社会安全研究

国外打击涉“暗网”犯罪的经验及启示

于 世 梁

(江西行政学院,江西 南昌 330108)

摘 要:“暗网”是必须借助专用工具才能访问的网络,它可以满足用户匿名访问互联网的需求,但也成为贩毒、走私、色情、洗钱、售假及从事恐怖活动的重要场所。“暗网”的访问匿名性、服务隐藏性和交易隐蔽性,增加了抓捕犯罪分子、摧毁非法网站、打击非法交易的难度。尽管如此,美欧等国家通过综合运用各种技术、成立专门执法机构、加强国际执法合作等措施,在打击涉“暗网”犯罪方面取得了显著成效,其经验值得我们学习和借鉴。

关键词: 互联网; 暗网; 洋葱路由; Tor; 暗网犯罪
中图分类号: D616 **文献标识码**: A **文章编号**: 1008 - 2433(2019)04 - 0005 - 07
DOI:10.16231/j.cnki.jhpc.2019.04.001

依法严厉打击涉“暗网”等新型犯罪活动,是公安部“净网 2019”专项行动的重点任务之一。“暗网”(Dark Web)是与互联网中的普通网络——“明网”(Surface Web)相对应的一种网络形态,它必须借助专用工具才能访问。“明网”与“暗网”最大的不同是,“明网”中提供的网络服务(如各类网站、邮件服务、论坛等)和网络访问者计算机的 IP 地址都是显现的(即 IP 地址不会被隐藏),通过 IP 地址可以确定网络使用者的真实身份。而“暗网”由于采用了匿名访问机制,网络使用者不会在互联网中留下自己的身份信息。“暗网”的匿名性在很好地满足人们匿名使用互联网的同时,也给违法犯罪活动提供了新的网络空间。

一、“暗网”已成为违法犯罪活动的重要场所

“暗网”的诞生源于对网络通信保密的要求,它广泛应用于军事情报部门。但是,任何技术都是一把“双刃剑”,正是由于“暗网”的匿名性,使其在 2004 年后很快成为走私、贩毒、售假、传播不良信息,以及从事恐怖主义活动的重要场所。

(一)“暗网”为违禁商品买卖提供了重要平台

毒品、非法枪支、各种假证、被盗信用卡、计算机病毒、黑客工具、公民个人信息等,都是不允许公开销售的,而“暗网”为这些商品的买卖打开了方便之门。2010 年,美国人罗斯·乌尔布莱特(Ross Ulbricht)在“暗网”中建立了名为“丝绸之路”(Silk Road)的非法交易网站,销售毒品、枪支、儿童色情、伪造证件等违禁商品。从创建到被关闭的两年间,“丝绸之路”商品供应商遍布十多个国家,总交易额超过了 12 亿美元,乌尔布莱特也依靠收取的每笔交易的 10% - 12% 的佣金赚取了近 1 亿美元[1]。2013 年 10 月 1 日,美国联邦调查局(FBI)探员在旧金山将乌尔布莱特抓获,“丝绸之路”随即被关闭。2015 年,乌尔布莱特因从事经济犯罪、洗钱、贩毒等被判处无期徒刑[2]。2013 年 11 月,就在“丝绸之路”被查封一个月后,“丝绸之路 2.0”重新上线,其创建者布莱克·本特霍尔(Blake Benthall)曾是一名供职于太空探索技术公

收稿日期: 2019 - 03 - 21

作者简介: 于世梁(1964—),男,江西余江人,中共江西省委党校(江西行政学院)文化与科技教研部副教授,主要研究方向:网络信息安全。

司(SpaceX)的飞行软件工程师。2014年11月6日,本特霍尔在旧金山被警方抓获,“丝绸之路2.0”被关闭[3]。

“丝绸之路”被查封后,2014年美国人亚历山大·卡兹(Alexandre Cazes)在“暗网”上创建了非法交易网站“阿尔法湾”(AlphaBay),主要经营毒品、非法药品、枪支弹药、黑客工具、各种伪造证件、儿童色情等违禁品。在2017年被警方查封之前,“阿尔法湾”拥有4万卖家和20万客户,非法药品的交易条目超过25万条,身份证件、信用卡等的交易条目超过10万条,交易额达10亿美元[4]。2017年7月4日,“阿尔法湾”遭警方关闭,卡兹也在次日被泰国警方抓获,并在即将被引渡至美国前死于曼谷的一所监狱。

