doi:10.3969/j.issn.1673-4823.2020.04.006

互联网的地下黑市——暗网的法律治理之策

贺晨霞
(湘潭大学 法学院,湖南 湘潭 411100)

摘要:暗网中充斥着诸多非法交易,现已成为犯罪分子以及恐怖分子活动的天堂。犯罪分子利用暗网实施犯罪的行为将对国家安全、社会稳定构成重大威胁。暗网因其隐匿性强以及交易方式的特殊性,加大了取证及监管的难度。治理暗网,必须提高网络技术水平,完善网络监管相关法律法规,加强打击暗网的国际合作以及政企之间的合作。

关键词:暗网;网络监管;网络安全;治理
中图分类号:D922.804 **文献标识码**:A **文章编号**:1673-4823(2020)04-0025-03

一、暗网与暗网犯罪

(一)暗网是什么

暗网是指那些存储在网络数据库里、不能通过超链接访问,需要通过动态网页技术访问的资源集合[1]。在网络世界里,存在一套"冰山理论",即我们平时所能访问到的网络数据只占整个网络数据量的5%,称之为"明网",而剩下的95%都隐藏在"冰山"之下,称之为"深网"。但暗网不同于深网,其不仅可以躲避一般搜索引擎,还能通过使用特殊加密技术隐藏相关网络信息。因此,暗网通常被认为是深网的一个子集。换言之,深网的深处才是暗网。暗网真正走进公众的视野,是因为一家名叫"丝绸之路"的网站。在该网站上,毒品是其出售的主要商品。除此以外,用户还能在该网站购买无登记的手枪、雇佣私人杀手……令人难以想象的是,暗网的创办者——罗斯乌布里希,是年仅29岁的获得过宾州州立大学硕士学位的学霸。

(二)暗网的运作原理

开启暗网大门的常用钥匙是匿名代理工具"Tor",因其像洋葱一样层层保护着数据,而被称作"洋葱路由"[2]。使用该工具访问暗网时,访问者的IP地址以及身份信息都将被隐匿,这使得犯罪分子的非法交易能被很好地隐藏起来。正是基于这一特性,暗网得不到有效监管,从而沦为犯罪分子自由的天堂。

(三)暗网中的非法交易

暗网作为一个隐蔽的罪恶天堂,充斥着诸多非法交易。例如,贩卖军火、毒品、身份证件、银行卡信息、人口以及人体器官等。暗网中不仅充斥着各种犯罪,还为恐怖分子招募人员、购买武器提供非法渠道。美国最大的一个从事毒品、武器和其他非法物品交易的网络平台——"阿尔法湾",自2014年创建以来,非法销售额累计已达10亿美元。很多人可能认为自己从未浏览过暗网,距离暗网很遥远,但事实并非如此。2016年,美国发生多起未成年人吸食毒品致死的事件,经有关部门调查,这些毒品均来自于"阿尔法湾"。为进一步取证,执法人员假扮用户,从"阿尔法湾"上购买了大麻、海洛因、冰毒、假身份证和ATM机盗刷器等非法物品。包裹上的邮戳表明,其卖家遍布美国各个地区。截至到"阿尔法湾"网站被关闭前,该网站上非法药品和有毒化学品的交易条目超过25万条,失窃身份证件和信用卡的交易条目超过10万条[3]。不仅如此,暗网里人口贩卖交易也十分猖獗。2017年7月16日,一名19岁的英国模

