·政治学研究·

DOI:10.3969/j.issn.1671-7155.2019.02.006

“暗网”:我国网络空间治理的新领域

于世梁

(江西省行政学院,江西 南昌 330003)

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

〔摘 要〕“暗网”是使用常规方法无法进入,可以实现匿名访问的网络空间。它虽然能够满足用户匿名访问互联网,但也给不法分子进行贩毒、走私、色情、洗钱、售假、从事恐怖活动等提供了重要场所。近年来,国际社会加大了打击涉“暗网”犯罪活动的力度,摧毁了多个大型“暗网”非法交易网站。中国作为互联网大国,面对“暗网”不可能置身事外,独善其身,打击涉“暗网”新型犯罪活动已经成为我国网络空间治理的重点任务之一。为此,我们应当学习借鉴欧美国家打击涉“暗网”犯罪活动的经验,结合我国的网络国情,在加强组织领导,完善法律法规,加强法制宣传,加强技术研究,加强国际合作等方面有所创新,走出一条具有中国特色的管网治网之路。

〔关键词〕暗网;网络空间治理;洋葱路由;Tor

〔中图分类号〕D035.29 〔文献标识码〕A 〔文章编号〕1671-7155(2019)02-0041-06

在互联网中,使用常规方法就能访问的网络,我们称其为“明网”(Surface Web),而必须借助专用工具才能访问的网络,我们称其为“暗网”(Dark Web)。“明网”与“暗网”最大的不同是,用户在访问“明网”时,网络中的设备和监控软件会记录终端计算机的IP地址从而让访问者的身份暴露。而“暗网”由于采用了匿名访问机制,访问者不会在网络中留下“痕迹”,因此,“暗网”可以满足用户匿名访问网络的需要,但同时也给贩毒、贩枪、走私、洗钱、色情、售假、从事恐怖活动等提供了新的场所。近年来,国际社会加大了打击涉“暗网”犯罪的力度,摧毁了多个大型“暗网”非法交易网站,抓获了非法网站的组织者和经营者。中国作为互联网大国,面对“暗网”不可能置身事外,独善其身。2016年3月,北京市公安局破获了一起中国公民利用“暗网”传播儿童色情信息的案件;2018年,“暗网”中文论坛出现多个售卖中国公民个人信息的网帖……随着我国涉“暗网”犯罪案件逐年增多,预防打击涉“暗网”犯罪活动已经成为我国网络空间治理的重点任务之一。

收稿日期:2019-02-24

一、“暗网”:互联网上的另一个世界

同电话通讯中每部电话或手机都有一个电话号码一样,互联网中的每一台上网计算机也必须有一个能够标明身份的IP地址。通过计算机的IP地址,能够确定上网人的身份,进而可以找到网络使用者。在“暗网”出现之前,对于那些希望匿名访问互联网而不留下“痕迹”的人(包括政府),无论采用何种方式隐藏自己的网络行踪,计算机IP地址都会最终暴露上网者的身份。因此,设计一种能够实现匿名访问的网络就成为政府的迫切需求。

1.“暗网”源于美国海军研究实验室

为了保护军方或情报人员在互联网上能够安全通信而不被追踪,20世纪90年代美国政府和军方启动了匿名网络研究项目。1996年5月,美国海军研究实验室(NRL)资助的数学家保罗·西维森(Paul Syverson)、计算机科学家迈克·里德(G.Mike Reed)和大卫·戈尔德施拉格(David Goldschlag)提出了一种被称为“洋葱路由”(Tor:the Onion Router)的匿名网络技术。

2002年,麻省理工学院(MIT)的两名毕业生罗根

·丁格伦(Roger Dingledine)和尼克·马修森(Nick Mathewson)加入了 Tor 项目,之后研究取得了重大进展。2003 年 10 月,第二代"洋葱路由"问世,匿名网络从想象变成了现实。2004 年,美国海军研究实验室因财政困难砍掉对 Tor 项目的支持资金,并以自由软件授权的方式公开了其源代码。之后,一个名叫电子前哨基金会(EFF)的组织接管了 Tor 项目的后续研发。

