滋蔓的暗网及网络空间治理新挑战

罗 俊

[摘 要] 21世纪初出现的匿名通信技术为编织暗网提供了基础,比特币的出现又为隐秘交易提供了理想的工具。在短短十年时间里,暗网中已经滋生出形形色色的不道德、病态、违法、犯罪行为,对国家安全、经济安全、社会治理等形成越来越大的威胁。这些行为可分为信息型、信息—交易型、信息—交易—实物型三类。由于暗网中的信息传递、交易支付极难被定位、追踪、监控,因此在侦查、取证等方面的难度远大于传统网络违法犯罪行为,使网络空间治理面临新的严峻挑战。近几年来,暗网已悄无声息地把触角伸入了中国,国内涉暗网违法犯罪开始露出苗头,社会各界需要高度重视其可能带来的多方面的危害性。而暗网治理是全球公认的难题,单纯技术性治理存在局限性,因此需要将多种手段结合起来,采取有针对性的多环节治理、积极推进有效的国际合作、完善表层网络与深层网络的信息安全机制等综合性治理对策。中国式政府主导下的多元主体共治的网络空间治理模式能够更好地适应综合性治理的要求,因此我国应立足于自身国情,充分发挥制度优势,探索暗网治理的中国方案。

[关键词] 暗网;匿名通信技术;加密数字货币;信息安全;技术治理;综合治理

[作者简介] 罗俊,武汉大学社会发展研究所研究员,湖北 武汉 430072

[中图分类号] G203 [文献标识码] A [文章编号] 1004- 4434(2020)05- 0001 -12
DOI:10.16524/j.45-1002.2020.05.001

随着互联网在全球范围的普及,人类社会步入了后信息化时代。借助新一代的信息通信技术,世界实现了突破时空限制的互联互通。现实空间与网络空间的深度融合,形塑着新的经济社会发展形态。与此同时,互联网也造就了21世纪来势汹汹的复杂形势,给社会带来了一系列始料不及的新问题,依托暗网(Dark Net)的不道德、病态、违法、犯罪行为的滋生与蔓延是其中之一。基于匿名通信技术编织起来的暗网,其用户、信息交互内容、交易支付行为极难被定位、追踪、监控,因而受到不法分子的格外青睐。在短短十年时间里,暗网成为充斥贩毒、色情、违禁品交易、洗钱、赌博、网络攻击、恐怖主义等不法行为的"暗黑世界",正对国家安全、经济安全、社会治理等形成越来越大的威胁。涉暗网违法犯罪在侦查、取证等方面的难度远大于传统网络违法犯罪行为,使网络空间治理面临更为严峻的挑战。互联网没有国界,涉暗网违法犯罪从北美、欧洲滋生,继而向世界各地蔓延。近几年来,中国也出现了涉暗网违法犯罪案件,虽然情况尚远不如美国等西方国家严重,但总体上呈现逐年上升趋势。中国社会各界需要高度重视暗网可能带来的顽固性的社会危害,在其尚未形成泛滥之势时深入思考治理对策。而治网必须先懂网,准确认识暗网的支撑技术、发展历史,系统深入地研究涉暗网违法犯罪的特点、现状与趋势,分析国内外暗网治理的方法、路径、效果等极为重要,在此基础上方能充分发挥中国的制度优势,探索出适合我国国情的治理对策。

一、暗网的关键技术:匿名通信系统与加密数字货币

(一)互联网的层次与匿名通信技术

互联网一般被分为表层网络(Surface Net)与深层网络(Deep Net),这种分类所依据的是网络信息内容能否被通用的网络搜索引擎索引。表层网络以通过超链接方式关联起来的网页构成,其信息内容能够被诸如谷歌、必应、百度等搜索引擎索引;深层网络包括动态生成网页、特定情景可浏览网页、非HTML/脚本化内容、未被链接站点、私有站点、被限制访问站点等[1],其信息内容虽然也存储在互联网数据库中,但不能通过超链接访问,通用的搜索引擎无法对其进行索引。暗网是深层网络的一部分,

通常被认为是深层网络的一个子集①。它虽然构建于公共的因特网之上，但用户必须通过特殊的软件、配置或经过特殊的认证才能够登录访问。对于表层网络，网络运营商与服务提供商(ISP)可以通过IP地址等信息确定用户在现实空间的地理位置，进而了解其身份；而暗网采用了匿名通信技术，只能侦测到用户连接到暗网以及通信流量的大小，无法识别用户的IP地址、侦测信息的内容、追踪用户的通信行为。

计算机科学家在设计互联网之初，面向的用户主要是科学研究者，因此并未充分预计到在互联网向社会经济各领域全面普及之后，网络信息安全与用户隐私保护等问题会变得何等重要。基于能够实现多个不同网络之间传输信息的TCP/IP(传输控制协议/网际协议)协议簇，互联网实现了突破时空限制的强大通信能力，但这些协议缺乏足以保证信息在传输过程中不被窃取的安全措施。信息攻击者运用一定的技术手段，不但可以截获用户的通信内容，而且能够清楚地观察到用户之间通信的过程。

对于军方、情报机构等特殊部门来说，利用互联网来传递有保密要求的情报显然是不安全的；对于政府、企业等组织来说，有很多不宜公开的机密信息需要传输；对于普通的互联网用户来说，也有很多隐私性的信息不愿被人知道，例如一些个人疾病的在线咨询、通过互联网进行的电子银行支付等，用户一般不希望与此无关的人掌握这些信息。保密性是网络信息安全的基本要求之一②，而采用匿名通信是实现保密性的有效办法。在通信系统中，匿名(Anonymity)指某一对象在其行动实体(Acting Entity)的集合中不可被识别的状态[2]。例如，在网络上某一信息发送者不能被从信息发送者群体中识别出来，则该用户是匿名的。常见的匿名通信技术有Tor、I2P等，其中又以Tor的应用最为广泛[3]。

1995年，美国海军研究实验室(NRL)的数学家保罗·西维森(Paul Syverson)与计算机科学家迈克尔·里德(G. Mike Reed)、大卫·戈尔德施拉格(David Goldschlag)合作开发了一种匿名通信技术——“洋葱路由”(The Onion Router，Tor)，其初衷是为了给军事情报传递提供一个安全隐秘的网络工具，以及保护使用公共互联网的政府人员与从事开源情报搜集的分析师。1997年，“洋葱路由”交由美国国防高等研究计划署(DARPA)进一步研发。2002年，保罗·西维森又与计算机科学家罗根·丁格伦(Roger Dingledine)、尼克·马修森(Nick Mathewson)合作，基于该技术开发了第一款测试版软件，并将其命名为“洋葱路由项目”(The Onion Router Project)，简称Tor项目，于2002年9月对外发布。2003年，Tor正式版本发布；2004年8月，保罗·西维森等发表了题为“Tor：第二代洋葱路由器”的论文[4]。以下就以Tor为例说明匿名通信系统的技术原理。

(二)匿名通信的多层加密多次转发机制

Tor匿名通信系统由若干路由节点、权威目录服务器(Authoritative Directory Server)、Tor客户端、网桥节点、隐藏服务器组成。路由节点由分布在全球的志愿者提供，所有的路由节点构成一个分布式的覆盖网络。权威目录服务器负责管理所有路由节点，并以一个“共识”(Consensus)列表的形式发布路由节点信息，该表每隔1小时更新1次，每次公布

