浅议利用“暗网”技术犯罪的防控对策

刘 烽

（广州市公安局网络警察支队，广东 广州 510030）

摘 要 相对于众所周知的因特网，“暗网”作为近年新兴的网络技术，它具有匿名性、隐蔽性、复杂性等特点。Tor作为“暗网”的主流访问工具之一，了解其规模与使用情况，对探索整个“暗网”空间资源具有重要意义。另外利用“暗网”发布信息风险低、成本少，使“暗网”成为了敌对势力、犯罪分子的一种新型工具，给案件的侦破增加了难度，违法犯罪有不断上升之趋势。本文从分析“暗网”的技术、现状出发，提出了相关犯罪的防控对策。

关键词 “暗网” 网络安全 防控

引言

在学术界，“暗网”的概念并没有一个明确的定义，术语“Dark Web”和“Darknet”经常被混用指“暗网”。互联网是一个多层结构，“表层网”处于互联网的表层，能够通过标准搜索引擎进行访问浏览。藏在“表层网”之下的被称为“深网（Darknet）”。而“暗网（Dark Web）”通常被认为是“深网”的一个子集，且需要借助特殊浏览器才能访问。如图1所示。

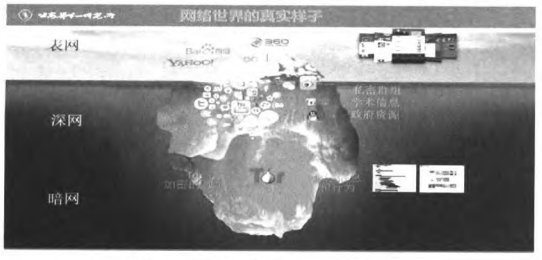

图1 网络世界的真实样子

1 Tor的现状

Tor（洋葱路由）是世界上最强大的隐私和在线自由工具。根据维基百科得到Tor网站的分类比例：暴力资讯0.3%、武器0.8%、黑客资讯1.8%、非法色情2.3%、极端主义资讯2.7%、毒品资讯8.1%.....

2 “暗网”犯罪的特点

2.1 高匿名性、去中心化、技术复杂

“暗网”使用分布式、多节点数据访问方法和多层数据加密来为每个数据包设计加密的IP地址以进行通信。要获得“暗网”在线记录，必须破解“暗网”使用的加密系统。Tor网络分布于全球各地有上千个中继节点，使其实现了彻底的去中心化；对于安全性，在密码学层面上，是无法被破译的。

2.2 资金交易方式匿名性、去中心化

“暗网”与比特币的“契合点”，很大程度来源于两者高度重合的匿名性特征，“暗网”提供匿名交易的平台和用户，比特币提供匿名的资产流通的方式。由于比特币采用去中心化的节点支付方式，并使用密码学的设计来确保货币流通各个环节的安全性，使得比特币无法得到有效的人为控制，不受传统业务渠道的监控。

2.3 跨区域性、跨国性特征明显

“暗网”网络由互联网上自愿运行Tor等工具的节点组成。具有跨越国家地域，在世界某一角落建立的“暗网”网站可以向任何国家或地区的“暗网”用户传播信息，而监管机构很

难追踪网站服务器和访问者的真实位置及身份。

2.4　意识形态混乱，犯罪形态多样化

“暗网”本身是由一群自由派和无政府主义者组建的，大多人在“暗网”上发表一些极端的言论，对社会的秩序稳定造成了极大的影响。另外有美国政府刻意地推波助澜所致。如香港的2014年“占中”事件及2019年借“修例风波”引发的暴乱事件。

2.5　犯罪数量、人群低龄化趋势不断上升

可以预计，“暗网”犯罪随着新技术和网络技术的发展，它给社会带来的潜在危害必然会不断增加。当前“暗网”用户中90后的群体已达到47%，00后占到了8.6%。在一起案件中接触“暗网”的用户多为25岁以内，其中最小仅14岁。“暗网”用户呈现低龄化趋势。据调查，广东访问“暗网”用户的比例占全国人群中最多，约21%，且有上升的趋势。

3　防止暗网犯罪的难点

3.1　高匿名性，监管难

Tor是属于一个匿名性极其强大的浏览器，其主要特征是采用了洋葱路由加密网络技术。当用户基于Tor访问“暗网”时，用户的路径会随机经过多个中继连接，而且每一次都是变化的，没有任何一个中继或服务器能够获悉完整的连接痕迹，在互联网上有着绝对的匿名性，从而导致他人无法追踪到用户的具体位置，监管极大。

3.2　货币交易的安全性监管难

比特币的去中心化、匿名、不可追踪、不被监管的数字货币会让技术犯罪形成一个闭环，贩毒、洗钱和恐怖主义等大行其道，并消失于无法解开的比特字节中。虽然区块链的账本是公开的，比特币钱包从理论上也是可以追踪的，但是在“暗网”多个平台中，都设置相应的风控策略，使得常规的传统资金流追踪手段无法使用，安全监管难。