(二)“暗网”为非法信息传播提供了重要渠道

“暗网”中的色情、绑架、暗杀等非法信息也极为丰富。“暗网”中有一个名为“洛丽塔都市”(Lolita City)的网站,其中的儿童色情照片超过100万张,注册会员达1.5万名[5]。2011年10月,“匿名者”(Anonymous)黑客组织摧毁了“暗网”上一个名为“自由主机”(Freedom Hosting)的托管服务器,该服务器托管了40多个儿童色情网站[6]。

2017年7月,一名20岁的英国女模特被骗至意大利米兰后遭两名男子绑架。绑匪以30万欧元的价格在“暗网”上将其拍卖。据警方透露,绑匪为一名英国裔波兰人,是贩卖人口组织“黑色死亡团体”(Black Death Group)的成员,该组织以在“暗网”上拍卖绑架的年轻女性为“主业”[7]。

2018年6月9日,美国伊利诺伊大学(UIUC)中国访问学者章莹颖失联。美国联邦调查局在调查这起失联案件时,逮捕了嫌疑人伊利诺伊大学博士生勃兰特·克里斯滕森(Brendt Christensen)。调查发现,克里斯滕森曾在2017年4月访问过“暗网”中一个名为FetLife的网站。而FetLife网站是一个以绑架、施虐为主题的社交网站,该网站有超过三千万张图片和四万段录像,注册用户达600多万人[8]。

(三)“暗网”为突破网络封锁提供了重要手段

互联网传播的信息良莠不齐。对网站内容进行审查,删除关闭违规网站,过滤、屏蔽不符合本国法律法规的国外网站是国际上的通行做法,包括美国、加拿大、欧盟等都是如此。为了防止国外不良网络信息流入国内,通常会在一个国家的互联网入口处设置防火墙,实现对国外不良信息网站的过滤和屏蔽[9]。

对于那些试图浏览被过滤的境外网站的人,“翻墙”是最常用的方法。目前在我国,“自由门”(Freegate.exe)“逍遥游”(FreeU.exe)等境外软件公司开发的几款软件,是最常用的“翻墙”软件[10]。但是,由于“翻墙”软件中使用的代理服务器地址是相对固定的,因此“翻墙”行为很容易被控制。不仅如此,通过“翻墙”访问国外网站,已经触犯了一些国家的法律法规。例如,我国《计算机信息网络国际联网管理暂行规定》明确规定,任何单位和个人不得自行建立或者使用其他通道进行国际联网。

而通过使用“暗网”软件(如Tor浏览器)来访问境外网站,可以很好地隐藏网络访问者的计算机IP地址从而躲避执法机关的监管,所以成为突破网络封锁的重要手段。与“明网”网站的域名大多以.com、.net等结尾不同,Tor系统中的网站域名都是以.onion结尾的,所以使用普通的浏览器无法访问“暗网”中的网站,用户计算机需要安装一个专门的访问“暗网”的软件。Tor浏览器(Tor Browser)是目前最流行的“暗网”访问软件,其全球下载量达到了每年近5000万人次[11]。

(四)“暗网”为恐怖组织活动提供了重要场所

为了抑制恐怖组织的快速发展,预防暴力恐怖事件的发生,国际社会加大了对恐怖组织的监控,大批涉及恐怖主义内容的社交网络账号和网站被关闭。为了躲避追踪和监控,恐怖组织已经开始通过“暗网”来发布信息、招募人员以及组织和策划恐怖袭击活动。