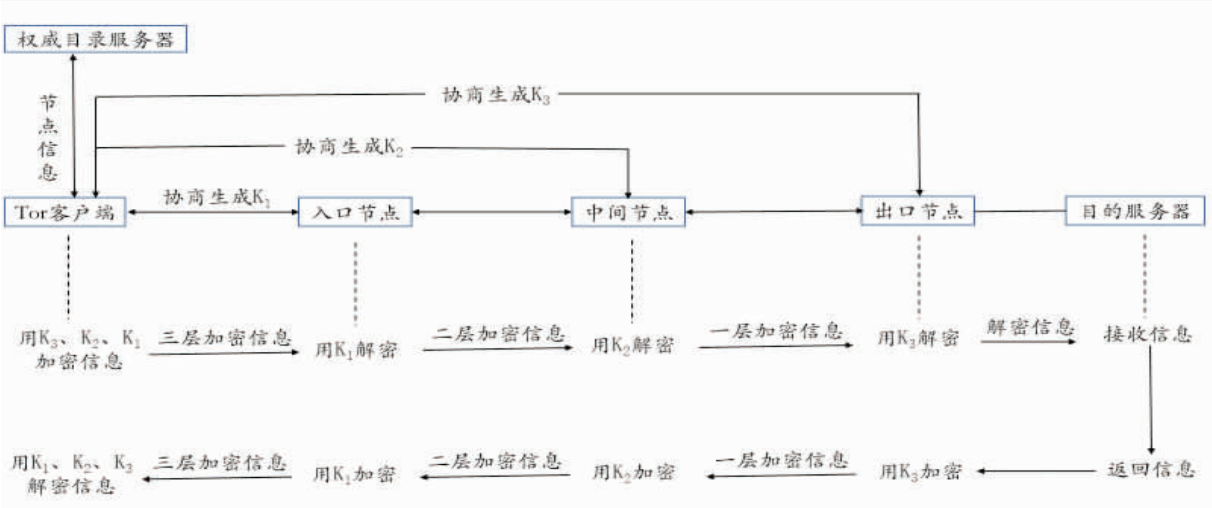

图1 Tor的多层加密多次转发机制

①在一些媒体报道与学术论文中，经常可以看到诸如“表层网络信息仅占互联网信息的4%，暗网中的信息占96%”之类的表述，这是混淆了暗网与深层网络的概念，暗网远远没有那样大的规模。

②一般认为，网络安全要求其通信具备五个属性：保密性、完整性、可用性、可控性和不可抵赖性。

的路由节点只有3个小时的有效期。当前Tor系统中共有约3万个由自愿者贡献的路由节点、9个权威目录服务器。用户使用Tor系统,需要预先下载安装一个Tor客户端。

Tor匿名通信系统在设计之初,就是以不让任何软件侦测到通信主体的IP地址、信息内容与通信过程为目的,因而采用了多层加密多次转发机制,其基本原理如图1。

进行匿名通信时,用户先通过运行Tor客户端来访问权威目录服务器,从"共识"列表中获取路由节点的IP地址、公钥[①]等信息,并采用加权随机的路由选择算法来选择若干路由节点,默认选择为3个(分别称为入口节点、中间节点、出口节点)。Tor客户端与入口节点协商生成共享的通信密钥K_1,以建立起第一段数据传输链路;然后通过第一段数据传输链路与中间节点协商生成共享的通信密钥K_2,以建立起第二段数据传输链路;最后通过第一、二段数据传输链路与出口节点协商生成共享的通信密钥K_3,建立起第三段数据传输链路;出口节点可以连接到目的服务器,由此建立起一条完整的从用户到目标服务器的匿名通信链路。然后,Tor客户端依次使用密钥K_3、K_2、K_1对用户想要发送的信息进行加密,形成三层加密的数据包,数据包就像一个层层包裹起来的洋葱。Tor客户端将三层加密的数据包发送到入口节点,入口节点使用K_1对数据包进行解密,解密后得到的是经过K_3、K_2二层加密的数据包,就仿佛是把洋葱剥掉了一层;继之,入口节点将二层加密的数据包发送到中间节点,中间节点使用K_2对数据包进行解密,解密后得到的是经过K_3一层加密的数据包,就仿佛是把洋葱又剥掉了一层;然后,中间节点将只剩一层加密的数据包发送到出口节点,出口节点使用K_3对数据包进行解密,解密后得到的就是原始信息了,就仿佛剥掉了洋葱的最后一层,露出了葱芯。出口节点将解密后的信息发送给目的服务器;目的服务器作出响应,发出回复信息。回复信息在通信链路中反向传输,也经过三层加密。Tor客户端收到信息后,对三层加密的数据包进行解密,获取目的服务器的回复信息。

通过以上步骤,Tor客户端与目的服务器之间完成了一次通信。在通信过程中,一方面信息的传输经过多次跳转,目的服务器只能侦测到出口节点的IP地址,而无法回溯出信息发送者的IP地址,因而无法对用户进行定位与追踪;另一方面,用户发送的信息内容以及转发路由信息经过层层加密,而只有用户的Tor客户端掌握全部的用于解密的密钥,他人破解密钥获知信息内容的难度极大。

美国军方认为最好有很多不同类型的人也使用Tor系统,这样更有利于隐藏情报人员的身份,故而于2004年发布了Tor的普通用户版本。2006年12月,电子前哨基金会(EFF)接管了Tor系统的继续研发,并负责维护Tor项目。电子前哨基金会是一个非营利的网络自由主义组织,致力于保护受政府权力迫害的美国公民[5]。自此,Tor作为一种免费、开源的程序,被越来越多的政府部门、社会组织、个人用户用作匿名通信与上网的工具,美国军方的情报人员也就隐匿在这些人群之中。

(三)从匿名访问到隐藏服务

借助于Tor系统的多层加密转发机制,用户可以实现对因特网的匿名访问。例如,某位患有艾滋病的用户想去"艾滋病论坛吧"向病友请教问题,但他不愿意暴露自己的身份。此时他就可以使用Tor系统,将"艾滋病论坛吧"网站服务器作为目的服务器,按上述步骤建立起匿名通信链路,则在浏览网页、与人交流时,他的IP地址无法被获取,从而保证其身份不被人探知。随着越来越多的软件乃至操作系统允许用户使用Tor链接发送所有流量,Tor系统的用户得以用各种类型的在线服务来隐藏自己的身份。而2013年前美国中央情报局(CIA)雇员爱德华·斯诺登对美国国家安全局的"棱镜"项目的揭露,使公众开始认识到表层网络几无信息安全可言。并且,斯诺登还曝光了美国国家安全局一份题为《Tor糟透了》的文件,该文件显示美国国家安全局企图彻底破解Tor系统,但发现困难重重,承认"我们永远不能做到随时把所有的Tor用户去匿名化"[6]。这不啻于为Tor系统作了一个全球性的广告,Tor系统的用户量由此快速增加。不少具有一定计算机专业基础的用户开始使用Tor系统,以保证上网时自己的IP地址、通信内容不被人定位、监听。目前,Tor系统的全球用户规模已达300万,已经成为最流行的匿名通信工具。

如果仅仅是被用于匿名访问表层网络的合法网站,Tor系统或许不会带来特殊的社会危害。然而,Tor系统不仅能使用户匿名,还从2004年起开始支持隐藏服务机制,隐藏服务器(Hidden Server)与隐藏服务目录服务器被集成在Tor系统的软件包中。隐藏服务目录服务器存储并为客户端提供隐藏服务器的引入节点(Introduction Point)、公钥等信息。隐藏服务器在启动时会选择3个引入节点,并将引入节点及其公钥信息上传至隐藏服务目录服务器。Tor客户端访问隐藏服务器时,首先建立经

①此处涉及不对称加密技术,限于篇幅本文不就此展开,有兴趣的人文社科学者可参考相关计算机密码学书籍。

3 次跳转的链路访问隐藏服务目录服务器，获取引入节点和公钥信息；继之，Tor 客户端选择一个汇聚节点作为客户端和隐藏服务器通信链路的汇聚点，并将汇聚节点的信息通过引入节点告知隐藏服务器；然后，Tor 客户端与隐藏服务器各自建立到达汇聚节点的链路，搭建经过 6 次跳转的通信链路，即可开始通信。在此过程中，任一节点无法同时获知 Tor 客户端 IP 地址、隐藏服务器 IP 地址以及数据内容，由此保障这类服务器在为 Tor 用户提供各种网络服务（如网络论坛、电子邮件、电子商务）之时，服务提供商与用户都不能被定位、追踪[7]。众所周知，表层网络中的万维网（World Wide Web，WWW）就是基于客户端—服务器模式而编织起来的，有了隐藏服务器，就意味着可以采用匿名客户端—隐藏服务器的模式，编织一个无法用普通软件进入的网络世界，暗网由此诞生。