3.3　跨区域性、跨国性的犯罪难查处

使用“暗网”者分布于全球各地，而涉案嫌疑人的犯罪链条涉及国内外，具有跨地域性，国际化。但由于各国政策、法律、制度和技术上认知等存在差异，“暗网”市场的卖家、买家和管理员都处在不同的司法管辖区。执法机构在打击“暗网”市场方面面临的重大挑战是找到市场的服务器，这些服务器通常位于其他国家，一般要数月的监测才能确定其位置。

3.4　难发现、难取证、难起诉

由于“暗网”通信具有节点发现难、服务定位难、用户监控难、通信关系确认难等特点，利用传统技术手段不易突破对“暗网”的侦察，在技术等多方面仍存在不小难度，致使相关职能部门极难发现和侦查。另外，“暗网”的取证存在很多挑战，如在暗网环境下，想定位指定的证据是极其困难的，同时网络传输数据是加密的。对此新型网络犯罪存在着侦查难、取证难、起诉难。

4　防范利用“暗网”犯罪的对策

4.1　加大宣传力度，打造网络安全生态

政府部门充分利用各种媒体、网络浏览入口、搜索入口、应用通道、终端主页扩大投送范围。通过定期曝光、案件通报、新闻通稿和新闻发布会提升宣传频度。‘暗网’不是‘法外之地’和‘避罪天堂’，充分揭示“暗网”的实质，减少“暗网”滋生发展的民众土壤，全力营造和形成健康良好的互联网生态氛围。

4.2　组建联合执法机构，加强国际间的交流合作

一建立联动合作机制。针对当前新型网络犯罪案件涉及领域广、隐蔽性强等情况，网警与其他警种应加强沟通协调，建立完善信息共享、数据共用新机制，提升对新型涉网违法犯罪的打击能力，形成网上网下一体化打防管控模式。二建立警企协作机制。深化与电信运营商、金融监管及第三方支付平台的沟通协作；加强与全国知名的互联网企业、高科技信息产业公司的战略合作，建立常态化信息共建共享共用协作机制，以最前端的技术支持服务公安机关打击防范“暗网”犯罪工作。三加强国际间警务交流合作。2015年始，欧美就成立了专门打击网络犯罪的“联合执法机构”，欧洲刑警组织还成立“暗网小组”，其主要职责是负责对“暗网”网络犯罪行为的预警和打击。

在我国，由于体制滞后，可学习借鉴欧美国家打击涉“暗网”犯罪活动的经验，完善制度，加强国际合作，积极推进建立全球范围内应对“暗网”网络犯罪的综合性国际法律和机制，加强与联合国相关机制、议题之间的互动和协调。

如：2016年6月，北京市公安局根据美国方面的通报，成功侦破了我国首例利用“暗网”传播儿童淫秽信息的犯罪案件，抓获了8名犯罪嫌疑人。

2017年7月，美国与欧洲刑警组织、荷兰、泰国等参与了打击“暗网”黑市行动，一举捣毁了当时全球范围内规模最大的黑市交易网站“阿尔法湾”等等。

4.3　加强技术人才培养及技术手段建设

—加强专业队伍的建设。与北京、上海等超大城市相比，在案件数量相当的情况，广州网警队伍明显不足，面对新型网络犯罪力不从心。必须树立高科技犯罪需要高科技人才队伍与技术手段应对的理念，建立打击新型犯罪研究中心，成立打击新型犯罪专业队伍。二加强专业人才的培养。网络安全技术是应对网络威胁的最直接、最有效手段。广州市局虽在全市公安中挑选并培训了多批次网络技术骨干，但仍远远不够。建议一方面采取外部聘请优秀专业人才的方式，充分利用外部先进的网络安全与侦查技术，以点带面培养更多专业技术人才。另一方面，采取走出去的方式，学习借鉴国外、国内同行管理和打击“暗网”犯罪的先进技术经验为我所用。三加强技术手段和专业设备的建设。在打击“暗网”犯罪中，技术、制度等多方面仍存在不小难度。应加强政府与企业在“暗网”技术上的合作，组织展开“暗网”治理技术专项工程攻关研究，研发出专用的“暗网”搜索引擎，用于探测+分析“暗网”的工具，具备监测、发现、调查能力、取证等功能的新型侦查系统和设备，提升办案效率。

4.4　主动出击，发现“涉暗”情报

—公安机关依托云计算、大数据分析、“智慧新侦查”技术，充分利用警综平台等信息资源，从中发现、提炼、整合利用“暗网”平台信息网络犯罪的线索。二公安机关加大网上信息巡查力度。一方面加强对本地网站、交互式论坛、博客等巡查搜索，建立完善的预警系统；另一方面，Facebook、推特等网站则是挖掘“暗网”资源地址的重要渠道，对已知Web站点内容进行深度爬取、分析，综合研判。

4.5　借鉴国外的侦查方法

4.5.1　“卧底”捣毁第二代“丝路”