2015年11月13日晚,伊斯兰国(IS)组织策划实施的法国巴黎市系列恐怖袭击事件造成重大人员伤亡。事件发生后,“匿名者”黑客组织对与IS有关的网站进行了大规模的网络攻击,数百个与IS有关的网站被关闭。与此同时,国际社会也加强了对互联网上与IS相关内容的监控,与IS有关的所有新域名刚被注册就被删除。2015年11月15日,即巴黎爆炸案发生的两天后,IS发布其官方网站“Isdarat”向“暗网”转移的消息,IS的哈耶特媒体中心(Al-Hayat Media Center)随即给出了如何在“暗网”联系IS的方法[12]。

“暗网”也是恐怖组织和恐怖分子购买枪支弹

药等物资的重要平台。制造2015年11月13日巴黎恐怖袭击事件的恐怖分子所持有的4把自动步枪，被证实是从“暗网”上购买的。2016年7月22日，德国慕尼黑奥林匹亚购物中心枪击案的制造者也从“暗网”上购买了一把半自动手枪和250发子弹[13]。

恐怖组织利用“暗网”开展活动，给国际社会跟踪打击恐怖主义造成了巨大障碍。2016年8月17日，联合国专家组在向联合国安理会提交的报告中指出，“伊斯兰国”“基地”等极端组织使用“暗网”招募成员，策划发动袭击，其在“暗网”上的加密信息即便是水平最高的安全机构也难以破解，并提醒各国政府对此保持高度警惕[14]。

二、“暗网”给全球网络空间治理带了重大挑战

为了保护军方和情报人员在互联网上能够安全通讯而不被追踪，20世纪90年代美国政府和军方启动了匿名网络(“暗网”)研究项目。1996年5月，美国海军研究实验室(NRL)资助的三位科学家提出了一种被称为“洋葱路由”(Tor: the Onion Router)的匿名网络技术，2003年10月，第二代“洋葱路由”问世，使匿名网络成为现实。“暗网”的诞生，给网络空间治理带来了新的重大挑战。

(一)“暗网”的访问匿名性，增加了抓捕犯罪分子的难度

用普通方式访问互联网(“明网”)，客户端计算机的IP地址会被途经的网络设备和服务器内部部署的监控程序记录下来。通过IP地址，用户的身份和网络踪迹可以被追溯。“暗网”则不同，它采用了分布式、多节点数据访问和多层数据加密技术。分布式技术可以把网络中安装了特定软件(如Tor软件)的普通计算机变成信息传递的中继节点；多节点技术使得信息传递从起点到终点需要经过多个(一般为3个)随机选择的中继节点；多层数据加密能够为客户端发送的数据包进行多层加密(一般为3层)。因此，当用户访问“暗网”时，经过多层加密的数据会在随机选择的多个不同的中继节点间跳转，任何一个中继节点都无法获得完整的连接路径，接收端也无法判断这个信息的来源，访问者不会留下能够标明自己身份的信息，从而可以实现完全的匿名访问。多层加密机制是“暗网”能够实现匿名访问的重要技术之一。由于对数据进行多层加密好像给每一个数据包加上了“洋葱”(Onion)一样的层层保护，“洋葱路由”(the Onion Router)由此得名。

“暗网”的访问匿名性，增加了对网络访问者进行溯源追踪的难度，这意味着执法部门即便发现了网络犯罪活动的线索，也很难确定嫌疑人的真实身份。2013年10月，“丝绸之路”网站的创始人罗斯·乌尔布莱特能够被联邦调查局成功抓获，并非是他在“暗网”上露出了“马脚”，而是因为他在“明网”上留下了太多的网络行踪。罗斯·乌尔布莱特在公开场合化名约什·特雷，职业为一名外汇交易员。2013年7月，在确定“丝绸之路”网站的服务器位于冰岛后，联邦调查局特工侵入了服务器系统，并盗用“丝绸之路”员工的网络身份与网站管理人员进行联络和交流，希望以此来查出创始人的真实身份，但一直未能取得突破。直到罗斯·乌尔布莱特在“明网”上发布新的招聘启事，使用了自己完整姓名的邮箱(rossulbricht@gmail.com)来接收简历时，警方才最终确定了他的真实身份并将其抓获。