Tor 是在计算机上安装的一个软件,用于运行和管理 Tor 连接的计算机网络。使用 Tor 的用户可以通过一系列虚拟通道而不是直接连接到网站,从而允许用户通过公共网络访问互联网而不会暴露个人身份及网络踪迹。正是由于用 Tor 技术构建的网络具有很好的访问匿名性,其一经推出便受到各界的欢迎,Tor 软件的下载量逐年攀升。随着使用者越来越多,Tor 网络得到了迅速发展,分布于全球各地的中继节点使其实现了彻底的去中心化。如今,无论是 Tor 的发明者,还是美国政府都已经失去了对 Tor 的掌控,Tor 网络成为一个游离于政府监管之外的"不法之地"。

2."暗网"能够实现完全的匿名访问

用普通方式访问互联网,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流量监控程序记录下来。因此,通过 IP 地址或途经受监控的网络设备,用户的身份和网络踪迹都可以被追溯。尽管有些人(比如黑客)会采用一些特殊技术手段来掩盖自己的网络身份和网络踪迹,但这只是增加了追查的难度。无论他做的多么巧妙和严密,最终都有可能因为留下的"蛛丝马迹"而被执法部门跟踪和查获。图 1 为普通网络访问流程。

图 1 普通网络访问流程

与普通网络访问流程不同,"暗网"是采用分布式、多节点数据访问和多层数据加密技术组成的网络。分布式是指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;多节点是指信息传递从起点到终点要经过多个(一般为 3 个)随机选择的中继节点;多层数据加密是指系统会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,从而实现完全的匿名访问。图 2 为"暗网"访问流程[1]。

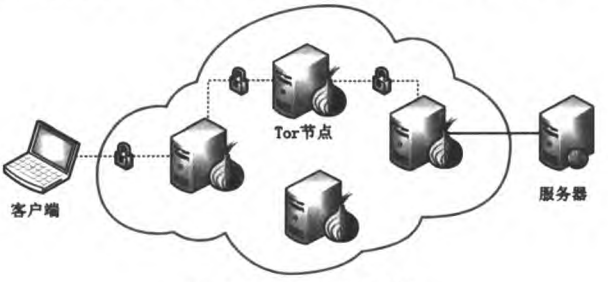

图 2 "暗网"访问流程

多层加密机制,是"暗网"能够实现匿名访问的重要技术之一。由于对数据多层加密,每一个数据包好像被加上了"洋葱"(onion)一样的层层保护,"洋葱路由"(Tor:the Onion Router)由此得名。要获取用户访问"暗网"的记录,必须破解"暗网"所使用的加密机制,这在目前是无法做到的。

在普通的互联网中,网站的域名大多以 .com、.net 等结尾,而 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Google等搜索引擎也无法搜索到"暗网"中的内容,访问"暗网"需要安装专用的浏览器。Tor 浏览器(Tor Browser)虽然不是访问"暗网"的唯一手段,但它是目前最流行最受欢迎的"暗网"访问软件。据统计,Tor浏览器的全球下载量达到了每年近 5000 万人次[2]。

二、"暗网":难以监管的"不法之地"

"暗网"的诞生源于对网络通讯保密的要求,它广泛应用于对网络通信安全要求较高的军事情报领域和商业机构。例如,纽约客(The New Yorker)在"暗网"中建有一个检举网站,脸书(Facebook)在"暗网"上也建了一个供用户访问的特别网站[3]。又如,以曝光政府机密文件而出名的维基解密(WikiLeaks),经常通过"暗网"与爆料者进行联系和沟通。曝光美国"棱镜"监控项目的爱德华·斯诺登(Edward Snowden),也是通过"暗网"将其所掌握的政府秘密文件泄露给媒体的[4]。但是,任何技术都是一把"双刃剑","暗网"因其良好的访问匿名性、信息加密性和服务器隐藏性,使其在 2004 年开源化后很快成为不法分子从事违法犯罪活动的新渠道。

