份

与通过联网、权限授予方式进入表网和深网不同,暗网需要配置Tor、I2P和Freenet等通信软件提供匿名协议才能获得访问。以2002年出现、目前创建暗网域名占比最大、开放资源最多的洋葱路由器Tor(The Onion Routing)为例,它最初由美国海军研究实验室创建,是一款被广泛用于隐秘的暗网自由通信的匿名通信软件。Tor“匿名性”的基本原理是通过隐藏流量分析来保护用户隐私、支持匿名浏览以及避开网络监控。Tor系统由超过上千个中继节点(或称服务器)组成,每个中继节点都是由全球志愿者免费提供[11],在用户运行Tor客户端时,系统采取加权随机方式为用户匹配入口、中间和出口3个中继节点,并建立“用户—入口节点”“入口节点—中间节点”“中间节点—出口节点”的3条通信链路,链路两端分别生成用户与3个中继节点共享的3个通信密钥。用户向目的服务器发送信息时,先使用3个密钥对数据包层层加密,数据包流经各中继节点时,每个节点用自己与用户端形成的对应密钥对传递信息的数据包进行解密,直至数据包送到目的服务器。在这一过程中,除了入口节点与用户电脑建立直接连接,还能识别最初请求者,入口节点将请求传递至中间节点、出口节点后,其他节点接收上一级节点的指令,只继续按照请求向下一个节点传递数据,并不记录流向,而作为传输终

端的目的服务器已不能识别指令和流量的真正来源[3],且按照 Tor 服务器建立10 分钟可用连接的频率,只显示退出的节点的 IP 地址每 10 分钟变化一次,从而达到隐藏用户真实IP 的目的。对于使用者而言,一旦启用了 Tor、I2P 和 Freenet 等特殊软件,就可以访问任何站点获取网络资源,既可以匿名浏览表网网页,也可以打开暗网站点而不会轻易暴露用户身份,还可以在暗网中匿名配置 WEB 服务,自由建立个人暗网站点发布非法内容,而不需要在域名管理机构注册或备案域名。

(二)以加密数字货币支付系统保证无痕交易

暗网具有自己独立的一套替代货币支付系统,所有交易以加密数字货币实施隐蔽支付。以 2008 年创建的、暗网市场最常用支付工具比特币为例,它是一种"去中心化"的在线虚拟货币,由存储账户余额的钱包文件组成,这些文件可保存在个人电脑上或委托给在线服务机构管理。比特币与传统货币相比具有以下四个特征:第一,拥有自主发行、管理和供求模式。比特币不受任何政府、法律实体的支持和银行、第三方机构的监管,没有中央发行人,新币发行过程被称为"采矿"(Mining),其价值完全由供求关系决定,交易比特币的人越多,其价格越高。第二,具有类货币的使用和兑换功能。比特币不仅可以用来购买商品或服务,也可兑换成人民币、美元、欧元、日元等传统货币。尽管大多数比特币交易发生在网上,但许多实体企业已经开始接受比特币。对此,一些国家虽未通过立法将其明确为法定货币,但也承认其作为一种"货币形式"①。我国对比特币实行较为严格的管控,将它定性为"虚拟商品",2013 年央行等五部委联合印发了《关于防范比特币风险的通知》,禁止比特币与金融机构和支付机构的接触,但对其他主体尤其是个人未作特别限制。第三,运用区块链技术实现转账。在线用户通过将交易添加到实行分散式电子分类记账的区块链中予以验证并转账。由于区块链采取点对点系统构架,组成的各个节点共享计算资源而不受中央节点的控制和协调,具有较好的抗操纵性和安全性,它不会拒绝某些用户使用其服务,对任何人开放,没有人能够阻止、关闭交易过程[4]。第四,与暗网、Tumble 技术结合使用具有高度匿名性。比特币交易虽不要求买家和卖家透露真实身份,但所有客户之间的比特币交易记录保留在区块链中。交易发生后,其他人虽不知道付款人和收款人的身份,但能够看到交易轨迹。为了进一步提高安全性和匿名性,一些暗网站点如"丝绸之路"利用 Tumbler 技术来处理比特币交易。作为一种代币混合协议,当买家在暗网付款时,站点使用一个中心化的智能加密 Tumbler 创建离线支付通道,所有参与者将会向其发送比特币并获得等量比特币的回报,形成若干虚假交易轨迹,从而模糊买家与卖家的比特币地址之间的联系,无法确定谁跟谁在进行交易。在比特币钱包管理和交易的过程中,如果将区块链与 Tor 等代理技术叠加使用,就可以帮助用户通过点对点网络进行匿名电子交易而查询不到单笔的交易记录,从而保障了暗网个人交易层面的高度匿名性。

(三)以 PGP 加密软件建立信息联系

PGP 软件(pretty good privacy),又称"优良保密协议",该软件使用各种加密算法对消息进行加密,并定期更新以解决加密漏洞。其加密原理在于,传统的加密采取对称加密,即利用单个密钥来加密和解密电子消息,这意味着在用户之间必须以某种方式共享密钥才能被解密,除非用户亲自传递,否则密钥有泄露风险,信息可能会被截获和读取。PGP 软件针对传统软件的安全漏洞发展出"公钥—私钥"的非对称加密技术,利用公钥加密消息,单独的私钥解密消息。由于私钥是由接收消息的用户确定的,所以不需要在用户之间传递额外信息,减少了能够解密信息的人员数量,增加了传输信息的整体安全性[5]。

在上述计算机技术支持下,暗网呈现出匿名通信与"去中心化"隐秘交易的特征,这必然导致原本"中性"的暗网在不同的适用目的下呈现出多重性质和用途。一方面,暗网在线匿名通信工具的特性被运用于军事通讯,执法机关情报收集,记者群体、企业和个人建立保密信息等合法用途;另一方面,由于该类软件通过改变网络路径使得用户难以被追踪,同样也可用于掩护犯罪活动,尤其是被恐怖分子加以利用实施恐怖活动。2015 年 11 月巴黎恐怖袭击之后,网站屡遭强制关停的 ISIS 发布了新的暗网地址,由表网转入暗网实施恐怖主义信息宣传。杰米·巴特利特也在《黑暗之网》中对暗网环境下的犯罪问题作过这样的描述:"一个能够搜罗网络中所有令人震惊、不安和充满争议的黑暗角落的术语——一个容纳了你所能想象的各种形态的罪

①在国际层面上,比特币的法定货币性质一直存在争议。俄罗斯、孟加拉国、玻利维亚和厄瓜多尔禁止使用比特币,并对非法交易予以惩罚;中国和日本等国禁止银行和金融机构转让比特币,但未限制个人交易比特币;德国没有将比特币归类为合法流通的货币,将其认定为是可以征税的财产;美国对于比特币相关的判例将其认定为"货币形式"。总体而言,比特币在国际上仍处于灰色地带。