(二)“暗网”的服务隐蔽性，增加了摧毁非法网站的难度

网络服务(net Server)指互联网上的各种应用，如WEB(网站)、电子邮件、即时通讯、网络论坛等等。在“明网”中，提供网络服务的计算机IP地址或域名(IP地址的另一种表示方式)都是显现的。因此，网络服务必须合法合规，否则将被执法部门取缔或关闭。

“暗网”则不同，Tor网络使用了一种被称为隐藏服务(Hidden Service)的技术，任何人都可以以匿名方式发布各类网站和其他应用服务，而不用担心会暴露自己的身份信息。此外，为了躲避执法部门的追踪，网络服务提供者还会经常将网站托管到不同的服务器上，这大大增加了执法部门确定网站服务器位置并将其摧毁的难度。

2006年，“暗网”中第一个成熟的非法交易网站“农夫市场”(The Farmer's Market)上线。据美国缉毒局(DEA)相关资料显示，“农夫市场”的客户遍及美国50个州及其他34个国家和地区，每年的营业额超过了100万美元。“农夫市场”上线后不久，美国警方就发现了该网站，但却一直无法确定网站服务器的具体位置。直到6年后的2012年4月，美国缉毒局与荷兰等地警方合作，逮捕了以

荷兰人马克·威廉姆斯(Marc Willems)为首的不同国籍的8名组织者,“农夫市场”才被警方彻底关闭[15]。

(三)“暗网”的交易隐蔽性,增加了打击非法交易的难度

货币结算,是商品交易的重要环节。传统的货币结算,由于需要通过银行金融系统来完成,所以商品交易很容易受到监管,交易双方的身份也很容易被确定。毒品、非法枪支等违禁商品的非法交易是“暗网”的重要内容。“暗网”的访问匿名性,不仅使得买卖双方的真实身份都处于隐藏状态,而且数字货币的出现,又很好地解决了通过银行支付受到金融体系监管的问题,这大大增强了“暗网”交易的安全性,加大了执法部门打击非法交易的难度。

目前,在“暗网”中进行非法交易,基本上都是使用虚拟的数字货币来进行支付结算的,其中比特币(Bitcoin)是最常用的虚拟数据货币。例如,“丝绸之路”指定的唯一交易货币就是比特币。比特币诞生于2009年,是一种去中心化的分布式虚拟货币,使用匿名的点对点交易。个人可以通过“挖矿”或通过接受比特币付款来获取比特币。当在交易中使用比特币结算时,比特币的交易情况将被记录在“公共分类账簿”(区块链)中。由于记录在“公共分类账簿”中的比特币交易信息是交易双方的比特币地址而非特定的比特币,且进行比特币交易需要使用个人私钥进行验证,这大大增强了比特币支付的安全性。此外,除了使用比特币作为“暗网”交易的主要支付货币,近年来其他虚拟数字货币如以太币(Ether)和门罗币(Monero)等,已成为“暗网”非法交易支付的新选择。

三、国外打击涉“暗网”犯罪的经验及对中国的启示

日益猖獗的涉“暗网”犯罪活动,引起了国际社会的高度关注。尽管对“暗网”的管控有很大的难度,但美欧等国家通过一系列的措施,在打击涉“暗网”犯罪中取得了显著成效,其许多好的做法和经验,值得我们学习和借鉴。