[收稿日期]2020-01-02
[作者简介]贺晨霞(1996—),女,湖南长沙人,硕士研究生,主要从事刑法学研究。

特被犯罪分子绑架并以 30 万美元的起拍价在暗网上公开拍卖。正是由于这一起起案件的接连发生，使得暗网备受人们的关注。

二、暗网的治理困境

（一）隐匿性强、用户范围广、交易方式特殊

暗网最大的特征就是隐匿性强。暗网采用的是匿名访问机制，当用户访问暗网时，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[3]。暗网允许任何人创建无法跟踪的服务器以进行匿名活动，服务提供商和软件开发者不仅不能监控操作者的路由信息，更无法得知其真实身份。暗网的用户范围十分广泛，使用者不光有恐怖分子、贩毒走私人员、上班族，甚至包括在校学生。据乔治城大学的一项调查统计，Tor 日常的用户量约为 95 万，广泛分布于德国、中国、美国、意大利、土耳其、英国等国家，其中德国与美国的用户较多[4]。与一般网站的支付方式不同，暗网主要通过比特币进行支付。由于比特币完全是靠点对点的对接进行交易，所以不需要买卖双方的个人信息，大大地“保护”了这些非法交易者的交易安全。

（二）社会危害性极大

一方面，暗网是政治异见分子滋生的温床。由于缺少法律监督和网络监管，一些反政治言论在暗网中迅速传播，其中还有一些极端组织利用暗网对其他国家的政权进行攻击。另一方面，暗网为恐怖分子提供了隐蔽的空间。恐怖分子往往利用暗网进行信息交流、恐怖活动部署以及购买物资等活动。例如，在中东地区，恐怖分子通过暗网进行恐怖行为的人员招募、策划以及煽动等活动。这些恐怖活动严重扰乱了社会秩序，给民众心理造成了极大恐慌，给国际执法活动造成了巨大障碍。

（三）取证、监管困难

在过去，犯罪分子受地域条件的限制，难以实现跨国性犯罪。现如今，全球进入互联网时代，基于网络的“时空压缩”特征，犯罪分子通过互联网传递信息时，可以突破时间和空间的限制，使跨地域、跨国界犯罪成为可能。由于暗网的跨国性及其对用户信息的匿名性、加密性的保护，致使执法机构无法对用户的信息进行追踪，给执法机构调取、收集证据以及监管工作造成了极大困难。

三、暗网的治理之策

从目前来看，暗网的用户主要来自发达国家，在暗网犯罪如此猖獗的情况下，中国作为国际性大国，应尽显大国的风范与使命，充当网络安全的坚定维护者，积极参与到暗网治理的行动中去。

（一）提高网络安全技术

暗网之所以发展得如此迅猛，得益于互联网技术的快速发展。暗网虽然比一般网络犯罪更难于侦查，但其始终不可能脱离互联网而独立存在。因此，治理暗网的首要措施就是提高网络安全技术。在提高网络安全技术的措施上，我们可以借鉴西方国家的相关经验。例如，英国拟大量增拨经费，计划在 5 年内投入 19 亿英镑用于打击网络袭击和网络恐怖活动，并集中全英国顶尖专家成立一个新的国家网络中心[5]。又如，美国国土安全部 2016 年就一次性招募了 1 000 名网络安全专家，使美国政府和军方拥有全球数量最多、规模最庞大的网络安全部队。为切实提高网络安全技术，一方面，中国应在网络安全技术研发上投入更多研发经费，为技术研发提供资金保障，开展暗网治理的专项研究。另一方面，中国应重视网络安全人才的培养。习近平指出：“网络空间的竞争，归根结底是人才竞争。”因此，只有培养更多的网络技术人才，才能引领中国科技发展，从而更好地为网络安全保驾护航。

（二）完善网络监管相关法律法规

中国网络相关立法发展至今，已颁布了多部法律法规以及部门规章。如 2014 年最高人民法院、最高人民检察院、公安部发布实施《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》，2015 年 8 月 29 日通过的《中华人民共和国刑法修正案（九）》新增“拒不履行网络安全管理义务罪”“非法利用信息网络罪”以及“帮助信息网络犯罪活动罪”，2017 年 6 月 1 日起施行《中华人民共和国网络安全法》等。虽然中国已颁布了多部法律法规，但仍存在立法对网络犯罪的规制范围过于狭窄，缺乏在法律中对暗网的具体规定等问题。互联网发展日新月异，相关立法需要针对实践中出现的新问题不断进行完善，从而适应社会的变化。针对上述问题，中国的立法工作应从以下几个方面着手：首先，在立法过程中，应当重视罪名设置的科学化和罪名体系的严密化，提高立法的技术性与科学性。其次，制订相应的法律依