犯和捕食者的领地。”[6]也许是人们对暗网发言活动和交易行为匿名性感到不安，近年来渲染暗网犯罪“恐怖性”的新闻介绍和文章很多，“暗网上出售几乎你能想象的任何东西”，“暗网上所做的任何事情都不涉及你在现实世界的身份和生活”，“订购玩具——儿童尸体，那些被挖去眼睛的性玩偶”[7]等。虽然与表网和深网相比，暗网具有隐秘与难以监管的特点，但它毕竟是构建在普通的互联网基础之上的网络运用，在暗网中发生的犯罪类型也并没有超出网络犯罪的范畴，反而是对于暗网犯罪没有数据佐证的夸张假设和描绘，刺激了普通人对于暗网世界的想象力和好奇心，一些潜在犯罪人和具有犯罪前科的人员想方设法进入暗网实施违法犯罪活动，而实际上，大多数犯罪人不一定会首选需要相当计算机操作技能要求的匿名网络实施犯罪。

三、国内暗网使用状况分析

进入并使用暗网是暗网犯罪发生的前提。虽然从理论上来说，所有网络犯罪类型都能以暗网为平台实施，但与犯罪相关的暗网的实际运用范围受两方面因素的制约：一是国家立法对于暗网性质的界定与使用监管的介入深度。暗网虽然具有匿名特性，但并不完全是“法外之地”，如果对其向本国网民的开放程度予以限制甚至禁止，从“违法性”上就能够阻截一部分人进入暗网世界、减少机会型犯罪。二是受进入暗网的个人计算机技能的限制。暗网站点无法通过常规手段访问，需要使用特定的软件、配置和授权才能登入。因此，涉及某些犯罪类型、持有特定犯罪目的、针对特定犯罪对象、具有某些个体特征的人员，在表网不能“得手”而转入暗网“下手”的强烈动机伴随下，同时暗网环境中该犯罪领域的“丰富资源”能够促成犯罪目标，犯罪人才会专门学习或利用本身已经具备的计算机技能进入暗网实施犯罪计划。研究我国的暗网犯罪与治理对策，必须考虑进入暗网实施犯罪的“有利”条件与限制条件对犯罪决意的影响，对中国网民使用暗网情况作出一个客观的定位和分级，而不是将一些具有发生可能性、但实际还未出现的，甚至人们主观臆想出的“暗网犯罪”作为立法完善和加强治理的基础。对此，应首先摸清近年来国内使用暗网、进而利用暗网从事犯罪的实际情况与发展趋势，然后分析国内常见暗网犯罪类型及对其执法打击与法律规制的困境，接下来探讨一些需要重视并正在形成规模效应的新型暗网犯罪，最后形成维护网络信息安全、治理常见高发新型暗网犯罪的具体思路与对策。

（一）使用暗网的合法性分析

在我国，使用暗网受到法律和行政法规的严格限制。早在1997年，我国出台的《计算机信息网络国际联网管理暂行办法》（以下简称《暂行办法》）第六条规定，“计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行建立或者使用其他信道进行国际联网”，并设置了违反该条将被责令停止联网、给予警告和罚款、没收违法所得的罚则。2017年实施的《网络安全法》第十条规定了建设、运营网络或者通过网络提供服务，应当符合法律、行政法规的规定和国家标准的强制性要求。条文中明确应当符合的“行政法规”当然包括了《暂行办法》中关于单位和个人不得非法实施国际联网的禁止性情形。第五十条对国家网信部门和有关部门依法履行网络信息安全监管职责作出规定，如果网络运营者违规传输信息，将被要求停止违法行为、采取消除等处置措施，对于源于境外的信息，采取技术措施和其他必要措施阻断传播。因此，利用暗网特殊加密信道非法传输信息的情形受《暂行办法》《网络安全法》的完全管控。

而以美国为代表的西方国家一方面允许使用暗网，另一方面采取窃听、截取暗网通信或规定特殊情形下通过紧急赋权关闭暗网的方式实施暗网管理。相比之下，中国相应立法的出台表明了国家对于包括暗网在内的秘密信息传输途径采取了源头控制的思路，以尽早防止非法网络技术破坏网络空间新秩序。基于此，暗网目前尚未对我国的网络安全造成严重的直接影响。但考虑到匿名暗网可能产生的犯罪空间和机会问题，国内相关部门和企业网络安全研究机构近年来也加强了对暗网的了解与监测活动。

（二）与犯罪有关的国内暗网使用行为分析

2017年以来，国外具有相当规模的暗网交易平台阿尔法湾（AlphaBay）和汉萨（Hansa）陆续被国外执法机构发现并联合捣毁，之后新建起的一些暗网中文论坛又发生了多起国内数据泄露和不法交易事件，令整个暗网环境之下的全球不法交易情况状态不明。为摸清我国国内隐秘使用暗网的最新动态，腾讯“守护者计划”安全团队对2018年中国网民访问暗网情况进行了调查摸排。参考其调查报告显示的结果，对反映出来的国内暗网使用行为作出以下分析。

第一，我国的暗网搭建和访问行为尚不突出。据腾讯统计，暗网日均访问用户数占比不足5%，1/3用户使用全局代理访问；广东用户占比最大约21%，其他省份访问占比大致平均，最高未超过7%；男性访问者约占77%，女性访问者约占17%，其余性别不详；19-27岁的访问者占比超过半数(52.1%)，其次分别是10-18岁(29.9%)、28-36岁(8.8%)等。以上数据显示，女性访问者所占比例较低，可能与女性对暗网色情、暴力资源的需求和兴趣相对男性较低有关，因为大量反社会行为的研究证据表明[8]，男性更会寻求刺激、更容易冒险，由此产生了暗网浏览行为的性别差异；广东地区相比于内地，外国来华人员较多，当地居民也较早地接触一些外来文化和信息，这或许是形成暗网访问地域差别的历史、文化方面的因素；进入暗网的访问者往往在计算机和网络技术方面拥有一定专业技能，因此在年龄结构上年轻人成为暗网访问的主体。

