暗网犯罪与多元治理:挑战与出路

陈 璐
(河南财经政法大学 刑事司法学院, 河南 郑州 450044)

摘 要:暗网已成为犯罪聚集的隐秘之地。暗网犯罪使国家安全面临新的挑战,包括对国家军事安全构成重大威胁、为恐怖主义犯罪提供新的避风港、破坏国家金融秩序以及对公民人身安全产生巨大威胁等,而传统刑事司法手段打击暗网犯罪面临取证困难、侵犯他国司法主权等问题。治理暗网犯罪仅仅依靠传统刑事司法手段并不能奏效,必须建立专门的暗网犯罪监测部门以及"产—官—学"协同合作机制,加强公私部门信息共享,提高电子取证技术,同时还要积极寻求国际刑事司法合作。

关键词:暗网犯罪;国家安全;应对路径
中图分类号: D917 **文献标识码**: A **文章编号**: 1009-3192(2019)01-0083-08
DOI:10.19536/j.cnki.411439.2019.01.013

网络空间是与现实空间并行的第二大犯罪空间,自20世纪90年代以来,世界各国不断加大对网络犯罪的治理并取得了显著成效。但令人不安的事实是,目前我们使用的互联网只是互联网的三层之一,即搜索引擎可以搜索访问的表层网络(这被称为surface web或者clear net),除了表层网络,互联网还包括搜索引擎无法搜索的深网(deep web)和暗网(dark net)[1]。这是两个使人感到陌生的词汇,很多网络文章将暗网描绘成一个直播虐杀、直播性虐、国际人口贩卖、军火毒品交易泛滥的人间炼狱,是警察侦查无法企及的法外之地[2]。2017年6月,中国公民章某某在美国的遭遇所引发的种种猜测,更加剧了民众对暗网犯罪的恐慌。任何被民众认为是犯罪法外之地的现象都应当引起刑法学者的高度重视,但目前国内对此的研究屈指可数,甚至暗网意指何物都未能厘清,原因可能是利用暗网犯罪的案例在我国很少①,但暗网的彻底匿名性、互联性特征使其犯罪呈现出娴熟的"think global, act local"策略[3],近年来中国公民在境外遇害案件不时有暗网的影子。全面认识暗网犯罪,并以危机意识看待暗网对我国国家安全的威胁,对打击网络犯罪、建立坚固可靠的国家网络安全体系具有重要意义。

一、暗网是什么

"暗网"的概念在20世纪90年代就被提出,但直到2013年美国著名暗网"丝绸之路"(Silk Road)的创始人乌布利希被捕,暗网才引起公众的普遍关注,而此时"丝绸之路"的匿名交易已达到150万笔,交易额超过12亿美元[4]。2017年7月,美国宣布铲除了全球最大的从事毒品、武器和其他非法物品交

收稿日期:2018-08-11

作者简介:陈璐(1982—),女,法学博士、博士后,河南财经政法大学刑事司法学院副教授,河南财经政法大学国家安全法研究所研究员,研究方向为刑法学、国家安全法。

基金项目:河南省2017年哲学社会科学规划项目"互联网金融犯罪风险和刑法应对研究"(2017CFX024);司法部2017国家法治与法学理论研究项目"网络诈骗犯罪的司法认定问题研究"(17SFB3020)。

①截至目前,我国已破获两例暗网犯罪案件。2016年11月,北京市公安局网安总队成功打掉一个利用暗网传播儿童淫秽信息的群体,抓获8名犯罪嫌疑人,这是我国破获的首例暗网犯罪案件。2017年10月,湖北省公安厅网安总队破获一起跨境收买、非法提供信用卡信息案件,抓获7名犯罪嫌疑人,摧毁一个专门利用暗网盗刷境外信用卡的犯罪团伙。

易的暗网“阿尔法湾”(AlphaBay),此消息一出,暗网再次成为全世界舆论的焦点。从世界范围来看,暗网的确已成为犯罪更为隐秘的聚集场地,但显然我们对此知之甚少。因此当务之急是还原暗网的真实面目,从概念上厘清暗网究竟为何物。