“暗网”技术是把“双刃剑”，2011年2月，第一代“丝绸之路”横空出世。2013年，“丝绸之路”被美联邦调查局关闭；仅仅几个月后，“丝绸之路2.0”卷土重来；在“丝绸之路2.0”创建之初，警方就已打入其内部管理层。在“丝绸之路2.0”成立一周年的前一天，美警方在美圣弗朗西斯科市逮捕了本特霍尔，并捣毁了该网站。

4.5.2　明网上露馅，主犯落网

“阿尔法湾”的创办者先后使用“Alpha02”和“Admin”（管理员）两个网名，曾一度使用一个hotmail邮箱发送致新用户的欢迎邮件，而这个邮箱经调查属于1991年10月19日出生的加拿大人亚历山大·卡兹。2017年7月5日，卡兹在曼谷正用笔记本电脑以管理员的网名接入“阿尔法湾”，并在论坛上答复用户发问，当场被泰国警方拘捕。

4.5.3　查洗钱，发现执法者监守自盗

“暗网”黑市通常使用比特币进行交易，然而，就像追查逃税或其他类似调查一样，从“暗网”转移出来的资金和资产流向可以给警方提供追踪线索。美调查局在追查用比特币等虚拟币洗钱的犯罪嫌疑人时，发现了“丝绸之路”网站案件中美调查组成员肖恩布·里奇斯监守自盗总价值约82万美元的比特币。

4.5.4　循邮路抓获毒枭

虽然“暗网”技术非常复杂，但“暗网”上的毒品交易却要依靠邮政系统或普通邮差送到买家手上。邮筒和邮局是执法人员的主要监管地点之一。2012年9月，美联邦调查局和邮政总局在西雅图从史提芬·萨德勒及女友中截获多包海洛因。警方分析，怀疑史提芬·萨德勒是“丝绸之路”网站名为“诺德”的最大毒品卖家。后警方通过技术跟踪及长时间调查取证，2013年7月将其抓获归案。

4.6　完善政企对接和协作机制

—落实等级保护备案和安全测评。深化

“一案双查”制度，推动建立健全网络安全责任制、问责制及网络运营主体责任，增强全社会维护网络安全的防护意识和主体责任意识，落实政企事业单位的重要领域信息系统安全体系“同步规划、同步建设，同步使用”，努力实现社会共治。二加强对“翻墙”工具的监管。协调网信、通信管理等互联网管理部门，深入排查安全隐患和管理漏洞，通过以源头治理和依法打击相结合、管理措施和技术防控相结合的方式，清理VPN违法违规使用单位，打击问题突出的VPN服务提供商，整顿违法违规的网络平台和接入服务商、信息服务商，严格落实属地管理责任制，构建新的网络管控阵地。三严打黑灰产业。围绕斩断“信息支撑、技术支撑、工具支撑、平台支撑”犯罪链条，保持对网络黑灰产业链条犯罪的严打高压态势。企业需要建立常态化审查机制，实现事先预警、事中阻断，事后修补漏洞；打击网络黑产是一个综合的社会化的工程，借助AI、大数据等新技术打击网络黑产，实现跨行业、跨政企联防联控，打破信息孤岛。

4.7　强化寄递物流的监管，加强对比特币等监管

网络贩枪、贩毒等违禁品，寄递物流在整个犯罪链条中扮演“最后一公里”的角色。必须做到：一要严格落实“五个百分百”制度（即寄递实名制、先验视后封箱、通过X光机安检、持证经营、从业人员登记等）；二要提高从业人员和加盟商的准入门槛；三要加强职业培训教育；四是加大五金、化工行业的管控力度；五要强化监督与落实。

比特币作为区块链技术的成功应用，在全部数字货币中居于核心地位。因此被广泛应用于洗钱、非法交易、匿名交易等。2013年12月，中国人民银行等五部委发布关于防范比特币风险的通知。其中规定比特币的性质应当是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。去年11月，央行对上海地区虚拟货币相关活动开展专项整治，对涉嫌违法犯罪的，可向公安机关报案。

4.8　强化证据意识

“暗网”的取证跟同其他网络取证一样，需在互联网取证的方法框架内进行，电子证据是惩治计算机网络犯罪的关键证据。针对“暗网”访问工具、网络环境等特殊性，对特定的站点制定单独的数据爬取规则和方法，做好对应的操作记录。对爬取和收集的各类文件，参照取证任务的目标进行数据分析、处理，以电子证据为突破口破解打击犯罪难题。

4.9　完善相关法律，提高震慑力

一加强“暗网”安全的立法规制。在全面落实《网络安全法》的同时，国家立法机关和执法部门还需加快推进“暗网”安全的立法规制。二《反恐法》的施行有助于加强防范和打击恐怖主义，然而《反恐法》中并未明确界定网络恐怖主义，打击网络恐怖主义缺少完善的法律保障。三加速推进《网络安全法》配套规定出台，明确司法认定情节。刑法285第3款对VPN的定性欠详尽。为此，应尽快完善法律法规，提高法律的震慑力。