第二，暗网上数据泄露和不法交易行为频发。据腾讯对暗网数据交易进行的统计，网购物流数据最多，占58.59%；购买身份证信息占13.43%；酒店数据占12.15%；社交账号数据占7.14%；其他占5.06%；企业信息占0.86%；博彩数据占0.56%；车主信息占0.53%；简历信息占0.48%；学生信息占0.41%；购物网站占0.37%；贷款数据占0.17%；出行信息、银行信息、股市数据、银行数据赚、交友网站等占0.05%。各类数据如果被电信网络诈骗团伙掌握，都可以针对被泄露公民个人信息的事主本人“适用”，为其专门编制某一特定类型的电信网络诈骗“剧本”，实施“精准诈骗”。例如，诈骗人针对流出的事主网购物流数据，根据其网购或物流商品的相关信息，对其实施冒充某购物网站客服类诈骗。

第三，非法获取虚拟数字货币成为新兴暗网黑产。据腾讯统计，几乎所有的暗网交易都使用虚拟数字货币来结算。掌握虚拟数字货币就能够在暗网中兑换商品、服务和法定货币，因此，“货币暴力”催生了以非法“挖矿”、勒索、黑客盗窃等威胁网络安全手段获取虚拟数字货币为业的新兴暗网黑产。以促成新比特币的发行非法“挖矿”为例，从事“挖矿”需要基本的挖矿软件(如CGminer、BFGminer或GUIMiner)、挖矿硬件(如AntMiner、Avalon或ASICMiner)、矿池、比特币钱包和接受、存储比特币的加密网上银行。其原理是由许多参与者利用“矿机”和挖矿软件运行特定算法产生算力，反复尝试不同的随机数对区块链网络上承载的未打包交易进行哈希运算，直到其中一名参与者找到一个随机数能够印证区块中的交易、构建出区块，由此被授予一定数量的比特币作为“挖矿”赚取的“奖励”。该系统最初设计为每开采一个区块发行50个比特币，之后每次开采210,000个区块时，降低发行率以防止通货膨胀[9]。为了利用他人正在运行的计算机作为“矿机”为自己挖矿获利，减少大规模挖矿需投入的计算机硬件、用电量等成本损耗，犯罪人通过对网吧等具有高性能计算机的特定场所植入木马、控制企业服务器组建僵尸网络、在网站植入网页挖矿代码等侵入他人计算机系统的方式实施非法挖矿牟利，以实现对虚拟数字货币的渴求，然后再进入暗网以比特币为工具从事洗钱和不法交易，由此催生了非法“挖矿”谋取暴利的暗网黑产。

综上，由于严格的立法管控，国内暗网网民在数量上远远低于未限制暗网使用的发达国家，占我国互联网网民总数的比重较小，因此，暗网犯罪在我国尚未达到泛滥的程度。当然这一结论也是建立在已知的执法数据基础上，暗网里也有腾讯安全团队等研究机构所“接触不到”的情形，在这些未知领域统计数据可能存在较大差别，很可能隐藏着犯罪黑数。2018年至今，随着一批大型暗网站点的攻破和部分暗网中文论坛的停办，暗网活动占比萎缩，腾讯安全团队没有继续再对暗网进行系统性的推进研究和数据追踪。但是一些常见的网络犯罪形态在暗网环境中固化下来，还有一些新的与虚拟数字货币有关的不法行为出现在暗网犯罪体系中，对其空间转移和生成速度须密切关注、研判，并提出相应犯罪治理对策。

四、暗网犯罪的常见高发类型及刑事打击重点难点

西方犯罪学家将网络犯罪分为四类：以网络黑客行为为代表的非法入侵、破坏计算机类犯罪；以诈骗和盗窃为代表的网络侵财类犯罪；以儿童色情和淫秽物品交易为代表的网络色情类犯罪；以雇佣杀人、暴恐袭击为代表的网络暴力类犯罪[10]。当前，占据暗网空间57%的非法内容包括但并不限于以上犯罪类型，除了色情、诈骗、破坏计算机信息系统、恐怖主义招募和通讯之外，非法金融、毒品贩卖、武器走私、假币等犯罪活动也在暗网中不同程度地存续[11]。因此，暗网犯罪应作扩大解释为“利用暗网实施的犯罪”。在国内犯罪实务方面，暗网犯罪呈现出一些常见高发类型，在侦查打击和刑法惩治过程中还面临一些制度和现实障碍，需要从调查思

路和法律适用上突破难点。

(一)暗网犯罪的常见高发类型

通过对2018—2020年上半年期间经国内法院判决的利用暗网从事犯罪活动的案件进行实案收集,发现暗网犯罪呈现出类型分布上的“两极化”特点:常见高发犯罪类型所涉罪名与犯罪手法较为集中,如计算机、色情、侵财类犯罪,此为严重的“一极”;网络暴力类犯罪,如雇佣杀人几乎处于空白状态,利用暗网实施恐怖主义活动在暴力程度上和行为本身所具有的社会危害性方面也极其有限,此为轻度的“另一极”;处于中间地带的是一些向“两极化”发展的偶然犯罪与不法行为。接下来针对常见高发的暗网犯罪和轻度网络恐怖主义犯罪的“两极”化犯罪类型,围绕刑法适用与打击难点展开分析。

1.提供进入暗网程序、工具的犯罪。国内法律和行政法规虽对连接暗网作出了禁止性规定,但仍有部分网民通过匿名工具使用暗网网络。进入暗网需要获取VPN翻墙软件、浏览暗网的Tor浏览器、暗网网址等基本工具,一些犯罪人利用访问暗网的“市场需求”,在表网上通过论坛发帖,QQ群、微信群等即时聊天软件,出售访问暗网的基本工具及相关信息,为他人进入非法网络提供程序、工具。该行为一方面违反了国家要求使用规定国际出入口信道连接网络的相关规定,另一方面导致了隐藏在暗网服务器中的匿名活动较高的触法风险。对该帮助行为独立适用刑法罪名、作为正犯行为予以评价,有助于从“入口”上减少暗网犯罪的倍增。《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的程序、工具罪的犯罪构成要件,最高法《司法研究与指导》对“侵入”作出的解释是“未经授权的人员违反国家规定擅自进入特定计算机信息系统”,暗网及其背后庞大的数据资源和信息体可归属于“特定计算机信息系统”,对于向他人提供进入暗网的基本工具的行为,情节严重的,应据此条之规定追究其刑事责任。