(一)暗网的技术解析

暗网是一种加密网络,只能用特殊软件、特殊授权,或对电脑做特殊设置才能连上,暗网的服务器地址和数据传输通常是匿名、匿踪的,使用一般的浏览器和搜索引擎找不到暗网的内容。与此相对,一般常用的互联网由于可追踪其真实地理位置和通信人的身份而被称为“表层网络”(也被称为“明网”)。接入表层网络需要IP地址等信息,且需要通过路由器等网络设备建立链接,一旦留下IP地址或途经受监管的网络设备,接入者的行踪就可被追查到。暗网虽然也需要借助公开的互联网当作终端,但它们使用的是非常规的网络传输协议和端口,暗网最常用的技术是Tor软件、I2P和256位AES加密软件,其中最著名是Tor软件[5],它是一种实现匿名通信的软件,其名源于“The Onion Router”(洋葱路由器)的英语缩写。Tor的设计原意在于保障用户的个人隐私,由于Tor用户的互联网活动(包括浏览在线网站、帖子以及即时消息等通信形式)相对较难追踪,可以实现不受任何监控地进行秘密通信的自由。Tor的工作原理是通过不同服务器构成多个层(就像洋葱一样),把客户端包在最里面,数据进入网络之前会被加密,因此任何服务器都不能偷取通信数据。用户可通过Tor连接由全球志愿者免费提供的包含7000多个中继的覆盖网络,从而达到隐藏用户真实地址、避免网络监控及流量分析的目的。

(二)暗网与深网的区别

暗网和深网经常被混淆在一起,但它们是两个不同的概念。深网是指除了暗网之外的所有不能被搜索引擎访问的网站集合①。深网最早在20世纪70年代由美国军方开发,目的是将美国国防部的网络与互联网隔离,以保障国家军事安全。只有被授权的目标受众才有权访问深网的内容,目前,政府、军方、司法机关、高校图书馆等是深网的主要用户,这大致相当于国内民众经常说的“内网”。深网在国内也是一个具有神秘色彩的词汇,但其实它在人们日常生活中无所不在。例如QQ、MSN私人聊天记录、微信群里的聊天记录等是他人搜索不到的,对他人来说,这就是深网;A的微信朋友圈对B进行了屏蔽,对于B来说,A的朋友圈内容就是深网。从这个意义上说,深网其实是一个相对的概念,表示某(部分)用户不能搜索到的私有内容,但对于授权用户来说,访问深网的内容并不需要特殊的软件工具,例如A的微信朋友圈虽然对B进行了屏蔽,但对于A来说,其朋友圈内容就是一个普通的表层网络。搜索访问需不需要运用特殊的软件、工具,是深网和暗网的主要区别。

(三)暗网的数据容量

关于暗网的内容容量究竟有多大,目前并没有确切的数据,但国外很多学者对搜索引擎无法搜索的网络容量(包括深网和暗网)进行了预测。影响力较大的有两种观点:第一种观点认为,搜索引擎无法搜索的内容是可搜索内容的400倍到500倍[6];第二种观点认为,搜索引擎可搜索的内容仅占整个互联网内容的4%,而不可搜索的内容占96%[7]。第二种观点被国内一些网络文章大肆引用,并加以歪曲,试图将这96%的数据解读成公众不可知的犯罪黑暗数据,引发了公众不必要的恐慌。很显然,网络文章对该数据进行了错误解读,96%的数据量包括所有无法搜索到的内容,不仅包括暗网的内容,还包括政府、国防部门、司法机关、高校科研机构网络图书、论文数据库、私人网络数据等深网内容,而后者的数据量要比暗网数据量大得多。国外学者一致认为,暗网是互联网最具创新力的地方,同时也是最危险的地方。“丝绸之路”的创始人最原始的目的就是要创建一个完全没有统治的、完全自由开放的经济模式,让人们体验生活在一个没有系统化权力的世界里是什么样子,因此暗网并不是为了犯罪而创制,但邪恶总是特别青睐匿名与隐蔽,这使得暗网很快脱离它原有的初衷,沦为犯罪者的聚集地。

(四)暗网内容是否全部与犯罪相关

卢森堡大学Alex Biryukov教授的研究团队分析了3050个暗网站点,发现这些站点使用的语言多达17种,84%的站点使用的是英语,此外也包括中文,这说明暗网用户已呈现全球化态势,世界各国都无法置身事外[8]。当然,人们最关心的还是暗网上的内容是否全部与犯罪相关。根据Alex Biryukov

①也有学者认为,暗网是深层网络的子系统,即深层网络包含暗网。参见Kristin Finklea. Dark Web[EB/OL]. https://fas.org/sgp/crs/misc/R44101.pdf[2018-07-10].

教授团队的研究,暗网上与毒品、色情、军火武器和伪造品等犯罪相关的内容大约占44%,服务类的内容占4%,这其中不仅包括合法的服务内容,也包括洗钱和雇用杀手,其余的内容涉及政治观点、科技、艺术、网络游戏等[9]。由此可以看出,暗网内容并非全部与犯罪相关,犯罪内容占比不足50%,但这个数字仍然足以让人担忧。总部设在法国巴黎的"益普索"(IPSOS)公司,是全球最大的市场调研机构之一,该公司2016年组织了一项名为《互联网安全与信任全球调查报告》的民意调查,接受调查的民众分别来自24个国家,调查结果显示,国际社会约有71%的民众认为"洋葱暗网"应该关闭;赞同关闭暗网的民众占比排在前5名的分别是:印度尼西亚为85%,印度为82%,墨西哥为80%,中国为79%,埃及为79%[10]。民意调查的结果表达了民众对暗网这个网络"黑森林"世界的恐惧和担忧,无论暗网犯罪比例如何,其与现实司法力量脱离所造成的不可知性使民众对国家的社会治理产生了怀疑和担忧。