(一)重视对“暗网”犯罪技术的研究

网络技术是打击网络犯罪最直接最有效的手段。如前所述,“暗网”访问的匿名性,能够隐藏计算机的IP地址,使执法人员很难确定“暗网”访问者的真实身份。用Google等搜索引擎也很难搜索到“暗网”中的内容。为了破解这些难题,美国政府与研究人员和网络安全专家合作,不断开展“暗网”去匿名化和识别隐藏服务的技术研究,以帮助执法机关收集“暗网”信息,确定“暗网”访问者。

2014年,美国国防部先进研究项目局(DARPA)启动了一个名为Memex的研究项目,用于提高对“暗网”隐藏内容的搜索能力,以帮助执法部门尽可能多地收集“暗网”中的信息,发现“暗网”中的各种违法犯罪行为。2015年4月,DARPA对外公布了Memex项目的研究进展情况。通过Memex技术,可以为执法人员查找人口贩子、毒品贩子和恐怖分子等特定人群提供帮助。

针对“暗网”访问的匿名性,美国联邦调查局开发了一个名为“网络调查技术”(NIT: Network Investigative Technique)的工具。NIT是一个基于Flash的应用程序,它能绕过“暗网”对访问用户的匿名保护,获得访问者计算机的IP地址和计算机注册信息(如MAC地址:计算机的物理地址)。但利用NIT技术的前提是必须先控制“暗网”中的网站服务器并植入NIT代码,再使用“钓鱼”执法来获得访问者计算机的IP地址等信息。

2014年8月上线的Playpen网站是“暗网”中一个专门提供儿童色情信息的网站,到2015年3月被美国联邦调查局查封前已发展成为全球最大的儿童色情网站,拥有21.5万名注册用户,内含2.3万个以上的儿童色情图像和视频的链接。2015年2月,美国联邦调查局控制了这个网站,并把该网站的数据迁移到自己的服务器上继续让其运行。在2015年2月20日至3月4日期间,有超过10万名用户访问了Playpen网站。美国联邦调查局使用NIT技术,获取了超过1300名用户的计算机IP地址,其中的137人遭到逮捕[16]。

(二)灵活运用各种网络技术手段

开发针对“暗网”的去匿名化和识别隐藏服务技术,是抓捕涉“暗网”犯罪嫌疑人和查封“暗网”非法网站的重要手段。但从目前使用效果来看,这些技术本身还存在一定的局限性。因此,灵活运用各种传统的技术,是国外执法部门侦破涉“暗网”犯罪案件的有效手段。

利用安全漏洞进行渗透、依靠罪犯的错误和失误确定他们的身份、通过卧底假扮顾客收集信息等是国外执法部门打击涉“暗网”犯罪活动的重

要手段。例如，在调查“阿尔法湾”的过程中，从2016年5月开始，执法人员假扮顾客，从“阿尔法湾”上购买毒品、假身份证等物品，来搜集网站的相关信息。2017年6月20日，荷兰警方抓获了非法交易网站“汉莎市场”(Hansa Market)的两名德国行政人员，在缴获的大量资料中发现了“阿尔法湾”的蛛丝马迹。警方发现，“阿尔法湾”网站管理者经常使用“Alpha02”和“Admin”两个网名，并通过微软hotmail邮箱收发邮件。正是这些线索，帮助执法人员确定了“阿尔法湾”创建者亚历山大·卡兹的真实身份。2017年7月5日，卡兹在曼谷被泰国警方逮捕时，正以“Admin”的网名接入“阿尔法湾”服务器，并在论坛上回答用户提问[17]。

“钓鱼”执法是国外执法部门抓捕涉“暗网”犯罪嫌疑人的另一个重要手段。执法部门在控制了某个非法网站后往往并不急于将其关闭，而是让其继续运行一段时间。在网站被控制期间，执法人员利用前面介绍的“网络调查技术”(NIT)或冒充网站管理者与访问者联系来抓捕其他的犯罪嫌疑人。“儿童游戏”(Childs Play)是“暗网”上一个恋童癖论坛，由加拿大人本杰明·福克纳(Benjamin Faulkner)在2016年4月创建。截至2017年9月被澳大利亚警方关闭时，该论坛的用户人数超过了100万。2016年，福克纳在美国弗吉尼亚因性侵一名女童被警方抓获，在对福克纳进行调查时发现他是Childs Play的创建者，Childs Play随后被澳大利亚警方接管。在网站被接管期间，澳大利亚警方与美国、欧洲警方保持合作，冒充福克纳与其他“暗网”访问者继续联系。在近一年的“钓鱼”执法中，警方发现了大约100名儿童色情图像和视频的制作者和提供者[18]。