1."暗网"已经成为违禁商品买卖的重要平台

电子商务是互联网应用的重要领域。淘宝、亚马逊等电子商务网站已经成为商品销售的重要平台。"暗网"中也存在类似的商品交易网站，但是其中销售的是毒品、非法枪支、黑客工具、各种假证等违禁商品。

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）正式上线。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 个州以及其它 34 个国家和地区，每年的营业额超过 100 万美元。"农夫市场"经营几乎所有的违禁商品，其中又以毒品和管制药品为主。2012 年 4 月，美国缉毒局与荷兰、哥伦比亚、苏格兰等地警方合作，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"随即被关闭。

2010 年，美国人罗斯·乌尔布莱特(Ross Ulbricht)在"暗网"中建立了一个名为"丝绸之路"（Silk Road）的非法交易网站，销售包括各种毒品、各类枪支、儿童色情、各种伪造证件等违禁商品达一万多种[5]。从创建到被关闭的两年时间内，"丝绸之路"总交易额超过了 12 亿美元，乌尔布莱特也依靠每笔交易收取 10%-12%的佣金，赚取了近 1 亿美元。乌尔布莱特因为在"明网"上发布招聘启事时使用了自己完整姓名的邮箱（rossulbricht@gmail.com）而暴露了真实身份，在 2013 年 10 月 1 日被美国联邦调查局（FBI）探员在旧金山抓获，"丝绸之路"随即被关闭[6]。2015 年，乌尔布莱特被以持续从事经济犯罪、贩毒、洗钱、从事电脑黑客等 7 项罪名判处无期徒刑[7]。就在"丝绸之路"网站被查封一个月后，"丝绸之路 2.0"在 2013 年 11 月重新上线，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"随即被关闭[8]。

"丝绸之路"被查封后，美国人亚历山大·卡兹（Alexandre Cazes）2014 年在"暗网"上创建了另一个非法交易网站"阿尔法湾"（AlphaBay），主要经营各种毒品、有毒化学物、枪支弹药、伪造证件、黑客工具、儿童色情等违禁商品。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[9]。2017 年 7 月 4 日，"阿尔法湾"服务器遭警方关闭，卡兹也在次日被泰国警方抓获。2017 年 7 月 12 日，就在卡兹即将被引渡至美国前，被发现死于曼谷的一所监狱内。

2."暗网"已经成为非法信息传播的重要渠道

"暗网"中除了进行违禁商品非法交易，色情、绑架、暗杀、暴恐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，视频数千个，注册会员达 1.5 万名[10](P146)。2011 年 10 月，黑客组织"匿名者"（Anonymous）在一次针对"暗网"的行动中，摧毁了"暗网"上运行的一个名为"自由主机"（Free Mainframe）的网站托管服务，该网站托管了 40 多个儿童色情网站，其中"洛丽塔都市"被列为最大的儿童色情网站之一，拥有超过 100GB 的数据[11]。

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物理系博士生勃兰特·克里斯滕森（Brendt Christensen）。调查发现，克里斯滕森曾在 2017 年 4 月访问过一个名为 FetLife 的网站。FetLife 是"暗网"中一个以绑架、施虐为主题的社交网络，该网站上有超过三千万张图片和四万段录像，注册用户达 600 多万人[12]。

3."暗网"已经成为恐怖组织活动的重要场所

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打击力度，大批涉及恐怖主义内容的社交网络账号和网站被关闭。为了躲避执法部门的追踪和监控，恐怖组织开始通过"暗网"来发布信息、招募人员以及组织和策划恐怖袭击活动。

"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"市场上购买的。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的障碍。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曾指出，"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"上的加密信息即便水平最高的安全机构也难以破解，并提醒各国政府应对此保持高度的警惕[14]。