二、暗网犯罪对国家安全构成重大挑战

互联网本身是一个"易攻难守"的基础架构,但暗网的难以追踪性却让这个架构变得"易守难攻",因为它本身就是黑客的乐园[11]。暗网对国家安全的威胁已成为全球性问题,近年来发生的多起恐怖袭击案件都与暗网黑市有着千丝万缕的联系。2017年7月,美国著名智库兰德公司(RAND Corporation)发布的《幕布背后:暗网上的非法枪支弹药交易》调查报告指出,暗网黑市对国家安全的潜在威胁极大,且不受地域限制[12]。

(一)暗网对国家的军事安全构成重大威胁

计算机网络在优化国家军事管理的同时,也给国家军事安全带来了新的冲击和威胁。进入21世纪,网络犯罪对国家安全最具威胁的形式表现为利用网络实施的恐怖主义犯罪、间谍犯罪以及非法侵入电脑系统犯罪。2013年,英国议会委员会主席Keith　Vaz在一份议会报告中指出,网络攻击对国家的威胁将比核武器攻击更加严重[13]。目前,暗网上存在大量与国家军事秘密相关的黑客雇佣服务以及非法交易,这里混杂着大量军事发烧友、政治异见人士甚至邪教分子和恐怖分子,他们基于不同目的通过黑客雇佣和非法交易等形式打探不同国家的军事机密,甚至他们自己就是网络黑客。网络间谍与黑客通过非法链接、非授权访问、非法得到服务、植入病毒等方式直接攻击国家军事系统内部网,对其进行侵扰、破坏或盗窃[14]。2018年6月,致力于技术安全的Recorded Future网络安全公司在监控暗网中的犯罪行为时发现,有黑客正在暗网出售美国军方的机密文件,这些机密文件包括用于维修MQ-9 Reaper无人机的维护课程书籍,以及描述简易爆炸装置(IED)部署策略的各种培训手册,此外出售的还有M1艾布拉姆斯坦克操作手册,船员培训和生存手册,以及详细说明坦克排战术的文件。高级军事机密的泄露为世界各国敲响了警钟,网络防御等级最高的军事系统已成为黑客的觊觎目标,这无疑为国家安全带来了巨大威胁。

(二)暗网为恐怖主义犯罪提供了新的避风港

首先,暗网为恐怖主义犯罪寻求武器提供了极大便利。暗网通常能够提供性能更好、价格更低的武器,其不可追踪的特性也受到暴力犯罪分子的青睐。2015年巴黎恐袭事件中,恐怖分子所持自动步枪被证实来自暗网上的中间商;同年,19岁的英国青年利亚姆里博德在网络上宣称要袭击纽卡斯尔学院,事后警方证实其拥有的枪支和子弹均购于暗网;2016年慕尼黑枪击案件中,一名"独狼"恐怖分子也使用了从暗网上购买的枪支和子弹[15]。美国兰德公司的研究表明,暗网上军火交易每月的交易额高达8万美元,其中枪支销售额占比最大,约占90%。美国是暗网上武器的最大来源国,60%的枪支都产自美国,其次是欧洲,约占25%。尽管目前尚无数据表明暗网上销售的武器有多少被使用进行犯罪活动,但可以肯定的是,日益增长的交易规模与恐怖分子的活动密不可分,对国家安全构成了巨大威胁。

其次,暗网是恐怖组织招募成员、募集资金的中转站。巴黎恐怖袭击发生后,伊斯兰国恐怖分子"弃明投暗",将宣传机器快速转移到了暗网,暗网已成为恐怖组织进行人员招募、技术培训、灌输极端思想、策划恐怖活动的重要平台和快速、廉价、匿名的交流工具[16]。恐怖主义舆论借助暗网快速传播,宣传复仇思想、影响社会稳定,利用冲突性话题激化网民情绪、制造恐怖心理,采用涉恐音、视频资料吸引不法分子加入,造成极端主义思想的迅速蔓延。美国国家安全中心司令迈克尔·罗杰斯在华盛顿美国网络安全事件会议上指出,ISIS这样的组织在暗网上筹集资金,这是我们应该关注的问题[17]。联合国专家组向联合国安理会提交的报告中警告

说,“伊斯兰国”等组织使用暗网招募外国成员,策划发动袭击,其加密信息即便水平最高的安全机构也无法破解。此外,暗网中使用的虚拟货币为暴恐分子开辟了融资新渠道,恐怖组织“伊斯兰祈祷团”接受的资金均经由暗网的比特币交易平台。