(三)成立专门机构进行组织协调

涉“暗网”犯罪活动涉及贩卖毒品、买卖非法枪支、贩卖人口、儿童色情、绑架暗杀以及极端恐怖活动等各个方面，这就使得打击涉“暗网”犯罪需要各相关部门的大力配合和共同协作。“暗网”访问的匿名性、信息的隐秘性和服务的隐藏性，决定了对“暗网”的管控需要专业技术人员的参与和支持。为此，成立针对“暗网”犯罪的专门执法机构，不仅能够组建更专业的队伍，而且能够提高各部门间的信息资源共享和协同行动能力。

以英国为例。2015年，英国政府成立了“联合执法机构”，其主要职责是负责对“暗网”网络犯罪行为进行预警和打击，包括“暗网”中针对儿童的各种犯罪，以及通过“暗网”贩卖毒品、贩卖妇女、贩卖枪支等所有可能涉及“暗网”的违法犯罪活动[19]。随着越来越多的犯罪活动向“暗网”转移，2017年8月，英国国家犯罪局(NCA)成立了“暗网情报部”(Dark Web Intelligence Unit)，通过招募网络专家和“暗网”分析师，来帮助查找“暗网”中的非法交易和其他违法犯罪行为，并负责与其他网络情报和执法部门合作，共同打击“暗网”中的贩卖人口、儿童性虐待、武器交易和洗钱等非法活动[20]。

(四)加强国际合作形成打击合力

“暗网”由于不受空间地域的限制，给各国打击涉“暗网”犯罪带来了重大挑战。通过加强国际合作共同打击涉“暗网”犯罪活动，已经成为国际社会的共识。在过去几年间打击涉“暗网”犯罪的重大行动中，不同国家间的联合执法发挥了重要的作用。

2016年2月，德国安全部门和来自其他六个欧洲国家的执法人员共同合作，对“暗网”中的一个违法交易平台的操作人员和使用者展开了一次大规模的搜捕行动。在这次联合行动中，警方逮捕了涉及德国、立陶宛、俄罗斯、荷兰、法国、瑞士、波斯尼亚等国家的9名犯罪嫌疑人[21]。2017年7月，“阿尔法湾”被查封，也是由美国联邦调查局、美国缉毒局、欧洲刑警组织联合法国、荷兰、泰国、加拿大和英国等数十个国家的执法部门共同完成的。

2018年5月，欧洲刑警组织宣布成立“暗网小组”，以提高打击涉“暗网”犯罪活动的能力。“暗网小组”的成员来自28个国家的警方及部分国家的网络安全公司。“暗网小组”的成立，标志着打击涉“暗网”犯罪国际执法合作进入常态化，这对于更好地共享各国应对“暗网”犯罪威胁的策略、技术和信息，更有效地联合各国执法部门打击涉“暗网”犯罪活动将发挥积极的作用。

“暗网”扩展了全球范围内非法交易和犯罪活动的空间，我国也无法摆脱“暗网”犯罪带来的影响和威胁。在国内，已经出现了专门讨论“暗网”话题的论坛和贴吧，网上也有详细介绍访问“暗网”方法的教程和攻略。尽管目前还没有发现类似于“丝绸之路”“阿尔法湾”的大型的“暗网”非法交易中文网站，但已经有人开始通过“暗网”进