2.通过暗网买卖公民个人信息的犯罪。公民个人信息和重要数据是当前暗网黑市交易的主要“商品”之一。当前,组成电信网络诈骗犯罪链条的上游犯罪团伙,主要涉及为电信诈骗集团实施“精准诈骗”提供公民个人信息、企业信息,为被骗资金的转移提供银行卡“人头”账户的从事黑灰产业的人员。他们将暗网作为打包售卖和转卖信息的重要“集散地”,为电信诈骗犯罪提供信息支撑。在非法购买公民个人信息的情形下,买家利用付费VPN(虚拟专用网络)突破中国互联网防火墙(又称“翻墙”),输入暗网网址非法登录暗网论坛和黑市,利用比特币购买公民个人信息。通常情况下,买家先用微信或支付宝扫码付款兑换一定数量比特币,再用比特币买入公民个人信息和数据的“商品”,扣币成功后,卖家会向买家发送一个包含mega暗网网盘的链接,点击链接mega网盘就会自动下载并保存该“商品”;在非法出售公民个人信息的情形下,卖家进入暗网论坛或市场注册账号,发布“查询服务”“信息出售”等标题的网帖,标明提供公民个人信息“查询”、出售等服务的项目、价格,之后将交易获得的比特币通过境外网OTC平台兑换成人民币转存国内个人账户。暗网上出售或购买的非法信息主要有:包含姓名、出生日期、身份证号码、住址、电话号码等公民个人基本信息,内含有手持身份证照片的“升级版”个人信息,包含姓名、住址、电话、车辆品牌、车辆型号、车牌号、发动机号等数据在内的购车信息,包括姓名、手机号、出生日期在内的购物信息,包括姓名、身份证号、手机号码、开户日期、开户券商、交易金额在内的炒股用户信息,个人存款、网贷(包括裸贷)、学籍注册和就业登记信息,社保用户数据、棋牌网站用户数据、游戏网站用户数据、购票系统用户数据,商用网站服务器后台管理权限、数据库,等;犯罪人在表网上找到卖家后再转卖这些信息获利或打包提供给电信诈骗团伙筛选使用。《刑法》第二百五十三条规定了侵犯公民个人信息罪的犯罪构成要件,对于上述通过暗网非法获取公民个人信息并提供给他人以获取非法利益,情节严重的,应依该条之规定追究其刑事责任。

3.通过暗网走私、贩卖毒品的犯罪。各国对毒品范围的界定存在一定差异,在法律适用方面也有很大分歧,以大麻为例,在我国将其作为毒品予以使用、控制和交易禁止,而在美国的一些州则实现了大麻使用的全面合法化或与大麻相关的毒品犯罪轻罪化的情形,澳大利亚绝大多数州对大麻走私贩卖的最高量刑也要低于其他种类的毒品交易,荷兰毒品立法对于持有和使用小剂量的大麻做出罪化处理[12],等等。由于立法和执法上的差异,一些境外卖家在暗网黑市上利用本地毒源出售大麻、“MDMA”(俗称“摇头丸”),其价格分别约为国内市场价的三分之一、二十分之一。近年来,一些成瘾人员和贩毒人员为供自己吸食或贩卖毒品牟利,开始通过Dream Market网站、“AB”网站以及其他暗网市场,向加拿大、德国、西班牙、荷兰等国境外匿名卖家分次购买LSD(麦角酰二乙胺,俗称“邮票”“纸皮”)、MDMA、氯胺酮(俗称“K粉”)、大麻等小剂量

“软毒品”,以比特币方式完成付款,境外卖家再使用 UPS、DHL 之类的国际快递物流或 EMS 将毒品每 10 克左右藏匿于一封挂号信件或邮包内邮递进境。《刑法》第三百四十七条规定了走私毒品罪的犯罪构成要件,对于上述违反海关法律法规以及国家对于毒品的管制规定,通过邮寄入境、收取国际包裹或邮件的方式获取毒品的行为,应按照该条之规定追究其刑事责任。

4.利用暗网宣扬恐怖主义、极端主义的犯罪。国外有研究认为,以网络为工具传播和宣传恐怖主义、极端主义思想,为恐怖组织筹集资金、招募人才,恐怖分子之间协调恐袭行动等在表网上实施的网络恐怖活动已经开始向互联网更深层的暗网转移[13],在暗网论坛和聊天室时常能发现一些宣扬恐怖主义、极端主义思想的煽动性言论和评论。由于通过 Tor 客户端浏览暗网需要经过多个路由节点“绕路”才能打开暗网站点,网页加载速度非常缓慢,暗网相关网页上主要是一些文字线程和少量低像素图片难以发布视频。一些不法人员、恐怖分子利用暗网论坛发布有关恐怖组织旗帜标识、作战实况、处决或掳杀俘虏等战场实景,以及带有杀人、斩首、切腹、爆头等血腥暴力内容的图片、视频文件的链接和邮箱地址,供人购买和交换。违法犯罪人出于好奇或以谋利为目的进入暗网非法获取或专门购买上述宣扬恐怖主义、极端主义的视频、图片资源,之后在互联网上与他人相互交换、分享或出售。《刑法》第一百二十条之三规定了宣扬恐怖主义、极端主义罪的犯罪构成要件,对于通过登陆暗网获取宣扬恐怖主义、极端主义的图、视频资料和网络资源,在表网向他人发送、分享,如果经过审读图、视频资源所载内容符合公安部《暴力恐怖、宗教极端、民族分裂等有害信息认定标准》的,属于宣扬恐怖主义、极端主义物品的行为,应依该条之规定对其依法追究刑事责任。一些犯罪人虽未将从暗网获取的恐怖图、视频资料与他人交换或出售,但拷入储存设备随身携带,在住所、办公场所或交通工具内存放,据其情节,也可能构成《刑法》第一百二十条之六规定的非法持有宣扬恐怖主义、极端主义物品罪。

5.利用暗网贩卖、传播淫秽物品牟利的犯罪。暗网活动的匿名性与针对封闭访问者设置的专门访问权限为非法资料、色情视频的交换、交易提供了便利。一些违法犯罪人以在暗网平台发布淫秽电子信息交易帖的方式,将淫秽视频、图片上传至暗网站点进行贩卖、传播;也有一些不法分子进入暗网获取一些表网上不能获得的“最新”的色情资料,如大量的儿童色情视频,之后进一步扩散到表网上进行散布、贩卖以谋取非法利益。《刑法》第三百六十三条、三百六十四条规定了贩卖、传播淫秽物品牟利罪、传播淫秽物品罪的犯罪构成要件,对于上述利用暗网贩卖、传播淫秽电子信息的行为,一经发现,应依此追究相应刑事责任。但需要注意的是,淫秽视频、图片等资料一旦从暗网转移到表网将形成多头传播,要打击暗网背后真正拍摄、制作淫秽视频的犯罪人会更加困难。因此,刑事实务中发现和追诉较多的是淫秽物品贩卖、传播型犯罪人,而非淫秽物品的制作者。