最初，一些具备计算机技能的极端自由派人士、无政府主义者、持有种族歧视观念者等为主流价值观所不容的群体，由于其言论在表层网络中受到管制，于是他们开始用隐藏服务器搭建网络论坛。这种隐秘的网站无法用谷歌、百度等通用搜索引擎来搜索，必须使用 Tor 这类匿名通信系统才能登录。除了隐秘论坛，暗网上还出现了隐秘聊天室、隐秘电子邮件等服务。此后，这类隐藏服务的方式被不法分子青睐，匿名通信技术被越来越多的人滥用，开始形成越来越严重的社会危害。这有违保护互联网用户的通信内容与行为隐私的初衷，也是美国国家安全局试图破解 Tor 系统的原因。

综上所述，由多层加密转发机制、隐藏服务机制等所构成的匿名通信技术体系，为编织暗网提供了基础。不过，基于这些技术还只能使暗网实现隐秘的信息服务，尚无法进行隐秘支付。2009 年，第一个加密数字货币——比特币的诞生又为暗网提供了一个有力的工具，帮助暗网实现了隐秘交易功能，此后对匿名通信技术的滥用一发不可收拾。

（四）加密数字货币与隐秘网络交易

2008 年美国爆发金融危机，并很快波及全球。美联储采用量化宽松政策向全世界转嫁危机，此举招致很多人的反感，数字加密货币正是在这种背景下诞生的。2008 年 11 月 1 日，中本聪（Satoshi Nakamoto）在计算机密码学网站“metzdowd.com”的邮件列表中发布了一篇题为《比特币：一种点对点的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）的论文，详细阐述了如何基于密码学、区块链、分布式对等网络（P2P）等技术创建一套去中心化的电子现金交易系统。这种系统的目标是实现一种新的交易方式：在交易双方没有建立相互信任，也无任何可信的第三方作为中介的情况下，实现可靠的远程点对点支付。比特币是这种系统生成的一种虚拟的加密数字货币，其与法定货币不同之处在于不依靠某个货币机构发行，而是依据特定的算法在网络节点通过大量的计算生成，因此不受任何国家央行、任何金融机构的控制①。去中心化与算法生成特性可以保证比特币无法通过大量增发来人为操控币值，因此中本聪认为比特币可以使民众免受金融机构滥发货币的掠夺；同时，基于计算机密码学的设计可以使比特币只能被真实的拥有者转移或支付，不需要交易双方的个人信息，因此能够确保货币的所有权与交易的匿名性。

2009 年 1 月 3 日，中本聪开发出首个比特币算法的客户端程序，比特币也正式宣告诞生。中本聪希望这种不受政府监管和控制的货币能够被广泛接受，在全球自由流动。然而，具有匿名、免税、免监管、可跨境交易特点的比特币，很快就衍生出一系列为其发明者所始料不及的问题。加密数字货币的匿名性能够保护交易者的隐私，但也能被用于洗钱等犯罪活动。比特币很快被暗网非法交易网站运营者关注，并被用作实现隐秘交易的工具。

在比特币诞生之前，暗网上就已经出现了进行非法交易的网站，早期最具代表性的是“农夫市场”（Farmer's Market），其在全盛时期号称“非法交易领域的亚马逊”。“农夫市场”网站搭建于 2006 年，最初使用 Hushmail 技术进行私密联络，2010 年后改用 Tor 系统。“农夫市场”经营各种各样的违禁品，其中又以毒品和管制药品为主，以提取佣金的方式获取利润。要实现非法交易，必须要解决支付问题。如果通过银行账户来支付，很容易暴露交易双方的身份，因为世界各国的银行都配备有严密的监控系统。因此，“农夫市场”采用“接力支付”方式来摆脱追踪，通过当时电子商务通用的各种支付模式辗转付款，乃至通过网络游戏账户、虚拟结算平台等进行“接力支付”[8]。然而，“接力支付”并不能完全摆脱追踪。2012 年 4 月，美国缉毒局（DEA）与荷兰、哥伦比亚、苏格兰等地警方和情报部门合作，破获“农夫市场”并逮捕了主要经营者。

“农夫市场”被摧毁后，成立于 2011 年的“丝绸之路”成为暗网世界中最著名的非法交易网站。“丝绸之路”将 Tor 系统与加密数字货币结合在一起，

①我国新近推出的法定数字货币（DCEP），虽然与比特币一样采用了区块链技术，但两者有本质的区别。法定数字货币是中心化的，由中国人民银行发行，是可监管的。

不仅用 Tor 系统来构建网络体系，还引入比特币用于结算，使支付变得更加隐秘且便捷；并且设计了复杂的监督系统实现了交易支付系统的自动托管和自动审查，以确保网站交易的安全可靠。由于运用加密数字货币建立了更为独立、安全的匿名支付系统，“丝绸之路”扩大了营业范围，不仅将洗钱作为其“主流业务”之一，还涉足色情、军火贩卖等多种网络犯罪[9]。此后，比特币成为暗网黑市的主要流通货币。

在比特币之后，莱特币、门罗币等加密数字货币也相继被一些暗网网站使用，当前在暗网中用于交易的加密数字货币已经有十几种[10]。由上可见，暗网网站以互联网为载体，利用匿名通信系统实现了隐秘的信息服务，而此后加密数字货币的出现，又为其提供了安全便捷的交易工具。当通信与交易都能够隐藏踪迹，那些不能在表层网络中进行的违法犯罪活动就开始在暗网中滋生并快速蔓延，造成了多方面的严重的社会危害。

二、暗网的隐秘世界：暗网行为类型及其社会危害

依托暗网的行为可分为三类，一是信息型，二是信息—交易型，三是信息—交易—实物型。信息型指仅靠信息传递就能实现的行为，例如网络引战（Troll）、宣传极端思想等；信息—交易型指需要信息传递与线上支付才能达到目的的行为，例如传播色情视频牟利、贩卖隐私数据、兜售网络攻击工具、组织网络赌博等；信息—交易—实物型指除了利用线上联络、交易，还必须在线下以邮寄等方式进行实物移交才能达到目的的行为，例如贩卖毒品、违禁药品、军火、假钞、假证件、人体器官等。

（一）信息型不良行为

1.网络去抑制负面效应的放大器。在现实社会中，个人受道德准则、社会规范的约束，必须在行为上保持自我约束与自我克制；而在具有匿名性特点的网络空间，由于无须为自己的网络行为承担责任，因此一些人会放松乃至完全丧失自我约束与自我克制，导致行为失范甚至为所欲为，这被社会心理学家称为“网络去抑制效应”（Online Disinhibition Effect）。在具有相对匿名性的表层网络中，网络欺凌与网络暴力现象一直伴随着社交媒体平台的发展成为全球性的“时尚”，“网络喷子”几乎无所不在。由于网络欺凌与网络暴力可能对人（尤其是青少年）造成严重的心理伤害，影响人的健康成长与发展，它已成为互联网时代的社会问题。而暗网具有近乎绝对的匿名性，因此网络欺凌与网络暴力现象更为严重，其最具代表性的是暗网引战。引战指网络用户基于某一言论或事件，通过在网络上发布恶意挑衅的帖子等手段，引诱他人与之辩论，进而在辩论中攻击、嘲弄、猥亵、中伤、侮辱、谩骂对方，使对方受到心理伤害。在暗网的一些论坛上，热衷于引战的匿名者宣称“就是要把快乐建立在别人的痛苦之上”[11]。相较于表层网络的欺凌与暴力行为，暗网引战为了伤害对方更加不择手段，无所不用其极，为从对方的愤怒与痛苦中获得心理满足而乐此不疲。值得注意的是，在暗网引战的人，会把那些挖空心思设计出来的引诱他人上当的“套路”、刻意“创作”出来的极具伤害力的语言、搜寻对方隐私信息的方法带到表层网络之中，从而增强了表层网络中恶意攻击、中伤、诬蔑他人的戾气，乃至发展成为侵害人身权益的“人肉搜索”等违法行为，助长不健康的网络信息内容生态，成为建立网络空间公序良俗的严重阻碍。