行色情信息传播和贩卖公民个人信息。

2016 年 3 月,北京市公安局接到公安部通报,美国国土安全部海关移民执法局在日常巡查中,发现有中国网民(IP 地址属于北京) 在境外网站发布儿童色情图片及视频。警方调查发现,在“暗网”一个英文论坛,某账号发布了大量儿童色情图像和视频。通过将技术手段与常规手段相结合,警方锁定了这个 IP 地址的嫌疑人北京某大学学生孙某。2016 年 3 月 13 日,警方在北京一小区将孙某抓获,在现场查获的电脑和移动硬盘中,发现了多达 3T 的色情图像和视频,其中儿童色情图像视频达 400G。据警方统计,孙某在“暗网”论坛中传播视频 100 多个,点击率高达 2 万多次[22]。

2018 年以来,在“暗网”中出现了多个售卖中国公民个人信息的帖子。2018 年 6 月 16 日,“暗网”上出现了售卖某招聘网站中国公民个人信息的帖子,涉及 195 万用户的求职简历;2018 年 6 月 19 日,有人在“暗网”上售卖某快递公司的用户数据,涉及包括寄(收) 件人姓名、电话、地址等在内的公民个人信息 10 亿条,全部打包售价 1 比特币;2018 年 8 月 28 日,有人在“暗网”上售卖某酒店 10 多个连锁店的客户数据,涉及客户的姓名、身份证号等信息约 5 亿条,以上信息以 8 比特币打包出售[23]。

在 2019 年年初公安部召开的“净网 2019”专项行动部署会上,公安部将依法严厉打击涉“暗网”等新型犯罪活动作为重点任务之一。这充分表明,“暗网”已经成为我国网络空间治理的重要领域。国外打击涉“暗网”违法犯罪的经验,对我国进行“暗网”治理有以下几点启示:

一是加强组织领导。尽管目前涉及中国公民的“暗网”犯罪活动还处于低发期,但可以预见,随着我国公安机关打击网络违法犯罪活动力度的加大,“明网”中违法犯罪活动的空间不断受到挤压,这必然会使网络犯罪活动不断向“暗网”转移。“暗网”在技术上的特殊性,也使得打击涉“暗网”犯罪将是一个长期的过程。因此,在我国网信部门和公安部门内部成立专门针对“暗网”犯罪的机构很有必要,这既有利于加强对打击涉“暗网”犯罪的组织领导,又有利于培养专业人才,锻炼专业队伍,积累实战经验。

二是加强技术研究。网络技术是实现“暗网”去匿名化和识别隐藏服务的最直接、最有效的手段。如前所述,美国执法部门已经开发出了“暗网”信息搜索技术(Memex) 和“暗网”去匿名化技术(NIT) ,这对于执法人员查找人口贩子,毒品贩子和恐怖分子等特定人群,确定犯罪嫌疑人真实身份提供了帮助。但是,这些技术目前只掌握在美国政府手中,其核心技术并没有对外公开。有鉴于此,国家有关部门应当组织国内网络安全研究机构和网络安全公司,联合开展“暗网”信息搜索和去匿名化技术的专项研究,不断提高我国“暗网”网络空间治理和打击涉“暗网”犯罪活动的技术能力。

三是加强国际合作。互联网的跨地域性,使得网络犯罪案件往往涉及多个国家,“暗网”更是如此。就我国而言,目前提供非法网络应用服务(如网站、论坛) 的托管服务器多隐藏在国外,这给摧毁非法网站,抓捕犯罪嫌疑人带来了很大的困难。涉“暗网”犯罪是一个全球性的问题,已经成为全球网络空间治理的重要内容,打击涉“暗网”犯罪的国际联合执法也已经成为一种常态。在这一背景下,我们应当充分利用好这些有利条件,拓展与其他国家网络执法的合作,积极参与国际社会打击涉“暗网”犯罪的联合行动,不断积累预防、打击涉“暗网”犯罪行动的实战经验,提高“暗网”网络空间治理能力。

参考文献:

[1]严言. 暗网是一个怎样的世界[N]. 国际金融报,2015 - 12 - 21(03).