三、国际社会打击“暗网”犯罪活动的主要经验

日益猖獗的涉“暗网”犯罪活动，引起了国际社会的高度关注。但是“暗网”的匿名性和隐密性，给国际社会打击涉“暗网”犯罪活动带来了很大困难。尽管如此，美欧等发达国家通过采取一系列措施加强对“暗网”的管控，在打击涉“暗网”犯罪活动中取得了显著成效，积累了许多成功经验，值得我们学习和借鉴。

1.加强技术研究

如前所述，“暗网”访问的匿名性，能够隐藏上网者计算机的IP地址，使执法人员很难确定上网者的真实身份。用 Google 等常用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安全专家合作，不断开发出可以识别某些隐藏服务和去匿名化的技术手段，帮助执法机关收集“暗网”中的数据，确定“暗网”访问者的身份。

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，来提高对“暗网”隐藏内容的搜索和分析能力，以帮助政府部门（执法机关）尽可能多的收集“暗网”里的信息。2015 年 4 月，DARPA 对外公布了 Memex 项目并开源了部分 Memex 的源代码。通过 Memex 可以对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。图 3 为 NIT 追踪“暗网”用户的原理[15]。

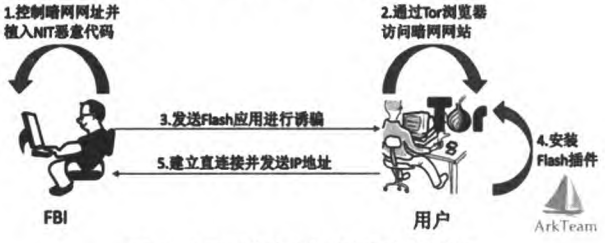

图 3 NIT 追踪“暗网”用户的原理

2.成立专门机构

通过“暗网”进行的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主义等各个方面，这就使得打击涉“暗网”犯罪活动需要各相关部门的共同协作。为此，成立专门机构能够提高执法部门间的信息资源共享和协同行动能力。

以英国为例。2015 年，英国政府成立了一个专门打击网络犯罪的部门——“联合执法机构”，其主要职责是负责对“暗网”网络犯罪行为的预警和打击，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[16]。

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）又专门成立了“暗网情报部”（Dark Web Intelligence Unit）。“暗网情报部”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”中涉及毒品、贩卖人口、儿童性虐待、武器交易和洗钱等非法活动[17]。

3.采用“钓鱼”执法

“暗网”访问的匿名性使得执法部门无法通过使用常规的网络侦察技术，来确定“暗网”访问者计算机的 IP 地址从而锁定访问者的真实身份。因此，“钓鱼”执法常被美欧国家的执法部门作为抓捕“暗网”违法者的重要手段。

“钓鱼”执法一般是执法部门在控制了某个“暗网”非法网站后并不急于将其关闭，而是让其继续运行一段时间，以抓捕更多的违法者。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，在 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，拥有超过 21.5 万名注册用户，内含超过 2.3 万个儿童色情图像和视频链接。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 日控制期间，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[18]。

“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，该论坛的用户人数已经超过 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"执法行动中，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[19]。

4.加强国际合作

"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。在过去几年间摧毁的多个"暗网"非法网站的联合行动中，不同国家间的联合执法发挥了重要作用。

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[20]。2017 年 7 月，"暗网"中最大的非法交易网站"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机关打击涉"暗网"犯罪活动将发挥积极的作用。

四、"暗网"：我国网络空间治理的新挑战

"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。当前，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"这种大型的"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等。

1.传播色情照片视频

2016 年，北京市公安局成功打掉一个利用"暗网"传播儿童淫秽信息的团伙，抓获 8 名犯罪嫌疑人，这是我国警方破获的首例涉"暗网"犯罪案件。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）在境外网站发布大量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。通过技术手段，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[21]。