(二)打击暗网犯罪存在的法律适用争议点、侦查难点及解决思路

上述关于暗网常见高发犯罪类型与刑事惩治的罗列梳理来源于暗网犯罪实案处理结果的一般情况分析,具体实务中,这些已有类型在侦查打击和刑法适用方面仍然存在一些追诉难点、司法施用障碍甚至立法无法完全评价的情形。针对暗网犯罪案件在处理过程中的一些复杂性问题和争议点,以及新型暗网犯罪的发展动向,拟作出进一步分析并提出解决思路。

1.对于提供进入暗网的“工具”作出扩大解释。近年来,随着一些暗网站点被执法机关攻破或被迫“下线”,一些暗网网站管理人员采取更多的验证手段对访问者进入网站作出限制以增强站点安全性。获取 VPN 翻墙软件、Tor 浏览器、暗网网址信息本是访问暗网的基本配置条件,也是进入暗网的重要工具,过去,浏览者只要按教程操作,大部分暗网站点都可以通过在 Tor 浏览器输入网址自由进出。当前,自我“保护”更为隐秘的暗网论坛、黑市和聊天房则设置了繁琐的准入条件。比如要求担保人推荐,即新用户在注册暗网站点用户名和密码之前,需由已通过验证的会员分享邀请码为其提供担保才能进入;实行自我推荐,即新用户必须按管理员要求上传非法材料才能通过入站验证,或是要求新用户出示曾在暗网上发布的一定数量信息,以证明浏览、参与过同类暗网论坛的话题活动。基此,对于进入暗网的“工具”已经不能狭义定义为网络配置工具及相关信息,对于为协助他人进入暗网,在表网上以传播或贩卖方式提供暗网教程、分享暗网站点邀请码,为新用户通过暗网验证提供便利条件的行为,都应当纳入《刑法》第二百八十五条第三款的追诉范围,予以刑事规制。

2.扩大“公民个人信息”的概念界定。对于利用暗网获取或出售公民个人信息的案件,在实际办

理过程中出现一些新情况，应进一步合理界定“个人信息”与“公民”的范围，精准打击侵犯公民个人信息犯罪。

2017年，《最高人民法院最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条明确了“公民个人信息”的概念，是指“以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等”。可见，司法解释对于“公民个人信息”的界定以信息所承载的“自然人身份可识别性”为基础。但在大数据时代，以电子账户为代表的网上用户身份已经广泛适用于包括快捷支付在内的高信任水平应用服务，如果犯罪人能够整合分布在各个应用程序中零散的被害人在线身份线索，以连接和相互印证的“信息加工”方式进行网上用户身份的拼接，就不再需要整体性的自然人身份的网络录入，直接通过在线默认的身份识别路径窃取被害人相关网络服务的身份授权。例如，电子邮箱申请虽未采取实名制登记，不属于能够确认或识别自然人身份的信息，但如果犯罪人获取大量电子邮箱的账号和密码，使用手机登陆电子邮箱，绑定非法获取的、与申请人本人无关的其他人员的信用卡，就能使用支付功能购买游戏装备、虚拟数字货币，或是利用帮他人充值、购物收取费用等方式将非法换取的虚拟财产变现获利。可见，电子邮箱在线信息虽不能直接对应特定公民个人信息，但它能与信用卡信息相结合，成为盗刷自然人信用卡的辅助工具。因此，对于未明显包含在司法解释范围内的在线信息，即使不能单独凭其直接确定自然人身份，但只要与其他信息结合，能够影响到特定自然人的财产权利、人身安全的，都应当纳入广义“个人信息”的范畴。

侵犯公民个人信息犯罪中的“公民”的范围是否仅限定为“我国公民”在实案处理中也存在一定争议。暗网的全球“流动性”与匿名多变的特点吸引了来自各国的猎奇者、违法犯罪者、恐怖分子建立平台发布非法信息与在线互动，暗网市场上大量售卖的公民个人信息更是无地域、国别限制，犯罪人非法获取的也并非仅是我国的公民个人信息，实践中也出现了国内犯罪人从暗网上获取国外的公民个人信息、实施针对外国人的电信网络诈骗或盗刷信用卡的案件。对此，有观点认为，刑法中的“公民”是指“中国公民”，外国人的个人信息不属于“公民个人信息”的范围。从刑法本身的规定来看，一方面，我国刑法并未明文将“公民个人信息”限定为“我国公民个人信息”，涉案外国人的信息应当同中国公民信息一样受到刑法的平等保护；另一方面，即使各国对于公民个人信息泄露和买卖存在是否入罪、入罪标准方面的差异，刑法调整范围确有不同，但基于属人原则仍应对中国公民实施的侵犯本国或其他国家公民个人信息的行为追究刑事责任。

3.建立毒品高危地入境邮件全面查验制度。近年来联络暗网卖家邮寄毒品的案件高发，海关查验进境邮件时如果发现毒品线索，立即报告海关缉私局立案侦查后，对涉案邮包或信件实施控制下交付，抓获前来收取国际邮件的犯罪人及其同案犯，现场拆封邮件查获毒品。“软毒品”在运输过程中，通常被制成邮票大小的片状物、用锡纸包裹后藏匿于国际信件内，或者黏合在普通商品的夹层中，通过机场X光机检查时仅显示邮政包裹内的商品，如不做人工拆封、使用快速检测板取样检测可疑物质成分，一般很难发现藏毒。而各地海关驻邮局工作人员对入境邮件进行查验、机场海关对航空运输邮包实施现场监管时，主要采取抽查拆检的方法，因此仍有一些藏匿毒品逃避海关查缉最后到达买家手中成为“漏网之鱼”。主营毒品交易的“丝绸之路”为了防止控制下交付，就曾为毒品卖家发货提供了详细的指导建议，例如，为了避免毒品搜寻犬例行的邮政调查，提醒卖家用真空密封的拉链包密封毒品并以酒精清洁包装以避免调查。在实案中，犯罪人以暗网交易、收取入境包裹的方式获取毒品只要成功一次，就会多次使用邮寄的方法走私毒品用于销售牟利，随着毒品暗网“屡打不绝”，未来将给海关查验毒品带来更大的压力和挑战。

对此，应摸清暗网售卖毒品的犯罪规律，依据大麻走私主要来源国的范围修改进境邮件筛查规则，确定高危风险等级的重点国家或地区，制发规范性文件要求对毒品高危地入境的包裹、邮件实行更加严格、全面的查验，提高拆封检测率，防止境外毒品流入国内市场。

4.形成淫秽信息快清与制作者重点追溯双向机制。与利用暗网售卖毒品不同，各类毒品是较为固定的“商品”形式，仅有种类和品质差别，但暗网上的淫秽物品具有新旧内容之分，这决定了暗网色情资源的传播途径就像一块石头投入水面所发生的一圈一圈的波纹，呈现出“暗域”向“明域”扩散的“波圈型”结构。“新货”被掌握在淫秽物品制作者手中，他们通过设置暗网访问权限与其认可的一些封