[2]黄伟. 暗网世界的黑色犯罪[J]. 检察风云,2017(23):16.

[3]方言. 两大暗网黑市覆灭记[J]. 中国信息安全,2017(11):72.

[4]肖竟. 全球最大“暗网”黑市被关闭[N]. 青年参考,2017 - 08 - 02(06).

[5]杰米·巴特利特. 暗网[M]. 刘丹丹,译. 北京:北京时代华文书局,2018:146.

[6]搜狐. 美国国会研究服务局公布《暗网》报告[EB/OL]. https://www.sohu.com/a/199766846_99943379,2017 - 10 - 23.

[7]搜狐. 暗网到底有多可怕·被卖妙龄女成性奴逃脱曝真相[EB/OL]. http://www.sohu.com/a/163000596_174521,2017 - 08 - 08.

[8]崔光耀. 暗网追踪:暗流涌动的世界[J]. 中国信息安全,2017(11):59.

[9]李文洁.论“翻墙”现象与中国的网络监管[D].中国社会科学院研究生院,2011-04-23.
[10]官国静.典型翻墙软件的网络通信特征研究[J].信息安全与通信保密,2012(02):67.
[11]王佳宁.“暗网”对国家安全的危害[J].网络安全技术与应用,2016(09):10.
[12]肖洋.“伊斯兰国”的暗网攻势及其应对路径[J].江南社会学院学报,2017(01):21.
[13]云贺.怎样打赢暗网攻坚战[EB/OL].http://www.lwinst.com/cjgjzk201716/4902.htm,2017-08-04.
[14]李珊.阿尔法湾覆灭背后[N].华商报,2017-08-04(B1).
[15]陶短房.“暗网”从未消逝[J].方圆,2017(16):40-41.
[16]环球网.FBI通过儿童色情网站钓鱼执法 卧底调查还是助纣为虐[EB/OL].http://world.huanqiu.com/exclusive/2016-01/8442341.html?agt=1079,2016-01-25.
[17]刘峣.已成非法交易温床 世界各国协力打击 暗网深几许?[N].人民日报(海外版),2017-08-11(08).
[18]杨舒怡.澳大利亚:暗网钓鱼捣毁恋童癖论坛[EB/OL].https://news.china.com/internationalgd/10000166/20171009/31551103.html,2017-10-09.
[19]潘宏远,姚文文.英国成立机构专门打击“暗网”[N].人民邮电报,2015-12-14(07).
[20]王丹娜.暗网治理需各国执法协同联动[J].中国信息安全,2017(11):80.
[21]黎楸萍.德国等欧洲七国合作联手打击网络犯罪交易平台[EB/OL].http://www.cac.gov.cn/2016-03/03/c_1118219987.htm,2016-03-03.
[22]刘子珩.揭秘“暗网”第一案背后的暗黑世界[N].新京报,2016-11-25(A13).
[23]腾讯.信息泄露是2018年企业网络安全所面临的头号威胁[EB/OL].https://www.wshenm.com/2018tencents.html,2019-01-07.

(责任编辑:王利宾)

Lessons of Policing the Dark Web for China

YU Shiliang

(Jiangxi Administration Institute, Jiangxi Nanchang 330108)

Abstract: The dark web is the World Wide Web content that requires specific software, configurations, or authorization to access. It serves the need to access to the Internet anonymously, but also becomes a playground for illegal activities like drug trafficking, smuggling, pronography, money laundering, selling fake goods and terrorism. The anonymity and invisibility of services and trades make it difficult to trace criminal activities, destroy illegal websites or trades. Nevertheless, western countries have deployed all kinds of technologies, established law enforcement agencies and enhanced international law enforcement cooperation, from which lessons are worthwhile to learn for us.

Key words: World Wide Web; Dark Web; Onion Routing; Tor; Dark net crime