(三)暗网结算工具成为国家金融安全的潜在威胁

诞生于2008年的比特币是暗网交易的最主要结算货币。比特币是一种虚拟货币,其转账由网络节点进行集体管理,交易各方可以隐藏自己的真实身份,它解决了没有中央清算机构条件下的结算难题,不需要依赖银行就能完成支付过程,从而避开了国家金融体系的监管,受到暗网市场的青睐[18]。2017年,国际执法部门在一起全球网络犯罪联合调查中,打掉了当前最大的两个暗网“阿尔法湾”(AlphaBay)与“汉萨市场(Hansa Market)”,这两大暗网平台每月使用比特币交易的毒品、淫秽物品及武器价值高达数千万美元。2018年,国际清算银行行长Agustin Carstens在其公开演讲中称比特币等加密货币是一种“泡沫、庞氏骗局和灾难的结合体”,唯一的功能似乎只涉及非法活动,各国应对其采取行动。

虚拟货币交易全球无国界流通,绕开了国家外汇管制,也无法通过银行等金融机构的交易记录来追查资金来源与去向,这使得虚拟货币游离于国家传统的金融监管体系之外,为用户逃避外汇管制、获取套利、非法集资、洗钱打开了方便之门,给国家金融监管带来了巨大风险。由于比特币是暗网买卖的硬通货,因此比特币的交易和回收业务在国外一直居高不下,这是比特币交易在我国兴起的重要诱因,吸引了大批国人试图投机获利,例如用人民币买进比特币,再以美元或者其他货币卖出,赚取差价,这种行为迅速成为我国外汇管理和反洗钱的一大隐患。2017年,中国人民银行等七部委联合发布了《关于防范代币发行融资风险的公告》,明确指出融资主体通过代币的违规发售、流通,向投资者筹集比特币、以太币等所谓“虚拟货币”,本质上是一种未经批准非法公开融资的行为,涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动。这一规定基本上否定了虚拟货币交易平台在我国境内存在的合法性,此后中国公民“翻墙”或者找代投参与国外融资平台的比特币交易越来越普遍,同时暗网也是实现交易的绝佳场所。尽管还没有数据显示中国公民在暗网中的比特币交易数量,但美国加利福尼亚大学发布的《中国网上地下经济调查》指出,在2011年中国大约有9万人参与网上黑市交易,造成53.6亿元损失,1.1亿用户成为受害者(占中国网民的22%),这说明隐藏于互联网深处的黑暗交易在我国已颇具规模和危害。应当指出,目前我国的网络黑市交易大多还处在“深网”阶段,即通过私人网络通信工具实现,但我们也必须保持足够的警惕,防止虚拟货币投资交易向暗网蔓延。

(四)暗网犯罪对公民人身安全产生巨大威胁

首先,暗网为违禁品交易提供了相对安全的平台,军火、毒品、虚假证件等非法交易在暗网隐蔽的世界里更加肆无忌惮。根据欧洲刑警组织的一份声明,“阿尔法湾”自2014年创立以来,已累计成交超过10亿美元,联合国毒品和犯罪问题办公室早在2014年《世界毒品报告》中就指出,暗网已经成为一个贩卖毒品的新的流行场所[19]。除此之外,暗网上出售身份证件也很常见,包括有效的和伪造的,其中护照、医院通行证和警察身份证,只需要10美元左右就能买到。这些违禁品交易对社会治安形成了巨大威胁,近年来在多个国家发生的毒品和枪支致人死亡事件中,警方都发现了暗网的身影。

其次,暗网是人口贩卖、雇凶谋杀等犯罪的助推器。联合国毒品和犯罪问题办公室2016年发布的《2016年全球人口贩运报告》显示,全球每年至少有250万人沦为人口贩运的受害者,其中妇女和儿童占受害者的79%,最常见的人口贩运目的是性剥削和强迫劳动,除此之外还有被迫充当乞丐、骗婚、色情产品制作以及人体器官摘除。该《报告》同时指出,暗网对这些犯罪起到了巨大的推波助澜作用,在“AlphaBay”与“Hansa market”被关闭之前,均能找到与这些犯罪相关的产品出售[20]。尽管这两大暗网已经被摧毁,但人口贩运、违禁品交易、儿童色情等犯罪行为在巨大的利益诱惑下会另辟渠道,一个暗网被打掉,还会有新的暗网建立起来,2013年被打掉的暗网“丝绸之路”就经历了四次复活,成为世界各国打击网络犯罪的难题。此外,近年来的雇凶杀人案件中也越来越多地出现暗网的身影。2016年美国新泽西警方破获了一起在暗网提供杀手谋杀服务犯罪未遂的案件,犯罪嫌疑人是一名来自纽约的18岁青年,其长期在暗网上宣传他的杀手服务。由于暗网的匿名性对犯罪的掩护作用,针对