据,明确监管部门、服务提供商、网络提供商、用户四方的权利与义务,落实网络信息安全责任[6]。最后,完善网络立法的相关规定。一方面,完善网络监管相关法律法规以及完善涉及国家安全重要信息系统的设计、建设和运行监督机制;另一方面,赋予相关部门更大的权力以应对网络紧急情况,加大惩治力度,有效预防网络犯罪的发生。

(三)加强物流行业的监管

物流行业具有隐蔽性、迅捷性以及低成本等优势,正因如此,暗网中的违禁品交易往往通过物流运输完成。目前中国物流行业法律规定尚不够完善,政府监管不够到位,让从事非法交易的犯罪分子有机可乘。因此,就有关部门而言,应该加强对物流行业的监管,对运送非法物品的物流公司严惩不贷。就物流公司而言,要加强自我监管,对在岗员工定期进行相关培训,加强物流工作人员对于违禁品的辨别能力,当发现可疑物件应及时向公安机关上报。

(四)促进国际合作以及政企合作

目前,利用暗网实施犯罪已成为国际网络安全治理的焦点问题。暗网多涉及跨国交易,因此,开展国际执法合作对处理暗网问题至关重要。此前,多国曾通过联合执法行动打击利用暗网实施的违法犯罪行为,如2016年11月,美国、英国、澳大利亚、加拿大以及新西兰的国际执法机构,共同发起了一场打击暗网非法活动的运动,该运动旨在通过跨国情报共享的方式打击国际犯罪[7];2017年7月,英国、加拿大、法国、德国、泰国以及欧洲刑警组织采取联合行动,关闭了全球规模最大的黑市交易市场——"阿尔法湾"。基于此,中国应以其他国家的多国联合行动为鉴,在互相尊重国家主权的前提下,建立高效的国际合作机制,共同分享暗网情报信息,积极同其他国家一起打击暗网犯罪。在加强国与国之间合作的同时,还应该促进政府与企业之间的合作,尤其是促进阿里巴巴、腾讯、百度等综合实力强的大型互联网公司参与到治理暗网的行动中去,使企业与政府共筑网络安全防御屏障,实现网络空间的长治久安。

参考文献:

[1] 秦玉海,杨嵩,陈杰针. 针对"暗网"的监管机制研究[J]. 辽宁警察学院学报,2017(5):31-34.

[2] 明乐齐. 暗网犯罪的趋势分析与治理对策[J]. 犯罪研究,2019(4):65-76.

[3] 于世梁. 国外打击涉"暗网"犯罪的经验及启示[J]. 河南警察学院学报,2019(4):5-11。

[4] 赵志云,张旭,罗铮,等."暗网"应用情况及监管方法研究[J]. 知识管理论坛,2016(2):124-129.

[5] 范江波. 暗网法律治理问题探究[J]. 信息安全研究,2018(7):593-601.

[6] 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.

[7] 周琳娜,高存. 暗网治理思路[J]. 信息安全研究,2018(9):846-852.

责任编辑:潘伟彬

The underground black market of the Internet

——The legal governance strategy of the dark web

HE Chen-xia

(School of Law, Xiangtan University, Xiangtan, Hunan, 411100, China)

Abstract:The dark web is full of illegal transactions, and has become a paradise for criminals and terrorists. Criminals' use of the dark web to commit crimes will pose a major threat to national security and social stability. The governance problem of the dark web lies in its high concealment and the particularity of the transaction method, thus increasing the difficulty of forensics and supervision. The governance of the dark web must improve the technical level of the network, improve the laws and regulations related to network supervision, and strengthen the international cooperation against the dark web as well as the cooperation between government and enterprises.

Key words:dark web; network supervision; network security; governance