2.病态亚文化社群的避风港。在暗网论坛中，有各种各样的病态亚文化社群，如厌食症社群、自残自杀社群等。这类人由于在现实社会中会受到规劝、强制以及一些人的歧视，于是他们躲到暗网之中，结成一个个“志同道合”的群组，在暗网论坛中相约节食，讨论如何自残、自杀。在这类群组中容易出现“维特效应”（Werther Effect）。“维特效应”的提出源于歌德的著名小说《少年维特之烦恼》出版后，在欧洲一度引发模仿小说主人公维特自杀的风潮。社会心理学把这种现象称为“行为传染”（Behavioral Contagion）。这些亚文化社群成员一般都非常团结友爱，他们相互陪伴、倾听，以排遣孤独、释放压力。然而这也正是其具有很大危害性的原因，群组中每个人都沉浸在获得众多支持的假象之中，因而不知不觉中把病态文化当作可接受的生活方式[12]。以这种方式逃离现实社会，虽然使他们避开了一些冷眼与嘲讽，但也在很大程度上失去了获得心理援助与救治的机会。

3.极端思想与扭曲价值观的聚集地。在互联网兴起之初，很多人就意识到它是一个散布言论的绝佳平台，极端自由主义者、极端民族主义者、无政府主义者、种族主义者、邪教徒等为主流价值观所不容的群体也极为重视网络世界带来的新机遇，纷纷在社交媒体等平台开辟出自己的宣传阵地。然而，这些人的言论很快就遭到主流网络媒体平台的封杀围剿，于是暗网成为他们新的聚集地。这类人在现实社会中本属少数，但互联网的全球连通性使世界各地持极端思想与扭曲价值观的人比以往任何

时候都更容易聚集起来，在暗网中形成一个个私密社群。对于加入这些社群的人来说，四周充满了与自己观念相契合的信息，每天都能够与似乎为数众多的“同道中人”交流，其中的意见领袖可以快速高效地散布其“理念”，因而这种社群中会形成很强的“回声室效应”(Echo Chamber Situation)①，很容易制造出“属于自己的真相”，不断强化参与成员的极端、偏见思想。身处这样的回声室中的人，往往在现实社会中难以被发现，而他们更难以凭借自我觉悟跳出思维定式。暗网中这些社群的长期存在，无疑会成为社会的极大隐患。

(二)信息—交易型不法行为

1.色情淫秽信息牟利的载体。在暗网中，各种有违道德伦理的不良嗜好被满足、被放大，例如色情淫秽信息极为泛滥，其中尤以儿童色情网站为甚。为满足恋童癖们的变态爱好，暗网上有人设立了专门的网站，一些丧失人性的歹徒控制无辜的儿童，通过在暗网上贩卖对他们实施性侵害与性虐待的图片、视频来赚取金钱，甚至提供一些超出正常人想象的变态服务，例如只要有人肯付费，就直播按照付费人要求的方式性侵、实施酷刑残害儿童的场面[13]。2017 年 6 月，德国警方破获了当时全球最大的儿童色情网站“极乐空间”(Elysium)，该网站搭建于 2016 年，仅用了约一年时间，就在全球发展了 11 万会员。网站上流通的儿童色情影像，从婴儿到幼童、男孩到女孩、同性与异性之间无所不包；其用户的地域之广、规模之大也令人震惊。据德国警方统计，2018 年，德国至少有 1 万名青少年及儿童沦为性暴力犯罪的受害者；世界卫生组织估计，全球范围内的受害者人数则多达 100 万。很大一部分恋童癖借助暗网观看、交流儿童色情影像，乃至进行儿童性虐待的犯罪行为，暗网为他们躲避追查创造了条件[14]。2019 年 10 月，多国警方联合行动捣毁了一个总部位于韩国的儿童性虐待暗网网站。该网站销售 25 万部儿童性虐待主题的视频，通过比特币进行交易。网站运营者以及来自 12 个不同国家的 337 名用户被起诉。美国、英国和西班牙的官员解救了至少 23 名被该网站用户长期虐待的未成年受害者，但仍有许多受害儿童尚未找到[15]。由于暗网的隐秘性，警方侦破的难度极大，往往是千辛万苦才捣毁了一个色情网站，但犯罪分子轻而易举地又建立起一个。据维基百科近年的数据统计，在暗网上色情网站的访问量仅次于毒品[16]，已经是不断成长的毒瘤。

2.非法数据交易的平台。在互联网时代，数据已经成为一种重要的资源，在人们挖掘数据的巨大价值，使之服务于经济社会发展的同时，通过非法获取数据倒卖牟利的黑色产业链也迅速形成，并且大多数非法数据交易都转移到了暗网。据 360 情报威胁中心的研究，当前在暗网上被非法交易的数据主要有以下几类：(1)实名信息，如姓名、电话、身份证、银行卡、家庭住址等包含实名的信息；(2)账号密码，如各类网站登录账号密码、游戏账号密码、电子邮箱账号密码；(3)保单信息，如保单号、保险信息、车险信息；(4)行为记录，如聊天记录、购物记录、差旅信息；(5)机密文件，如财务信息、合同信息、风险投资信息；(6)用户信息，如邮箱号码、账户列表、QQ 号码、会员列表等不包含真实姓名的信息；(7)电话号码，属于用户信息，如账户名及手机号码、注册号码。其中实名信息是被贩卖最多的一类，占比为 45.2%，其次为账号密码、数据库、用户信息、电话号码、行为记录等。从暗网上数据交易事件的数量来看，其涉及的前九大行业分别是金融、互联网、生活服务、交通运输、IT 信息技术、教育、政府、医疗卫生、电信运营商。买家获取数据后的用途多种多样，其社会危害程度也存在差别。以实名信息(包括政企机构与个人)为例，这类信息主要被用于实施精准营销与精准诈骗。在精准营销方面，保健品、保险、理财、房地产中介等行业是实名信息的主要购买者，在获取数据后，他们基于大数据技术对人群基本属性、行为习惯、商业价值等进行多种维度综合分析，实现精准的用户画像，然后通过电话、短信、邮件、电脑弹窗等方式，针对性地对目标客户精准投放广告。其中老人和学生的个人信息最受欢迎，前者的信息经常会被一些公司用来推销保健品，后者的信息则被一些教育机构用于招生宣传。在精准诈骗方面，如果不法分子购买到了个人的姓名、性别、年龄、身份证号码、住址、电话、婚姻状况、邮箱、微信、存款贷款、购房购车、行踪轨迹、医疗记录等重要信息，就可以依据不同人的不同特点针对性地设计诈骗方式。据中国银联发布的安全提醒，电信诈骗案、盗窃银行卡、非法套现、冒用他人银行卡、网络消费诈骗等案件，有超过 90%是由于个人信息泄露引致，非法数据交易已成为这些犯罪的主要源头[17]。

3.计算机网络黑客工具的交易所。自互联网普及以来，技术黑客就一直在威胁着网络安全，成为难以治愈的互联网顽疾。而暗网为黑客提供了一个

①回声室效应指在一个相对封闭的环境上，一些意见相近的声音以夸张或其他扭曲形式不断重复，令处于其中的大多数人认为这些扭曲的描述就是真正的事实，使之固守于符合自身偏好的信息与观念的“茧房”之中。