暗网犯罪的刑事打击还没有呈现出常规化作业的特点,暗网犯罪平台"前仆后继"、不断革新加密技术逃避监管,使威胁公民人身安全的犯罪行为越来越走向不可知的深渊。

三、传统刑事司法手段打击暗网犯罪的困境

当前,全球用在保护网络安全的费用已达到800亿美元,但网络安全形势依然不容乐观[21]。暗网犯罪彻底匿名性的特征使传统刑事司法手段很难获得有效的犯罪线索,对其打击难度极大,是对未来世界各国刑事司法治理网络犯罪的新挑战。

(一)暗网犯罪取证难度极大

打击暗网犯罪最大的技术难题是取证困难。有学者指出,互联网环境中的证据问题正面临着技术和法律的双重挑战。从技术上说,收集证据是确定侵害原因及程度的第一步,但网络证据若非立即收集很容易丢失或者被覆盖;从法律上来说,对于法律所要求的侵害或者损失事实,受害人往往并不能进行有效的举证[22]。暗网犯罪由于其跨国性以及多层匿名技术的复杂性无疑使取证更加困难。传统刑事案件侦查依赖于案发现场调查,通过物证调查、摸排走访等传统侦查手段锁定犯罪嫌疑人,DNA、指纹等生物证据与犯罪嫌疑人身份具有直接对应的关系,但暗网犯罪痕迹存在于匿名的网络空间,以电子形式存在的犯罪证据通过常规的网络技术无法获取,甚至受害人或侦查人员都无法确定犯罪行为是否和暗网有关,在很多时候需要经过复杂的跨境搜索、综合分析、比对关联、剥茧抽丝,突破和跨越虚实空间的隔阂,才能真正追击疑犯,惩治犯罪。2017年9月13日,国际检察官联合会第二十二届会员年会暨代表大会召开了"电子证据与司法协助"专题会议,与会专家指出,网络没有国界之分,治理网络犯罪离不开电子证据……但迄今为止,并没有出现得到国际社会普遍认可的电子证据获取机制或者规定。对跨境获取电子证据的严格限制、各种匿名加密技术的无限自由化以及加密数字货币的诞生,都给在数字化时代追诉犯罪增添了诸多困难。

(二)侦查暗网犯罪涉及国家主权等问题

在侦查网络犯罪(包括暗网犯罪)的过程中,许多国家事实上都避开了协作取证的方式,直接依靠技术手段进行自行取证,例如远程勘验与强制披露等。所谓远程勘验,就是将整个因特网或局域网当成一个完整的犯罪现场,由执法人员通过网络对远程计算机信息系统实施勘验,发现、提取与犯罪有关的电子证据。在实践中,侦查人员在本国使用取证电脑,点击取证工具,通过技术手段即可远程登录境外的服务器等电子设备,检索和提取其中的电子证据。这种适用于虚拟现场的勘验方式,已经被广泛运用于司法实践。2016年,最高人民法院、最高人民检察院、公安部联合发布的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》明确规定,对于原始存储介质位于境外或者远程计算机信息系统上的电子数据,可以通过网络在线提取。为进一步查明有关情况,必要时,可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验,需要采取技术侦查措施的,应当依法经过严格的批准手续。跨境搜查则是传统搜查的网络版,是一国执法人员在获得法律授权后进行的在境外搜查电子证据行为,其搜查方式被称为网络调查技术,也可以理解为黑客技术。一个国家的司法机关如果在未经他国允许的情况下,直接对他国的服务器进行调查取证,有可能被认为是间谍行为,或者敌意行为,甚至是网络武装攻击行为,存在侵犯其司法主权的嫌疑。例如我国侦查人员在办案过程中需要获取嫌疑人曾经通过网络电话(skype)和谁频繁联系过、被害人在Facebook上发布消息时的位置在哪里,但这些网络运营商均在我国境外,那么在获取这些信息数据时就会存在很大障碍,如何避免可能引发的外交风险,也是一个棘手的问题。

四、打击暗网犯罪的多元应对策略

(一)建立专门的暗网犯罪监测部门

目前,网络犯罪专门执法机构在我国已初步确立,形成了公安部网络安全保卫局——省公安厅网络安全保卫总队——市公安局网络安全保卫支队——各分(县)局网络安全保卫大队的四级网安机构,主要承担打击网络违法犯罪、维护网络安全的责任。但是应对暗网犯罪,我国还未主动出击,仍处于接受国外情报线索的被动应急阶段,在北京警方打击利用暗网传播儿童淫秽信息的案件中,美国国土安全部海关及边境保护局提供的犯罪线索就起到了关键作用。自2017年以来,世界各国应对暗网犯罪的措施正在逐步升级。欧洲刑警组织的欧洲网络犯罪中心(European Cybercrime Centre)在