闭访问者共同组成对社会产生犯罪影响的“暗阈”中心点，即“最小范围”的匿名交易空间，封闭访问者从中获取最新资料，然后在暗网自由空间里向其他普通访问者进行传播或转售，其接收者再转入以保密性和匿名性极高的 Telegram 等国外在线社交平台、国内网站将色情资源推向更大的网络空间范围，形成“暗域”中心点向“明域”放射的数据资源。在这一犯罪结构差序化格局中，越是接近“暗阈”中心点的非法交易“安全性”越高，相反，在表网上从事淫秽物品传播或贩卖活动、处于“波圈”末端的人员，却可能因为在线搜索了与淫秽物品有关的关键词，被严密的网络监控识别其寻找色情资源的违法意图及其真实身份成为刑事打击对象。而实际掌握淫秽物品第一手来源的色情视频制作者以暗网为掩护，匿名潜藏在“暗阈”中心点，与之接触的封闭访问者极其有限，色情资源经 N 级传播者向各互联网服务器输出后反倒形成类似于暗网的中继路由节点对初发点的保护效果，因此淫秽物品制作者的活动很难被侦测。

可以说，涉及淫秽物品的暗网犯罪，传播环节越多、程度越深、范围越大，追踪淫秽物品制作者的情况就会变得越复杂。2020 年曝光的韩国“N 号房”案件的发现与调查过程就是一个现实例证。“N 号房”案件是指犯罪人通过 Telegram 建立 80 多个秘密聊天房间，将被欺骗和威胁的包括未成年人在内的女性作为性剥削对象，在聊天房内共享非法拍摄的性视频、照片和受害人真实身份信息以非法牟利的案件。据韩国警方统计，通过支付商品券或虚拟货币在“N 号房”付费观看的人员，包括具有重复可能性的参与人员高达 27 万人，这些淫秽物品和色情视频的“需求者”和“消费者”均属于“波圈型”结构中的最外围人员。韩国警方拘捕的首批“N 号房”运营者则是初期运营团队所建色情聊天房中的付费会员，之后才加入正式运营团队。随着案件线索的积累与推进，侦查活动才进入到制作视频、设计“N 号房”经营模式并培育运营成员的中心点，追诉至“N 号房”的创建人。

Telegram 社交软件与其他普通软件相比，虽然具有相互交换加密与“阅后即焚”的自毁消息功能，高度隐蔽了“N 号房”运营活动，但它毕竟是属于表网范畴内由传统信息交换平台所提供的 SNS（即社交网络服务 Social Networking Services），要在暗网中打击采取加密技术的淫秽物品制作人、与制作人保持稳定联络的“最小范围”内封闭访问者难度更大。然而，研究暗网色情资源的“波圈型”扩张结构，给了我们这样的启示：传播淫秽物品类犯罪的“波圈”范围能缩能伸，主要依赖于扩散的传播途径能够将犯罪链条传动到多远，如果不尽早切断和阻击传播环节，传播“动势”会将色情产业链条扩展到更广阔的网络空间，获得愈强的“生命力”，制作者也会因此“被保护”得愈深。因此，除了发现和打击外围“明阈”范围内的传播淫秽物品类犯罪人，并逐层内扩至“暗阈”中心点，还不能忽略截断传播环节的有效方式，因为犯罪人虽然落网，但其发布的淫秽物品资源并没有因为缺乏人的因素而丧失活性，它们留在网路上随时被新的“宿主”发现、利用从而能够维持未来的犯罪传播链条。因此，一经发现各互联网服务器上的色情资源必须以更快的速度清除其下载和交易路径，才能制止幕后制作人“安全”地隐藏在不断叠加、累积的庞大数据背后，增加侦查人员深挖来源的难度。

对此，应通过立法或网安部门制定规范性文件的方式，规定对于网站和社交网络中发现的“淫秽物品信息”，从指令相关互联网企业删除到完成清理的时限不得超过 24 小时。在“淫秽物品信息”的删除范围上，也应当扩大信息对象适用，对于群众举报或主动发现的以预览方式提供的不完整色情视频、仅有一些“引入性”描述的图片和文章，虽因阅览权限问题没有涉及直接的淫秽物品内容，但其发布目的在于引诱他人以付费方式查看完整的色情视频、图文，具有后期补给违法色情内容的空间的信息，也应当在介入调查、保存相关电子证据以后，要求互联网应用平台管理者作快速清除处理。

5.关注和研判三大领域暗网犯罪发展趋势和最新动向。除上述常见高发暗网犯罪类型之外，还有一些目前发案数量较少、但考虑其未来犯罪化发展趋势值得高度关注的犯罪案件类别。第一，在政治安全领域，应加大对于暗网恐怖主义活动、利用暗网匿名通信串谋实施危害国家安全犯罪的发现和打击力度。一是密切关注利用暗网的危安通联行为。实施恐怖袭击与其他危害国家安全的犯罪通常需要在一个秘密网络空间中协调、向参与者下达指令，而暗网具有天然的匿名通联优势，Tor、I2P 和 Freenet 电子邮件、实时聊天房、暗网版社交网络平台以及即时聊天工具的秘密聊天模式，容易成为危安人员勾结犯意的工具。例如 2014 年香港“占中”事件和 2019 年香港暴乱事件中，活动的组织者通过匿名网络与外国、境外机构的组织、人员进行秘密通联，推动事件发展进程。二是涉及恐怖分子利用暗网筹款、购买爆炸物和武器、招募人员等恐怖