绝佳的交流、交易的场所。在暗网中有形形色色的黑客论坛，黑客们不仅可以在这里“切磋技艺”，还可以进行漏洞交易，推销各种恶意软件。例如，Windows 等操作系统的漏洞在黑客论坛上标价叫卖，特洛伊木马、僵尸网络等实施非法网络攻击的工具在这里兜售。一个原本技术并不高超的普通黑客，只要进入了这类论坛，就可以购买或租用各种工具，从而获得快速发起破坏力极大的网络攻击的能力。暗网加速了黑客技术的扩散，不仅扩大了对网络安全的威胁，还衍生出了诸如网络勒索之类的新型犯罪，其最典型的案例是“想哭”(WannaCry)勒索病毒事件。事件源起于 2017 年 4 月，黑客组织“影子经纪人”(Shadow Brokers)宣布在暗网上成功入侵了美国国家安全局的网络战武器库，并公开叫卖窃取的网络攻击工具。其中有一款名为“永恒之蓝”(EternalBlue)，可以利用 Windows 操作系统的危险漏洞来获取系统最高权限。有不法分子对“永恒之蓝”进行改造，制成能够用加密方法锁定被攻击计算机内文件的蠕虫病毒。感染该病毒后，用户无法打开自己的文件，而如果想恢复这些文件，就要按照不法分子提供的账号，支付价值 300 美元的比特币。2017 年 5 月 12 日，不法分子发动网络攻击，导致了一场全球性的互联网灾难。据事后统计，至少 150 个国家、30 万名用户的计算机被锁定，影响涉及金融、能源、医疗、科研、教育等众多行业，造成的损失达 80 亿美元。此后，网络安全专家虽然找到了阻断攻击的办法，但已造成的损失无法挽回。因为“想哭”勒索病毒的命令控制(Command—and—Control，C&C)服务器部署在暗网，无法对其进行定位、追踪[18]，所以尽管多国警方通力合作展开侦破，但犯罪分子至今仍逍遥法外。

(三)信息—交易—实物型不法行为

信息—交易型不法行为是通过信息传输与信息类商品的交易来实现，因此可以在互联网这一信息载体上完成；而对于实物类的非法交易，其实物移交无法通过网络来实现，因此必须要线上—线下相结合才能完成。当前，在暗网中最为猖獗的是毒品、违禁药品、枪支、假钞、假证件等非法交易，此外还有贩卖人口、人体器官等犯罪活动，这类行为一般采用类似于表层网络中电子商务平台的方式。此外，恐怖主义分子也转向利用暗网来策划、组织恐怖活动。

1.隐秘黑市：暗网中的非法交易网站。在已知的暗网黑市中，最先出名的是美国人罗斯·乌布利希(Ross Ulbricht)于 2011 年 1 月搭建的“丝绸之路”网站。乌布利希起初打着“拥护自由主义”“维护自由理想”“保障监督与批评权利”的旗号，继之又宣称要创建一种完全不受统治的、彻底自由开放的经济模式，以使人们体验一个没有系统化权力的世界。但不久之后，“丝绸之路”就转向了贩毒等非法交易。由于此前有“农夫市场”这类网站在暗网上培育起了相当规模的毒品买卖人群，“丝绸之路”很快在毒贩圈中传播开来，不断有贩毒者前来入驻，买家们也接踵而至。乌布利希给买卖双方提供服务，收取 8%~15%的手续费。乌布利希还参考亚马逊网站为“丝绸之路”建立起完善的购物机制，包括互评机制、客户论坛、交易纠纷解决机制等。“丝绸之路”发展迅猛，注册用户很快超过了100 万，交易商品从毒品向各种违禁品拓展，上架商品超过 1 万种，其中约有 70%是毒品，其他包括枪支弹药、假钞、假护照、假驾驶证、盗用的信用卡信息等，甚至还有来自十几个国家的杀手。此外，这种网站还无疑是犯罪分子绝佳的销赃场所。在两年多时间里，“丝绸之路”销售了价值 12 亿美元的违禁品，乌布利希从中赚取了 8000 万美元的佣金。“丝绸之路”比“农夫市场”更为猖獗的犯罪活动引起了美国联邦调查局的注意，他们派遣卧底假冒毒品买家潜入“丝绸之路”，尝试利用技术手段找到网站运营者的踪迹，但困难重重。最终，乌布利希不慎在表层网络暴露了蛛丝马迹，以及在邮寄一批假证件时无意中泄露了自己的地址，于 2013 年 10 月被美国联邦调查局抓获。

乌布利希的落网并不意味着暗网黑市会有所收敛，仅一个月后，乌布利希的追随者布莱克·本特霍尔(Blake Benthall)就在暗网上推出了“丝绸之路 2.0”。美国联邦调查局用了一年时间跟踪“丝绸之路 2.0”的服务器和用户，终于在 2014 年 11 月联合欧洲刑警组织将其捣毁，本特霍尔被捕认罪。对于如何破获“丝绸之路 2.0”，警方未予公布，有人猜测警方或许是利用了 Tor 的某个未知漏洞，查获了隐藏网站的 IP 地址[19]。仅 2 个月后，一个名为“重生丝绸之路”(Silk Road Reloaded)的非法交易网站又在暗网上线，它在技术上有了进一步的提高，采用了比 Tor 匿名性更强的 I2P(Invisible Internet Project)技术，除比特币外，它还支持多种数字加密货币支付，不过，一年后“Silk Road Reloaded”因经营不善而倒闭。2016 年 5 月，另一家暗网网站“加密市场”(Crypto Market)变成了“丝绸之路3.0”，各种非法交易的买家卖家又纷纷迁入这个暗网黑市[20]。乌布利希与本特霍尔的前车之覆，并未对从事非法交易的后来者起到足够的警示、震慑作用，而是更多地促使他们在匿名通信技术方面进一步加强，在线下行

为方面愈加谨慎。一个暗网非法交易平台被捣毁，很快就会有新的平台来填补，并且侦破难度越来越大。“丝绸之路 3.0”至今仍在运营，暗网上这类网站还在增加。

2.恐怖主义分子的新工具。自 21 世纪初始，恐怖主义就已经把互联网作为自己的工具。起初，恐怖主义分子主要是利用互联网进行内部联络、组织恐怖活动，在表层网络宣传极端思想、散布恐怖信息、招募人员等。恐怖主义这种网络化的趋势，很快引起了世界各国的国家安全机构、反恐部门的高度重视，迅速调集力量对恐怖分子网站、社交媒体中恐怖主义分子开辟的论坛等进行密切监控。2009 年，联合国反恐任务实施力量工作组(CTTTF)将网络恐怖主义犯罪行为界定为四类，即网络恐怖袭击、利用互联网传播恐怖活动相关非法信息、利用互联网进行恐怖活动联络和资助恐怖活动、利用互联网收集信息和获取技术[21]。由于在表层网络的行为容易受到定位、跟踪、追溯，随着网络反恐手段的不断提升与完善，恐怖分子进行以上犯罪行为的风险越来越大。例如“伊斯兰国”(ISIS)在表层网络的一举一动都受到各国的密切监控，各国都采用有效的技术手段屏蔽或过滤极端主义内容，并且通过 IP 地址定位等手段对恐怖分子实施追踪、抓捕。在这种情况下，暗网无疑为恐怖分子提供了一个更为理想的工具。近几年来，恐怖分子的活动向暗网转移，暗网的隐秘信息服务与隐秘交易功能为恐怖活动提供了前所未有的便利，给打击网络恐怖主义带来了新的严峻挑战。当前，暗网恐怖主义活动主要有以下几类。

(1)内部联络与对外宣传。暗网为恐怖分子提供了一个安全的内部联络工具，使他们能够隐秘地进行信息交流、更为广泛地串联，以策划、组织、部署、实施恐怖活动。恐怖组织还利用暗网宣传极端思想[22]，例如基地组织在表层网络的宣传活动遭到打击之后，于 2015 年 12 月在网上发布“Tor 浏览器安全指南”(Tor Browser Security Guidelines)，详细讲解如何下载、安装和使用，引导目标用户向暗网转移，并教授如何防范被反恐部门定位与确定身份。恐怖组织还将表层网络的宣传信息备份到暗网网站上，当表层网的网站被封杀时，就通过匿名论坛、聊天室或者电子邮件发布暗网上镜像网站链接地址，指引成员和支持者前往。例如，2015 年 12 月，伊斯兰国恐怖分子在法国巴黎策划实施枪击爆炸事件，随后迅速将其宣传机器——生活媒体中心(Al-Hayat Media Center)转移到了暗网，并在 Shamikh 论坛上发布了访问方法。该网站即是一个镜像网站，镜像了许多公告栏的信息，包括多年来积累的多国语言翻译的视频和文件[23]。