协助打掉暗网AlphaBay之后,就一直倡议创建协调的执法途径以打击暗网犯罪,这个倡议在2018年付诸实施,一个专门负责应对暗网犯罪的暗网调查小组得以成立。英国国家犯罪局(National Crime Agency)亦于2017年成立了专门的暗网情报部门(Dark Web Intelligence Unit),主要职责是收集相关数据信息,协调其他相关部门共同打击暗网犯罪行为。此外,德国于2016年成立了名为安全领域信息中央办公室(ZITiS)的新网络安全部门,通过产品开发协助德国安全机构应对网络犯罪和恐怖主义,并监控暗网中的非法活动。由于暗网犯罪依赖复杂的网络科技、不分国界且难以借助传统的司法手段破获,建立专门的机构监测、打击暗网犯罪已得到世界上越来越多国家的采纳。2017年开启了全球合作打击暗网犯罪的序幕,我国已破获的两起暗网犯罪说明我国绝不是与暗网隔绝的净土,对此我们应保持足够的清醒和重视。其他国家的经验值得我们借鉴和学习,建议公安部网络安全保卫局特别成立暗网犯罪特别监测小组,专门负责暗网犯罪情报的接收与监测,以此加强我国打击暗网犯罪的力度,增强我国深度参与国际刑事司法合作的能力。

(二)建立"产—官—学"协同合作机制,致力于暗网犯罪的深度研究

"产—官—学"相结合(the combination of industry, official and university)是现代国家社会治理创新、发展核心科技产业的普遍做法。当前,我们身处互联网信息科技爆炸的时代,行业壁垒使刑事司法部门的监测、侦查技术远远落后于犯罪技术,甚至许多互联网违法行为已经超越了当前法律和监管部门的规制范围,因此治理暗网犯罪仅仅依靠政府部门并不能奏效,还必须依靠互联网企业和科研机构的力量,后者能够为核心技术问题的解决以及决策提供有力支撑[23]。早在1997年,美国就成立了"国家网络执法师培训联盟"(NCFTA),由美国联邦调查局、微软等民营企业以及大学联合组成,旨在为国家提供网络犯罪情报以及警察执法培训。2014年,日本成立了"日本网络犯罪中心",该组织由日本警察厅、日本信息安全研究生院大学以及互联网企业联合成立,开展打击黑客的技术研发、警察执法培训,同时与世界其他国家的同类组织开展合作。2017年英国成立"国家网络安全中心"(NCSC),通过政府、企业等部门合作实现打击网络犯罪的职能。这些组织已经在实践中发挥了打击网络犯罪的重要作用。2018年,受欧盟经济和社会研究委员会的委托,兰德公司欧洲分部与曼彻斯特大学合作开展了一项关于冲突、犯罪和安全的研究项目,旨在探讨世界范围内非法武器的交易规律,重点关注暗网在推动和促进该贸易中所起的作用,例如暗网上买卖枪支的方法,同时预估暗网军火交易的规模和范围、查明军火的运输路线和常见的运输技术以及暗网可能对政策制定者的影响等等[24]。这是继两大暗网被打掉之后欧盟应对暗网犯罪的新举措,无疑将进一步加深对暗网犯罪规律的掌握。在我国,目前还未形成有效的针对网络犯罪的"产—官—学"协同合作机制,但"产—学"合作机制已开始了初步探索。例如2015年中国人民大学刑事法律科学研究中心、中国犯罪学学会、腾讯研究院犯罪研究中心共同筹建了"中国人民大学网络安全与犯罪研究中心",这是我国首个多家单位跨域协作研究网络安全与犯罪问题的专门机构。很显然,这种合作机制中还缺少官方这一主角的身影。打击暗网犯罪虽是政府主导的执法行为,但没有任何一个国家或实体能够单独去应对它,私营和公共部门之间的伙伴关系至关重要,"产—官—学"机制能使各方开展协同合作,充分发挥各方专长,确保抗击暗网犯罪的行动产生切实效果[25]。

(三)加强公私部门信息共享,提高电子取证技术

信息技术的发展提高了刑事司法部门获取、分析犯罪信息的能力,甚至从根本上改变了刑事司法的过程[26]。但毋庸讳言,在电子取证技术方面,刑事司法部门仍然落后于犯罪分子。近年来我国十分重视刑事司法部门电子取证业务的发展,截至2014年底,我国公安机关开展电子数据取证与鉴定工作的实验室已有300多家,公安部第三研究所也设立了司法鉴定中心为司法部门提供规范高效的电子数据和声像资料取证检验和鉴定服务[27]。但西方国家的经验表明,电子取证技术的革新往往并不是由国家刑事司法部门主导的,而是由互联网行业主导的。在美国,最顶尖的电子取证产品由互联网商业公司研发,例如美国Guidance公司的EnCase软件、AccessData公司的FTK软件和JAD公司的Internet Evidence Finder取证分析工具等[28]。科学研究也不断研发新的软件模型促进电子取证技术的革新,例如有学者将贝叶斯网络模型(Bayesian belief network models)运用到网络犯罪的调查取证中,以便快速收集和识别可疑数据[29]。目前,我国