2.贩卖公民个人信息

2018 年以来，在"暗网"中文论坛出现了多起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，其中涉及 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 10 亿条快递数据，涉及包括寄(收)件人姓名，电话，地址等公民个人信息，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，包括客户的姓名、手机号、入住时间、离开时间、房号等记录约 2.4 亿条，涉及 1.3 亿客户的姓名、身份证号等信息约 5 亿条，以上信息以 8 比特币打包出售；2018 年 12 月 30 日，有人在"暗网"中文论坛售卖某酒店客户数据，涉及姓名、身份证、住址、电话等公民个人信息 30 多万条[22]。

3.浏览境外非法网站

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。为了防止国外不良网络信息流入国内，通常会在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[23]。

对于那些试图浏览被过滤境外网站的人，"翻墙"是突破网络封锁的常用方法。目前，"自由门"（Freegate.exe）"逍遥游"（FreeU.exe）等境外软件公司开发的几款软件，是国内应用最广泛的"翻墙"软件[24]。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。而且，使用"翻墙"软件访问国家禁止访问的国外网站，已经触犯

了国家的法律法规。《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信道进行国际联网。而通过使用 Tor 软件来访问国家禁止访问的境外网站，由于可以很好地隐藏自己计算机IP地址而躲避执法机关的监管，所以近年来成为我国网民用来“翻墙”的重要工具。

为了遏制网络电信诈骗、网络涉枪涉爆、网络赌博、网络淫秽色情、网络侵犯公民个人信息等网络违法犯罪愈演愈烈的态势，近年来我国公安机关连续开展了“打击整治网络侵犯公民个人信息犯罪专项行动”“涉网络诈骗等多发性犯罪网络服务平台专项整治行动”和“净网 2018”等专项行动，查封关闭了一大批非法网站，抓获了一大批涉嫌网络犯罪的不法分子。公安机关对网络违法犯罪活动采取的高压态势，极大地压缩了“明网”中犯罪分子的网络活动空间。在这一背景下，“明网”中的网络违法犯罪活动极有可能全面转入“暗网”这个地下网络空间中。

近年来，新闻媒体对“暗网”事件的频频曝光，将“暗网”不断推向中国公众视野。随着我国访问“暗网”人群的不断扩大和涉“暗网”违法犯罪案件的不断增加，“暗网”已经成为我国网络空间治理的新领域，“暗网”犯罪也给我国网络空间治理带来了新挑战，预防和打击涉“暗网”违法犯罪活动已经成为我国网络空间治理的重要内容。

[参考文献]

[1]暗网毒贩为之疯狂，神秘发明人竟被提名诺奖！[EB/OL]. http://www.sohu.com/a/126563182_117959，2017-02-17.

[2]王佳宁.“暗网”对国家安全的危害[J].网络安全技术与应用，2016，(9).

[3]《新闻周刊》：暗网毒品交易网站“丝绸之路”的兴衰[EB/OL]. http://finance.sina.com.cn/stock/usstock/c/20150225/212421592746.shtml，2015-02-25.

[4]倪俊.从社会治理角度认知暗网的威胁与应对[J].信息安全与通信保密，2017，(11).

[5]陶短房.“暗网”从未消逝[J].方圆，2017，(16).

[6]严言.暗网是一个怎样的世界[N].国际金融报，2015-12-21.

[7]黄伟.暗网世界的黑色犯罪[J].检察风云，2017，(23).

[8]方言.两大暗网黑市覆灭记[J].中国信息安全，2017，(11).

[9]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.

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

[11]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.

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

[13]云贺.怎样打赢暗网攻坚战[J]，财经国家周刊，2017，(16).

[14]李珊.阿尔法湾覆灭背后[N].华商报，2017-08-04.

[15]网络调查技术(Network Investigative Technique)[EB/OL].http://www.arkteam.net/? p=2794，2017-09-29.

[16]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.

[17]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).

[18]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.

[19]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.

[20]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.

[21]刘子珩.揭秘“暗网”第一案背后的暗黑世界[N].新京报，2016-11-25.

[22]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.

[23]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硕士学位论文，2011.

[24]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，(2).

（责任编辑 张 娅）