(2)人员的招募与培训。恐怖组织还在暗网上招募新成员，并为世界各地的追随者提供技能培训，例如设置如何制造炸弹、如何实施恐怖袭击等培训课程，其中尤以培训“独狼式”袭击者造成了巨大的社会危害。“独狼”指在网上受恐怖主义等激进教育，自购或自制武器装置，并独自发动恐怖袭击的人。由于暗网的匿名性，反恐部门无法知晓哪些地方有哪些人被恐怖组织成功洗脑，因此“独狼式”袭击具有潜伏周期长、随机性大的特点，令安全部门防不胜防，依靠传统的反恐模式难以应对。由上可见，恐怖组织借助暗网的世界连通性和匿名性，极力在全球范围内扩散恐怖主义，使反恐形势愈加严峻。

(3)募集与转移资金。恐怖组织筹集资金的方法除了石油出售、走私、绑架等传统方式，近年来又借助数字加密货币与暗网衍生出了新的方式，例如以比特币募捐、网络勒索、人口贩卖、器官交易。一个自称与“伊斯兰国”有关的美洲恐怖分子小组在进行线上募资时声称：“人们不可能将一家银行转移给圣战组织，在异教徒政府统治下的圣战者应该意识到，一个可能的方式就是使用比特币进行匿名捐助，这能够为圣战提供价值数百万美元的比特币财富，每一个圣战者口袋里的每一分钱都将化为支持圣战的不竭动力。”[24]打击恐怖组织的黑客组织 Ghost Sec 曾追踪到一个价值 300 万美元的比特币钱包，证实数字加密货币已成为恐怖组织筹集资金的新渠道。比特币适合于洗钱的特点也被恐怖分子充分利用，例如“伊斯兰祈祷团”接受的资金均经由“暗网”的比特币交易平台，而“奋斗伊斯兰无痕基金”(Fund the Islamic Struggle without Leavinga Trace)则将圣战募捐资金转化为比特币的暗网镜像，通过名为“比特币与暴力抗争的福音”(Bitcoin and the Charityof Violent Physical Struggle)操作教程来指导如何使用暗网进行秘密金融交易[25]。此外，恐怖组织还利用暗网平台的非法交易赚取金钱，如贩卖人口、性奴，出售洗劫而来的古董、从俘虏身上摘取的人体器官等。

(4)购买武器与破坏装置。暗网黑市早已成为恐怖分子的“军火库”，在“丝绸之路”这类非法交易网站，可以较为容易地买到枪支弹药。例如“伊斯兰国”进行巴黎暴恐案的武器就是通过暗网购买的，据斯图加特检察官办公室(Stuttgart Prosecutor’s Office)的官方文件，枪械贩卖方是德国暗网销售商“DW Guns”。此外，一些比枪支更为危险的物品也

在进入暗网黑市。2016年4月,美国总统奥巴马在华盛顿对来自50个国家的元首和外交部长致辞中,描述了恐怖组织如何在暗网上购买铀、钚等核材料,并称如果恐怖分子通过无人机对平民区散播放射性物质,那将是美国最大的反恐噩梦[26]。

三、暗网的跨界治理:技术性治理悖论与综合性施治

由于互联网突破空间限制实现了全球互联,所以暗网极大地扩展了非法交易等犯罪活动的边界,其威胁也必然是世界性的。美国兰德公司就曾在其暗网研究报告中指出,暗网所构成的威胁不受地域限制,因此中国可能与其他国家一样面临危险,可能有中国的违法交易者活动于一些英文暗网网站上[27]。随着Tor、I2P等匿名通信系统的日益成熟,互联网用户接入暗网的技术门槛越来越低,操作也越来越简便。起初,国内接触暗网的大多是具有一定计算机专业知识的年轻人,但随着各种使用暗网的工具逐渐从境外流入,使中国互联网用户不再需要特别复杂的安装操作就能访问暗网;并且国外的暗网开发组织还研发了基于智能手机的应用程序,借助移动端扩大暗网的使用群体,导致暗网用户开始出现平民化趋势。公开报道显示,中国破获的首起涉暗网犯罪是2016年国内用户通过境外暗网网站传播强奸、猥亵女童视频牟利的案件[28]。从近几年国内破获的案件来看,起初是少量具有相当英语水平与计算机专业知识技能的中国用户接触到了境外的暗网网站,并有人开始参与非法交易;此后滋生出暗网中文网站,这意味着在降低技术门槛之后又去除了语言方面的障碍。虽然中国暗网用户的规模还远不及北美与欧洲,但随着进入门槛的降低,很可能导致暗网的进一步蔓延。当前,国内涉暗网违法犯罪中最突出的是非法数据倒卖与色情淫秽信息牟利[29],其他一些非法交易也开始露出苗头,其社会危害性已不容忽视,暗网正在成为中国网络空间治理的新领域。由于独特的国情,中国的暗网治理必然有其特殊性。因此,既要有选择性地借鉴西方国家的治理经验,更要注重最大程度地发挥中国的制度优势,探索适合中国具体情况的治理路径。

(一)技术型治理:暗网测绘与去匿名化

暗网治理是全球公认的网络空间治理难题,由于涉暗网违法犯罪具有高技术性、高隐蔽性、跨国性等特点,对其实施监管的难度极大,尤其是在侦查与取证方面。由于暗网中的不法行为,不论是信息传递还是交易都是隐秘进行,极难用技术手段拦截其信息,即便拦截也难以破译,因此侦查难度远大于表层网络案件。目前,虽然有美国破获“丝绸之路”“阿尔法湾”,荷兰破获“汉萨”,德国破获“华尔街市场”等打击暗网非法交易平台的成功案例,但相较于暗网中数百个比较活跃的网站,当前破获的暗网犯罪仍只是少数,并且这些案件的侦查耗费了大量的人力、财力。由于无法攻破加密技术,警方有时是抓住了不法分子因疏忽大意而漏出的破绽;有时则是采用钓鱼、卧底等手法,例如设立虚假的非法交易网站,引诱非法购买者上钩;有时是假扮购买者与暗网网站上卖家联系,伺机获取有用信息。由于暗网动态性极强,通信链路与服务器不断更换,因此非法交易过程的电子数据无法取证;即便抓住了罪犯,只要罪犯不供出密码,有些证据也无法获取。鉴于产生以上难题的根源在于暗网所采用的匿名通信技术与数字加密货币技术,因此政界、学界不少人认为应该依靠技术突破来从根本上解决问题。当前,暗网的技术性治理主要围绕以下两个方面展开。

1.通过测绘掌握暗网的总体状况。虽然极难对暗网中的隐藏服务器、匿名访问者进行定位、追踪,但通过技术手段还是能够了解一些基本情况。通过对暗网入口、链接、内容的检测与采集,能够在一定程度上掌握暗网的使用人数、网络结构、数据资源、交易规模等。例如,知道创宇研发的“暗网雷达”以技术手段持续测绘暗网,通过构建分布式暗网节点监控、服务发现、内容采集、弱点探测、智能监测、情报研判、证据保存等平台,实现对暗网服务的发现、识别、分类、采集、监测功能,以及挖掘威胁情报、提供监测和分析服务[30]。此外,对暗网网站所有的历史数据进行快照存档,并进行数据关联性分析,也可以发现暗网活动的蛛丝马迹。

2.研发去匿名化技术。网络安全研究人员正不断研发可识别隐藏服务、用户的去匿名化技术。当前运用的主要方法有两种:一是寻找Tor、I2P等匿名通信系统的技术漏洞(转发协议的漏洞、编写代码时出现的纰漏等),利用这些漏洞实现去匿名化,例如转发协议可能存在漏洞,导致某些标识没有完全被清除,就可以利用这个标识来定位消息发送者;二是在暗网中部署一些留有后门的路由节点,暗网需要大量分布式的路由节点,监测者可以加入进去。自己的节点是可以监控的,因此当监测者的节点被选中时,就可以监测到转发信息的流量甚至截获信息内容。

总体来说,当前暗网的技术性治理主要致力于暗网隐藏节点发现、隐藏服务定位、暗网用户的网

络行为分析,以及暗网流量追踪和通信关系确认等。技术手段上的突破无疑是打击暗网违法犯罪的关键之一,然而仅凭技术手段治理暗网其实无法从根本上解决问题,因为技术性治理存在固有的局限性。