电子取证行业发展已处于起步阶段,例如厦门市美亚柏科信息股份有限公司研发的数据取证工具、视频分析及专项执法装备,在新型智能终端取证以及云储存系统取证技术上均处于国家领先水平。近年来,国家安全部门、工信部门以及司法部门越来越重视互联网企业电子取证行业的发展,经过酝酿,2016年《网络安全法》首次以国家基本法的形式确认了电子取证领域公私部门协作的原则,其第28条规定"网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助",这为我国扶持、培育互联网企业开发电子取证产品提供了政策导向和法律支持,也为刑事司法部门克服电子取证难题指明了方向。

但公私部门协作的最大难题是信息共享,建立有效的合作以及克服双方对信息共享的忧虑仍然困难重重。传统的刑事司法文化对信息共享持排斥态度,因此发展合作关系以及确定哪些信息应该共享、可以共享并不是一件容易的事情,刑事司法部门将面临如何展开共享合作、如何确保信息安全等诸多难题[30]。尽管困难重重,但一些国家正在开始尝试,例如美国微软公司设立了"数字犯罪部(Digital Crime Unit)",在打击跨国网络犯罪方面发挥了重要作用。该部门在全球30个地点开设分支,通过各种创新方法,帮助有关国家开展遏制网络犯罪行动,并取得了卓有成效的进展。我国互联网企业亦开始尝试基于AI、云计算、大数据等技术对网络犯罪的实证研究与产品研发,2016年9月,全国首个互联网数据取证公众服务平台正式上线,该服务平台是"政府主导+互联网企业"研发的协作成果,通过保全、取证、法律服务、举报四大功能使个人也能便捷地获取合法电子证据,对网络犯罪举证问题具有极大的启示意义。

(四)积极寻求国际刑事司法合作

暗网犯罪多涉及跨境交易,因此国际刑事司法合作至关重要。2014年,国际刑警组织全球创新中心(Interpol Global Complex for Innovation)在新加坡宣告成立,该中心的成立标志着全球警务进入电子时代,作为打击网络犯罪的新型机构,该中心在协助打击暗网犯罪跨国性行动方面已经卓有成效。在取缔世界最大的暗网市场"AlphaBay"犯罪团伙行动中,共有来自美国、荷兰、泰国、加拿大、英国、法国等国家的数十个政府监管部门参与了打击活动,是史上最大规模的一次国际网络犯罪打击行动。如果没有国际刑事司法合作,很难想象依靠某一个国家的力量能将非法交易横跨全球的暗网打掉,我国破获的暗网犯罪也在很大程度上得益于国际刑事司法协助。2016年10月17日,《联合国打击跨国有组织犯罪公约》缔约方第八届会议在维也纳召开,其主要议题是打击跨国有组织犯罪的国际合作,尤其侧重于引渡、司法协助、移交被判刑人员和没收事宜的国际合作,但到目前为止,国际社会还未形成针对网络犯罪全球合作的法律框架。

不同国家在规律规定、执法方式千差万别的情况下实现协同一致并不是一件容易的事情。例如不同国家对毒品、枪支及其组装部件的法律规定各不相同;各国政府对虚拟货币的监管态度也并不一致。此外,打击暗网犯罪的国际合作困境还包括地区性网络犯罪法律文书已过时且规定并不一致;传统合作模式不能在确保尊重国家主权前提下实现网络犯罪的跨国侦查、电子证据获取等合作需求;云计算、加密技术等新技术以及暗网犯罪形式不断翻新给刑事司法国际合作带来技术挑战等。面对这些复杂挑战,联合国毒品与犯罪问题办公室网络和新兴犯罪首席官员尼尔·沃什表示,联合国是谈判制订网络犯罪国际公约最合适的场所。国际社会应根据和平、主权、共治、互惠原则,在联合国框架下制定全球性打击网络犯罪法律文书,探索各国普遍接受的网络空间国际规则和国家行为规范,通过系统的规范设计凝聚有关入罪标准、管辖协调、情报共享、执法程序以及对国际合作请求迅速作出回应等方面的国际共识,弥补国际合作的法律空白或冲突,建构全球法律框架,促进各国打击网络犯罪法律和实践的协调一致。

参考文献:

[1][7]S Suneetha, M Usha Rani. Unveiling Deep Web, a High Quality Quantitative Information Resource [J]. International Journal of Latest Trends in Engineering and Technology, 2017(2):167.