活动在实案中较少，但仍应加强追踪和识别。以恐怖融资为例，一些暗网网页挂上比特币钱包地址，邀请捐赠者点击为伊斯兰极端圣战组织捐款，或是在显要位置以文件形式发布使用暗网为恐怖组织秘密融资的实用指南[14]。由于暗网隐藏的生态系统有利于恐怖组织宣传、招募、融资和规划，打击治理恐怖主义的安全战略战术仍要延伸到暗网领域。第二，在社会安全领域，应对利用暗网实施的涉枪犯罪加强查缉和打击力度。在表网上交易风险极大的各类违禁物品，如枪支弹药、毒品、公民个人信息、淫秽物品及证件信息在暗网黑市中均能找到购买资源。实案中一些非法出借枪支、非法持有枪支的犯罪人之间就是通过暗网建立联络，通过设置“秘密传递点”的方式约定接头时间和地点，由出借人将放有枪支的包装盒放置于公共场所，借枪人到约定地点“寻枪”以实现双方互不照面的出借行为，从而达到相互隐匿真实身份、降低查缉风险的不法目的。利用暗网从事枪支流通容易滋生抢劫、杀人、以危险方法危害公共安全以及恐怖活动等严重暴力犯罪，社会危害性极高，对此流通方式应高度重视。第三，在经济安全领域，应严厉打击从暗网中获取黑客软件和在线工具以攻击数字资产交易平台、盗取企业数据库密码等破坏计算机信息系统行为。暗网上的黑客工具种类众多，犯罪人如果以表网中特定的交易平台和企业数据库为目标，分析、评估其漏洞类型，有针对性地下载或购买漏洞利用套件，就可以通过交易平台进入账户窃取电子货币，或者析出企业数据库密码向企业实施勒索。近年来，勒索软件不断翻新、攻击数量呈指数级增加，对企业重要数据资产的威胁逐年上升，企业网络安全团队和专门从事暗网监控和研究的网络安全公司应当探索合作模式，在暗网市场中监测、发现一些正在出售的最新的漏洞和恶意软件“商品”，评估自身系统是否存在未发现的安全漏洞问题以及哪些软件将对本企业数据库构成最大的安全风险，从而有针对性地根据攻击方式调整系统配置，以降低黑客软件攻击的力度。

五、暗网犯罪的新动向及其综合治理对策

暗网犯罪在发生形式上与暗网空间紧密相连，部分犯罪类型单纯属于攻击计算机信息系统犯罪，但更多的是利用暗网的匿名性从事非法交易、危害国家安全和社会安全的活动。现行刑法对以暗网为工具实施的犯罪，在计算机犯罪罪名和传统的罪名体系框架下基本可以实现追诉和惩治。《网络安全法》《国家安全法》《反恐怖主义法》《香港特别行政区维护国家安全法》等相关立法的支持也有利于将更多形态的暗网犯罪行为纳入刑法打击半径之内，通过合理解释将传统刑法延伸适用于暗网活动空间，因此，规制暗网不法行为并不存在太大法律适用上的障碍。暗网犯罪治理的真正难点在于不法行为在暗网中的匿名发生性以及隐秘技术所带来的调查难度，即不在于刑事追诉中的“诉”，在于如何实现“追”。对此，提出以下对策配合暗网犯罪的刑事打击。

（一）利用犯罪行为的“空间转移”与调查新技术祛暗网匿名特性

暗网虚拟空间的匿名特性给网络案件调查带来一种颇具迷惑性的“假象”，尤其是真实用户不断秒变的 IP 地址、难以定位的网站服务器、多层加密的匿名聊天、区块链点对点网络交易发生后即被抹去单笔记录等，完全改变了以犯罪人数字空间行为轨迹、信息流和资金流查证等循“迹”追踪为主要内容的侦查作用方式。就像暗网中贩卖色情视频的交易双方而非视频的制作者，被认为是利用暗网实施淫秽物品犯罪的“源头”，侦查行为指向的犯罪空间往往才是“发生交易”的这一匿名暗网站点。但这一认识忽略了一个问题：非法视频并不是在暗网上拍摄出来的，真实世界才是真正的犯罪空间。帮助美国 FBI 发现和抓捕“丝绸之路”的创建人罗斯·威廉·乌布利希的关键证据并非是他在暗网空间中的某个活动轨迹，而是他不经意间发布在表网上的一个电子邮件地址。乌布利希通过表网寻找 IT 助理、对“网页如何嵌入 Tor 网”提问时，将个人的 gmail 电子邮件地址留在了网站上，虽然他意识到风险之后进行了删除操作，但仍然被警方成功追踪。此外，其他暗网创建人也是在表网空间领域被发现和控制的。暗网只是一个“相对”独立的空间领域，它是互联网的延伸部分，暗网犯罪人存在于相互交织的真实与虚拟空间，一定会同时或交替使用生活物理空间、表网空间和暗网空间从事线上和线下活动。与犯罪迁移理论所揭示的犯罪人从表网空间移动到暗网空间的路径相反，空间转移理论支持这样一种观点：犯罪人总会走出并超越暗网犯罪空间，在互联网世界的表网部分与现实世界发生沟通和互动，而这正是启动传统侦查方法落地查证犯罪人的重要时机。因此，通过加强对表网上暗网信息的全面筛查、网络监控和情报分析，把握犯罪行为发生空间转移的时机，能够有效帮助侦查人员结合暗网

主要节点及其传输路径对犯罪人实施定人定位，应将对暗网空间领域的钓鱼执法和侦查视线同时部署于表网空间领域。

对于暗网的夸张宣传，让潜在犯罪人以为，如果执法机构没有先进的技术手段去匿名化，就很难遏制和打击暗网犯罪。对于完全匿名的 Tor 网络并非不能进行有效的刑事侦查，例如，利用犯罪分析技术方法可以从暗网论坛发布的视频或图片中挖掘和追踪一些与犯罪人身份有关的重要拍摄信息。但也仍然需要加快投入和研发最新的、更多的技术手段、更隐秘的侦查手段以追踪和反制滥用暗网的不法情形。一方面，加强暗网信息检索、暗网节点识别等祛匿名化暗网应用工具的技术研发和升级。之前主要是通过发现和利用匿名通信软件的漏洞或安插留有后门的中继路由节点，截获传输数据包以间接方式祛匿名化，后来美国国防部先进研究项目局(DARPA)研发出 MEMEX 暗网搜索引擎，可以直接通过数据块分类与识别挖掘暗网信息，获取普通搜索引擎不能获取到的隐秘内容。它最初是为监控深网领域的信息追踪而开发设计，之后被应用于监测暗网活动，但在搜索范围和使用功能方面还需要进一步完善。另一方面，对暗网站点中危险隐蔽社区实施技术布控和用户分析。例如，开发暗网聚焦爬虫自动获取暗网站点信息，利用社交网络分析和超链接分析探知犯罪人、恐怖组织线上人际关系结构的潜在模式和发展动态，定位暗网犯罪和恐怖活动轨迹较为集中的隐蔽社区，在危险隐蔽社区中布网安插刑事特勤，监测和收集用户访问数据，分析具有重大犯罪嫌疑的用户特征并结合其表网活动轨迹进行比对追踪等。