(二)技术性治理悖论:匿名与去匿名技术的对抗赛

在通信过程中保护信息安全是一种广泛的现实需要。任何一个国家、组织都会有一些需要保守的机密信息,企业有自己的商业秘密,普通公民也有属于自己的隐私。这些都是正当合理的需求,并且在一些特殊领域,信息保密至关重要,例如军事指挥和控制系统,必须以隐秘通信来保证其免受敌人的识别和攻击。除非从国家到个人都放弃使用功能最强大、效率最高的互联网来传递信息,否则就会面临网络信息安全问题。从匿名通信技术的代表Tor系统的发展史来看,它首先是为满足军方、情报部门保密传输的需要,继之被扩散到特殊群体,然后对普通用户开源,最终成为违法犯罪分子的有力工具。这实际上显示出作为最先进的信息工具的互联网自身存在一个悖论,一方面人类社会的发展需要高效的信息通信技术,至少在当前与可预见的未来,互联网具有无可替代的作用;另一方面互联网的技术特点又决定了使用常规通信方式几无信息安全可言,因此匿名通信技术是一个不可或缺的补充,但匿名通信技术的滥用又会衍生出一系列极具危害性的暗网违法犯罪行为,成为人类社会发展的阻力与破坏力,人们不得不耗费大量的人力物力来应对来自暗网的威胁。

互联网悖论决定了暗网技术性治理的悖论。一方面,致力于防范互联网信息被恶意侵犯的计算机专家在不断改进、优化匿名通信技术,进一步完善匿名通信系统,以满足国家、企业、个人的信息安全需要;另一方面,致力于对抗暗网违法犯罪势力的研究人员在千方百计地寻找匿名通信技术的漏洞,想尽一切办法实现去匿名化。由此,在网络空间形成了匿名通信技术与去匿名技术的对抗赛,并且这种比赛还将长期持续下去。

在技术对抗赛的背景下,暗网违法犯罪分子与执法部门之间"道高一尺魔高一丈"的技术攻防战也将继续下去。例如,执法部门研究Tor等匿名通信系统的技术漏洞,违法犯罪分子则不断填补漏洞。事实上,暗网网站在这种攻防战中不断升级,如今的暗网黑市已不仅仅有"丝绸之路"这类集中式管理的网站,还有将商品、信息、支付、反馈流程分散的网站,从技术上破解的难度越来越大。

由上可见,虽然对暗网进行测绘、研究去匿名化技术是应对网络威胁的最直接的手段,各国政府也正在促进相关研发工作,但想以此来实现对暗网的有效监控和治理,可能在某一时期收到显著成效,但不可能一劳永逸地解决暗网问题。即便最后计算机专家攻破了Tor、I2P等现有的匿名通信系统,新的匿名通信技术也会很快出现,开发者可能是军方、情报部门的专家,也可能是民间的计算机高手或黑客。对于暗网的另一个关键支撑技术加密数字货币来说,情况亦是如此,即便能够研发出将比特币去匿名化的技术,也无法保证不出现"中本聪2.0"。所以,单纯通过技术性治理来解决暗网违法犯罪问题实际上是不够的。当然,这并不是说不需要技术性治理,而是说还必须采用其他手段。

(三)综合性治理:多环节、跨国界与信息安全机制建设

治理危害社会的行为,一是通过教育等正向引导的方式,二是依靠舆论压力、法律强制力进行抑制。暗网并不是不法行为产生的根源,而是因为削弱了对不法行为的抑制力,从而起到了放大器与催化剂的作用。暗网中所有的具有社会危害性的行为,从网络欺凌到色情交易,从毒品贩卖到恐怖主义,其实都先于暗网出现。因此在暗网治理中,应该将多种手段结合起来,实施综合性治理。

1.多环节治理。互联网用户从接触暗网到参与不法行为需要经历一个过程,各种违法犯罪行为也有多个环节。在单纯技术性治理存在局限性的情况下,需要针对各种不良行为、违法犯罪行为的特点,从各个环节着手,采取多环节治理的方式。对于信息型行为,要向社会公众普及暗网基本知识,使公众认识暗网的危害,呼吁公众尤其是未成年人远离暗网,从而最大程度地抑制暗网的蔓延。对于信息—交易型行为,要从信息源头开始治理,例如,对当前我国最为严重的非法数据交易,要设法切断不法分子的数据来源。数据泄露主要有三种情况,一是个人缺乏保密意识,无意中泄露隐私信息;二是掌握数据的机构、企业的风控意识淡薄或风控措施不力,其数据存储设备遭网络黑客攻击导致泄密;三是数据保密制度缺失或监管存在漏洞,内部人员利用职务之便,私自出卖自己企业、客户的信息牟利。如果有效阻断信息的源头泄露,暗网上自然就不会有这类信息商品。这需要公众提高用户保密意识,有效保护个人隐私;需要数据掌握者切实负起责任,采取有效措施保障数据安全。对于信息—交易—实物型行为,卖家先要获取实物,支付后还要通过实物移交才能完成交易,因此可以通过加强违禁品管制,加强物流行业的监管来斩断黑色产业链条,这需要通过合理的制度安排调动多方面的力量

2.加强国际合作。暗网没有国界,对暗网的治理有赖于开展积极有效的国际合作,以使世界各地通力围剿暗网违法犯罪行为。当前开展国际合作的主要障碍在于不同国家和地区在政策、法律、制度和技术上存在差异,其中尤其是追求网络霸权的技术大国,一直将互联网武器化,利用暗网进行意识形态渗透,在全球培训政治异见分子,借助暗网与告密者和持不同政见者沟通,实现个人与公众匿名交流和共享文件,甚至采用黑客手段来挖掘政治人物的污点。在暗网中有目的地从事针对某一国家的反政府、反社会的宣传串联活动,如西亚、北非和中东一些国家发生革命或动乱,策划者在当事国家屏蔽舆论信息的情况下,利用暗网突破了政府封锁,鼓动民众参与,进而加剧社会混乱,加速政权更迭[31]。正因如此,其对全球暗网治理的态度模棱两可,一方面不愿放弃暗网这一武器,另一方面又因自身遭受非法交易的危害、恐怖主义的威胁等而不得不应对。在这种情况下,致力于建设人类命运共同体的中国应当争取国际网络空间治理话语权,旗帜鲜明地反对侵犯他国网络主权的行为[32],积极推进建立全球范围内应对暗网违法犯罪的综合性国际法律和机制,同时加强与联合国相关机制、议题之间的互动和协调[33]。倡导建立多方、透明和民主的互联网治理机制,推动制定网络空间行为规则,规范各类主体行为,加快建立网络空间新秩序。

3.完善表层网络与深层网络的信息安全机制。用户使用互联网都会有一定的目的,使用表层网络与深层网络的目的一般是正当合法的,而使用暗网的目的大部分是不正当、不合法的。在当前的暗网使用行为中,正当的目的主要是保护合法的企业机密、个人隐私等。正是因为暗网能够有效保护用户的合法信息,所以有人以此为暗网辩护。例如,运营Tor项目的电子前哨基金的负责人称,匿名通信系统在保护用户合法权益方面具有不可替代的作用。必须承认,表层网络与深层网络的信息安全机制存在重大缺陷,这无疑为暗网的存在提供了充足的理由。正因如此,世界大多数国家的法律法规尚未完全对暗网访问与隐私保护之间的问题作出更为明确的规定。因此,对暗网的治理还需要有更深层次的思考,如果能够通过网络技术的改进与合理的制度安排,在表层网络与深层网络建立起可靠的信息安全机制,则互联网用户的一切合法使用行为就无须依靠暗网。在这种情况下,公众对暗网的使用就真正失去了正当性,就可以通过严格清晰的法律来使公众远离暗网,不仅能够有效控制暗网的蔓延,并且在打击暗网违法犯罪方面可以采取更为严厉的手段。当然,在表层网络与深层网络建立可靠的信息安全机制是一项浩大的工程,甚至是要实现“互联网自我革命”,实现这一目标需要依靠一系列的技术创新与制度创新,可谓道阻且长。但是,破解“互联网悖论”将最大程度地遏制暗网违法犯罪等负面效应,营造出一个清朗安全的网络空间,因此值得尝试并为之付出艰苦的努力。