[2][6]Daniel Sui. The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box [J]. Woodrow Wilson International Center for Scholars, 2015(3):6.

[3]Yuval Ben-Itzhak. Organised cybercrime and payment cards[J]. Card Technology Today, 2009(2):10.

[4]Jamie Bartlett. The Dark Net: Inside the Digital Underworld[M]. London:William Heinemann Ltd, 2015:

3.

[5] Ross W Bellaby. Going dark: anonymising technology in cyberspace [J]. Ethics and Information Technology, 2018(6):10.

[8][9] Alex Biryukov, Ivan Pustogarov, Fabrice Thill, etc.. Content and popularity analysis of Tor hidden services [C]. Madrid: 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops, 2014:3.

[10] 2016 CIGI-Ipsos Global Survey on Internet Security and Trust [EB/OL]. (2016-07-03) [2018-07-11]. https://www.cigionline.org/internet-survey-2016.

[11] 左亦鲁.国家安全视域下的网络安全——从攻守平衡的角度切入[J].华东政法大学学报,2018(1):148-157.

[12] Giacomo Persi Paoli, Judith Aldridge, Nathan Ryan, etc.. Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web [EB/OL]. (2017-07-01) [2018-07-11].https : // www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf.

[13] UK losing the battle against cybercrime [J]. Computer Fraud & Security, 2013(8):1.

[14] 王军.观念政治视野下的网络空间国家安全[J].世界经济与政治,2013(3):45-61.

[15] 云贺.怎样打赢暗网攻坚战[EB/OL].(2017-01-06)[2018-07-10].http://www.lwinst.com/cjgjzk201716/4902.htm.

[16] 焦康武.总体国家安全观视域下我国暗网犯罪应对研究[J].犯罪研究,2017(6):78-89.

[17] Ryan Ehney, Jack D Shorter. Deep web, Dark web, Invisible Web and the Post ISIS World [J]. Issues in Information Systems, 2016(4):36-41.

[18] Sesha Kethineni, Ying Cao, Cassandra Dodge. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes [J]. American Journal of Criminal Justice, 2017(5):141.

[19] Julia Buxton, Tim Bingham. The Rise and Challenge of Dark Net Drug Markets[J]. Policy Brief, 2015(1):2.

[20] Global Report on Trafficking in Persons2016[EB/OL]. (2016-09-01) [2018-07-11]. https://www.unodc.org/documents/data-and-analysis/glotip/2016_Global_Report_on_Trafficking_in_Persons.pdf.

[21] Doug Irving. The Digital Underworld: What You Need to Know [EB/OL]. (2016-06-24) [2018-07-11]. https://www.rand.org/blog/rand-review/2016/06/the-digital-underworld.html.

[22] Winston Krone. Legal and Technical Issues Concerning Evidence in Data Breach Cases. Published in 2012 PLI Privacy and Data Security Law Institute (Thirteenth Annual) Course Handbook [EB/OL]. (2012-08-12) [2018-07-11]. http : // kivuconsulting.com/wp - content/uploads / 2012/08 /2012-Legal_and_Technical_Isues_Concerning _ Evidence Breach_Cases_WKrone.pdf.

[23] Adam Salifu. The impact of internet crime on development[J]. Journal of Financial Crime, 2008(4): 440.

[24] International Arms Trade on the Dark Web [EB/OL]. (2014-04-01) [2018-07-11].https: //www. rand. org / randeurope / research/projects/international-arms-trade-on-the-hidden-web.html.

[25] Public-private partnerships needed to combat transnational cyber-crime [EB/OL]. (2015-04-02) [2018-07-11] .http://www.unmultimedia. org/radio/english/2015/04/public - private-partnerships - needed-to-combat-transnational-cyber-crime/index.html.

[26] April Pattavina. Information Technology and the Criminal Justice System[M].Thousand Oask: Sage publications Inc, 2005:8.

[27] 金波,杨涛,吴松洋.电子数据取证与鉴定发展概述[J].中国司法鉴定,2016(1):62-74.

[28] Cover all the cases with the right computer forensics toolkit [EB/OL]. (2016-06-01) [2018-07-11].https://www.magnetforensics.com/computer - forensics/cover-all-the-cases-with-the-right-computer-forensics-toolkit/.

[29] Hayson Tse, Kam-Pui Chow, Michael Kwan. A Generic Bayesian Belief Model for Similar Cyber Crimes [J]. Advances in Digital Forensics, 2014(2): 243.

[30] Maureen Brown. Criminal Justice Discovers Information Technology[J]. Criminal Justice, 2000(1):249.

责任编辑:何恒攀