(二)倒逼互联网企业强化暗网信息源头管控

在实案中发现，相当数量的犯罪人最初是通过一些媒体不实宣传了解到暗网“深不可测”的特性，出于好奇，才开始通过浏览互联网网页主动了解进入暗网的方法和操作技术。国内一些搜索引擎和知识普及、经验交流的论坛、网站不仅能够查找到专用软件 Tor 浏览器的下载链接以及安装浏览器进入暗网的详细教程，还能搜索到防止被执法机构地理定位和识别的“详细说明”，并能获取登录暗网所需要的、如“暗网中文交易市场”“自由国度论坛”“暗网中国”“茶马古道”等相关中文暗网平台网址。进入暗网市场和论坛后，也可收获更多免费的或打包贩卖的其他中文或英文暗网网址，大量低俗色情视频、木马程序、洗钱话术教程。犯罪人与不法分子之间可以通过暗网论坛和聊天功能匿名接触交往，相互学习网络犯罪技术和手法，甚至形成犯罪合意从而对现实世界产生不法威胁。表网上的相关互联网企业若不履行监管责任或履责不到位，就会成为滋生暗网犯罪的“帮凶”。

《网络安全法》第四十七条规定：“网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。”第四十八条规定：“任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。”对于未履行用户发布信息、提供应用软件管理义务的，第六十八条规定了相应的行政处罚措施，《刑法》第二百八十六条之一规定了拒不履行信息网络安全管理义务罪。但在实践中，该刑法罪名适用率较低，原因在于互联网企业对于监管部门的整改要求基本不会置之不理，都会按照指令删除非法信息或关闭相应网页。因此“拒不整改”的构罪条件不会真正成立，至于整改之后能否继续投入人力、物力保持中长期治理效果则不作为刑事追责的考量因素。《网络安全法》的处罚措施按惩罚程度排序由轻到重分别为警告、没收违法所得、罚款、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。对此，在实践中应对违规互联网企业从严从重适用《网络安全法》惩罚强度更重的行政处罚措施以倒逼其强化暗网信息的专业检测与清除活动，切实履行用户身份信息审查、违法信息处置和信息安全报告义务，建立、完善发布暗网相关信息的投诉和举报机制，从源头上真正减少暗网犯罪的发生。

(三)加强暗网犯罪国际刑事执法合作与情报交流

暗网环境下灵活的个人数字身份、闪变的匿名 IP、执法监管的困难为地理位置分散的网络犯罪合作者提供了联络便利，容易在世界范围内形成若干“陌生人犯罪集团”实施跨国犯罪。“丝绸之路”的主要犯罪成员就是生活在不同的国家，通过暗网共同在线经营一个犯罪集团的典型案例。创建人乌布利希居住在美国，网络专家加拿大人克拉克住在爱尔兰，比特币供应商沙隆利用位于埃及、捷克共和国、南非、巴西和其他地方的服务器获取非法访问信息

和机密数据，集团主要成员之一多纳戈尔将犯罪所得转移至中国，阿里征集比特币为ISIL提供资金支持[15]。基于暗网犯罪的无国界性和暗网网站服务器全球分布的复杂性，为打击暗网不法活动之需要，各国应通过订立双边、多边与地区合作协议建立共同打击暗网犯罪的国际合作机制，积极建构治理暗网犯罪国际体系，强化网络恐怖主义情报交流与执法合作，加快暗网新站点的数据挖掘、发现和治理进程。

（四）建立以比特币为代表的虚拟数字货币金融监管体系

暗网加密交易的实现与虚拟数字货币这一从区块链技术衍生出来的金融应用密不可分。由于契合了暗网的匿名性、秘密性、匿踪性特点，虚拟数字货币成为暗网交易唯一可被接受的支付方式。以占总市值46.66%比特币支付为例，它可直接由付款人转移到收款人，而不涉及第三方金融机构或非银行汇款机构，具有交易信息的加密“安全性”。因此，暗网上遍布以比特币为代表的虚拟数字货币兑换服务，兑换商收到匿名买家的现金存款后，将现金兑换成比特币，然后转入买家在暗网站点的账户，从中抽取一定数量佣金。近年来，国外利用暗网虚拟数字货币从事非法汇款业务、洗钱和恐怖主义融资的案例增多，加之最近美国联邦法院判例确认比特币是华盛顿特区《货币传输法》所涵盖的“一种货币”，对比特币法定货币性质的认可将导致利用比特币洗钱风险的增加，但同时也为暗网非法站点比特币交易从业人员“洗钱”罪名的成立增加了判例支持。但如果将比特币作为一种“商品”或类货币看待，对暗网比特币兑换商诉以“洗钱”罪名则存在一定的法律障碍，类似于采取我国“非法经营”的罪名显然更合适。针对虚拟数字货币反监测性和匿名性的特点，在技术方面，应加快研究区块链分布式账本记录的交易数据写入方式，通过技术手段从中发现真实的交易对手信息；在监管制度方面，在国内2013年出台的《中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会关于防范比特币风险的通知》基础上，可通过正式金融监管立法将以比特币为代表的虚拟数字货币纳入监管框架，要求比特币集中交易平台按照金融机构反洗钱标准，履行安全风险申报和疑似洗钱报告义务，令集中交易人买入、卖出比特币实名、留痕、可追溯，同时加强与美、英、日、韩等比特币金融交易平台最为集中的国家之间的刑事司法合作，共同探索暗网支付工具反洗钱国际合作机制。

[参考文献]

[1]John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath, Jana Shakarian and Paulo Shakarian. Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence[J]. The Cyber Defense Review, 2016(2).

[2][7]匿名者.深网 Google搜不到的世界[M].北京：中国友谊出版公司，2016：21，127.

[3]Hsinchun Chen, Edna Reid, Joshua Sinai, Andrew Silke, Boaz Ganor. Terrorism Informatics[M]. Springer Publishing Company, 2005：2.

[4]丹尼尔·德雷舍.区块链基础知识25讲[M].马丹，等，译.北京：人民邮电出版社，2018：155.

[5][10][15]Sesha Kethineni, Ying Cao, Cassandra Dodge. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes[J]. Am J Crim Just, 2018(43).

[6]Jamie Bartlett. The Dark Net [M]. Windmill Books Ltd, 2015：2.

[8]亚历克斯·皮盖惹.犯罪学理论手册[M].吴宗宪，译.北京：法律出版社，2019：26.

[9]Grinberg, R. Bitcoin: An Innovative Alternative Digital Currency[J]. Hastings Science & Technology Law Journal, 2011(4).

[11] [14]Gabriel Weimann. Terrorist Migration to the Dark Web[J]. Perspectives on Terrorism, 2016(3).

[12]刘建宏.新禁毒全书（第六卷）外国禁毒法律概览[M].北京：人民出版社，2015：24-31.

[13]Oz Sultan. Combatting the Rise of ISIS 2.0 and Terrorism 3.0[J]. The Cyber Defense Review, 2017(3).

[责任编辑：戴庆瑄]