四、代结语:暗网的全球治理与中国方案

在设计互联网之初,计算机科学家并未也不可能充分考虑其在成为人类最主要的信息通信工具后所需要的信息安全保证。20世纪末,美国军方着手研发匿名通信技术,以满足军事与情报部门隐秘传输信息的需要。此后,匿名通信技术逐渐向外扩散,直至对普通互联网用户开源。借助于匿名通信系统,一个个隐秘网站被搭建起来,编织成了通用搜索引擎无法索引的暗网。而基于区块链技术、对等网络技术的加密数字货币的出现,又实现了去中心化、可匿名、点对点的支付,为隐秘交易提供了理想的工具。当通信与交易都能够隐藏踪迹,那些不能在表层网络中进行的活动,就开始暗网中滋生并不断蔓延。经过大约十年的时间,暗网中出现了各种不道德、病态、违法、犯罪行为,造成多方面的、巨大的社会危害,暗网已然成为新型网络威胁。互联网没有国界,暗网的威胁也必然是全球性的。近几年来,暗网已悄无声息把触角伸入了中国。虽然中国暗网用户的规模还很小,但随着Tor、I2P等匿名通信系统的日益成熟,互联网用户接入暗网的技术门槛越来越低,操作也越来越简便,有可能导致暗网的危害进一步蔓延。社会各界对此应予以高度重视。

对暗网实施监管的难度极大,对其治理是全球公认难题,尤其是对涉暗网违法犯罪案件的侦查与取证面临重重困难。难题产生的根源在于暗网所采用的匿名通信技术与数字加密货币技术,因此从技术上寻求突破被作为关键手段之一。然而,由于互联网在信息通信与信息安全之间的悖论,技术性治理实际上会形成匿名通信技术与去匿名技术的对抗赛,以及暗网违法犯罪分子与执法部门之间的技术攻防战。

在单纯技术性治理存在局限性的情况下,应该将多种手段结合起来实施综合性治理。首先,互联网用户从接触暗网到参与不法行为需要经历一个过程,各种违法犯罪行为也有多个环节,因此可以针对各种违法犯罪行为的特点,从各个环节着手,

采取多环节治理的方式；其次，暗网治理需要开展积极有效的国际合作，以使世界各地通力围剿暗网违法犯罪行为，中国应当争取网络空间国际治理话语权，积极推进建立全球范围内应对暗网违法犯罪的综合性国际法律和机制；最后，对暗网的治理还需要有更深层次的思考，探索如何通过网络技术的改进与合理的制度安排，在表层网络与深层网络建立起可靠的信息安全机制，使互联网用户的一切合法使用行为无须依靠暗网，通过严格清晰的法律来使公众远离暗网，从而有效控制暗网的蔓延。

暗网正在成为我国网络空间治理的新领域。我国有着与欧美国家截然不同的国情，在网络空间治理理念上也有鲜明的差异。美国、欧盟偏向于通过非政府行为主体方式进行治理，而我国力图构建政府主导下多元主体共治的格局。对暗网实施综合治理，要求行政部门、司法部门、互联网企业、科研机构、教育机构、社会公众等多元主体的积极参与高效协同，我国在政府主导下的多元主体共治模式能够更好地适应这种要求，而欧美基于“以多利益攸关方”的治理模式虽然在某些方面有其优势，但常常因为多方的利益博弈而削弱其治理效能。例如，美国对待匿名通信系统扩散与加密数字货币监管的模棱两可的态度，其实就是多方利益博弈的结果。因此，我国在探索暗网治理的可行对策时，一方面要注意借鉴欧美国家的有益经验，另一方面更要立足于中国的国情，充分发挥自身的制度优势，探索出暗网治理的中国方案。

[参考文献]

[1]Ciancaglini V,Balduzzi M,Goncharov M,etc.Deepweb and Cybercrime_It's not all about TOR [R]. Cupertino: A Trend Micro Research Paper,2013.

[2]谭庆丰，时金桥，王学宾.匿名通信与暗网[M].北京：科学出版社，2019：3-4.

[3]How Big is the Dark Web [EB/OL]. https://trac.torproject.org/projects/tor/wiki/doc/How Big Is The DarkWeb,

[4]Dingledine, R. Mathewson, N. Syverson, P. Tor:The Second-Generation Onion Router [R]. San Diego, CA: 13th USENIX Security Symposium,Aug 09-13,2004.

[5]黄伟.暗网世界的黑色犯罪[J].检察风云，2017(23).

[6]钱童心.暗网强大到设计者都无法销毁 中国也可能有风险[N].第一财经日报，2017-08-23.

[7]罗军舟，杨明，凌振，等.匿名通信与暗网研究综述[J].计算机研究与发展，2019(1).

[8]陶短房.“暗网”从未消逝[J].方圆，2017(16).

[9]方言.两大暗网黑市覆灭记[J].中国信息安全，2017(11).

[10]米沃奇.被“抛弃”的比特币与前赴后继的暗网新宠[J].电脑知识与技术，2018(8).

[11][12]杰米·巴特利特.暗网[M].刘丹丹，译.北京：北京时代华文书局，2018：236-241.

[13]意大利恐怖“暗网”：未成年人付费看虐童直播[EB/OL]. http://finance.sina.com.cn/chanjing/cyxw/2020 -07 -20/doc-iivhvpwx6428927.shtml?cref=cj，2020-07-20.

[14]姜姝.德国宣判全球最大“暗网”儿童色情网站案[EB/OL].http://finance.sina.com.cn/roll/2019 -03 -13/doc -ihsx-ncvh2018589.shtml，2019-03-13.

[15]汤晨.全球范围内逮捕数百人 多国警方联合行动捣毁韩国一大型儿童性侵暗网[EB/OL].http://www.thecover.cn/news/2831188，2019-10-17.

[16][28]常鑫.大学生境外传播儿童淫秽视频 受害者均来自农村[EB/OL]. https://xw.qq.com/edu/20161110005629-00，2016-11-10.

[17]2018 年暗网非法数据交易总结[EB/OL].http://www.100ec.cn/detail——6492707.html，2019-01-22.

[18]朱慧容.勒索病毒背后的比特币“暗网”疑云：普通人难以触及 [EB/OL].http://www.chinanews.com/gj/2017/06-04/8241498.shtml，2017-06-03.

[19]惜辰.丝绸之路 2.0 被封 俄毒品黑市 RAMP 何以逍遥法外? [EB/OL]. https://tech.163.com/14/1116/23/AB77-R0BO000915BF.html，2014-11-16.

[20]史中，方枪枪.暗网电商“丝绸之路”第 4 次上线 仍以毒品交易为主[EB/OL]. http://m.haiwainet.cn/middle/354-1839/2016/0516/content_29928948_1.html，2016-05-16.

[21]United Nations Coounter-Terrorism Implementation Task Force Working Group Report (CTTTF). Countering the Use of the Internet for Terrorist purpose[R].2009.

[22]张伟伟，王万.暗网恐怖主义犯罪研究[J].中国人民公安大学学报(社会科学版)，2016(4).

[23][25]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(1).

[24]Danna Harman.U.S.-based ISIS Cell Fun Draising on the Dark Web,New Evidence Suggests[N].Haaretz,2015-01-29.

[26]陈森，刘永茂.网络反恐任重道远[N].解放军报，2017-09-08.

[27]刘峣.暗网深几许[EB/OL]. http://world.people.com.cn/n1/2017/0811/c1002-29463726.htm，2017-08-11.

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

[30]知道创宇 404 实验室.2018 上半年暗网研究报告[EB/OL]. https://paper.seebug.org/686/，2018-09-04.

[31]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).

[32]匡文波，童文杰.治理之道：携手构建网络空间命运共同体[N].人民日报，2017-06-01.

[33]刁世峰.“暗网”毒瘤 得全球联手铲[N].人民日报海外版，2019-07-22.

[责任编辑：戴庆瑄]