暗网犯罪的趋势分析与治理对策

明乐齐*

内容摘要：随着互联网技术的蓬勃发展，网络违法犯罪日益凸显，其中以暗网为代表的网络犯罪，因其独具一格的犯罪形式和特点更加活跃猖獗。犯罪分子利用其隐蔽性强的特点，肆意在暗网进行恐怖宣扬、毒品交易、贩卖人口、武器倒卖、色情服务、数据泄露和公民个人信息买卖等违法犯罪活动，给国家和社会造成了极大的威胁和安全，更给人民群众的财产带来重大损失。为此，只有不断深化技术创新，挤压暗网生存空间；注重源头治理，铲除暗网滋生链条；强化侦查打击，遏制暗网高发势头；加强国际合作，推动打击成果效能；健全立法管制，提升打击的纵深度。通过深化暗网的技术管控与治理，加大对暗网犯罪的打击力度，不断完善和创新打击惩治的新机制、新办法，真正还互联网络一个晴朗的明天。

关键词：网络空间；暗网犯罪；趋势分析；治理对策

一、引言

近年来，互联网已经成为促进人类社会发展进程中不可或缺的重要力量。然而，伴随着互联网络特有的无界性和隐蔽性特点，也给社会安全带来了诸多隐患，特别是网络违法犯罪高发频发，由此引发的各种矛盾和社会问题不断显现。而在网络空间中最为隐蔽、最为黑暗的“暗网”，更承载着极为恶劣的网络犯罪行径，尤以毒品交易、杀人越货、贩卖武器、买卖销赃、色情服务、信息倒卖、数据泄露、恐怖宣扬和政治颠覆等犯罪行为几乎充斥着整个暗网中。“暗网”已经成为网络犯罪的代名词，藏污纳垢的“潘多拉魔盒”。

二、暗网的概念及界定

（一）何谓暗网

暗网，也叫做“不可见网”或“隐藏网”，而更确切的技术名字叫做“隐藏的服务器”。是指存储在网络数据库里、并不能通过普通链接进行访问，需要采用动态网页技术进行访问的一种资源集合。暗网的服务器均在国外，不会被日常所用的谷歌、百度、360 搜索等搜索引擎直接抓取，是一种建立在互联网基础之上，经过加密的匿名网络。它是一种需要使用特定的软件、设置或授权才可接入的深层网络，同时还具有被限制访问的站点功能。“暗网”最初起源于美国军事情报机构的相关系统，由于保护数据的密码类似与洋葱一样层层进行包裹，由此被称作“洋葱路由”（TOR）。因此，网民要想访问暗网必须要借助类似“洋葱路由”的特殊软件再加上动态请求方能进入，访问者在上面不会留下任何痕迹。类似这样的深层网络有些是合法可行的，但更多的是藏着不可告人的秘密。

* 明乐齐，云南省公安厅网络安全保卫总队副高级技术主管。

（二）暗网的历史由来

多年前，暗网并不为公众知晓，它主要依靠对于海量用户的操纵、不受约束的比特币在网络中实施交易。“暗网”最早进入公众视野得要从贩毒网站—-“丝绸之路”（Silk Road）被查封事件说起。2013 年 10 月，世界著名的毒品买卖网站“丝绸之路”被美国 FBI 查抄，该网站 29 岁的创始人罗斯·乌尔布莱特（Ross Ulbricht）遭到逮捕[1]。与此同时，有种种网络监测证据表明，国际恐怖组织“伊斯兰国”也不断将恐怖活动的宣传工具转移到阴暗的网络之中。另外，曾经红极一时并被称为“世界上最大的 BT 种子服务器”的海盗湾（The Pirate Bay），也于 2018 年 3 月遭到美国、荷兰、瑞士等国家的取缔与查封，继网页频繁显示离线后，它们在暗网上的域名也已离线，这个一直隐匿在暗网中具有网络分享与下载功能的重镇随之遭到崩溃瓦解[2]。而从 2017 年开始，陆续被美国 FBI 等机构捣毁的阿尔法湾（AlphaBay）和汉萨（Hansa），更是当时规模领先的暗网交易平台，他们的命运和前途与海盗湾如出一辙[3]。因此，“暗网”，一个原本局限在 IT 行业和部分不法群体中的名词，却在 2018 年不断刷新大众的认知。据相关机构统计，全球如今每天大约有 250 万名网民浏览“暗网”[4]。“暗网”还常与“个人信息”、“比特币”、“勒索”、“黑市”等字眼相伴，化身为各类犯罪信息汇聚和违法交易横行的“不法之地”。暗网上还出售着几乎你能想到的任何东西，你可以买到欧盟和美国等国家的假护照，毒品和各种枪支弹药，甚至名人的裸体自拍等等比比皆是。暗网，需要通过“洋葱路由”（TOR）浏览器才能进入，TOR 浏览器最初以高度匿名性与高度隐私化而著称，很多使用 TOR 的人也是为了这一合理诉求而来。只不过正如俗话所说，有人的地方就有江湖，当各色人都涌进来之后，暗网也就如同表网一样，既有普通用户也有犯罪分子。当你接触暗网时，就可能受到了环境的影响和感染，不知不觉身不由己，走向了违法犯罪的深渊。

（三）暗网犯罪的法律界定

2018 年，美国多个政府部门联合开展有史以来第一次暗网卧底活动，一共打掉 35 个暗网交易平台，并缴获了价值 2360 万美元的商品，其中包括 2000 比特币[5]。“暗网”的黑色力量之广泛、全球黑灰产业之庞大，超出了人们的想象。特别是利用比特币的暗中黑色交易模式，它将罪恶的触手伸向了违法犯罪的每个领域。2013 年被美国政府打击和曝光的“丝绸之路”（silk road）网站中，毒品交易、枪支贩卖、性奴服务、儿童色情等违法犯罪活动应有尽有，甚至是人体器官的买卖也在其中，用网站创始人乌布利希的话来说就是“一个经济仿真体”，暗网变成了网络违法犯罪的避风港[6]。因此，暗网中的服务提供者提供服务或产品必须符合法律法规的要求，否则就构成了网络犯罪。如在欧盟国家，如果不提供真实信息的电子商务服务提供者，违反欧盟《电子商务法》中第五、第六条的相关要求将受到法律制裁。而我国《网络安全法》更明确规定，提供网络产品和服务的单位

[1] 长铗：《黑暗网络“丝绸之路”的覆灭细节详细曝光》，来源：https://www.8btc.com/article/5528,2019 年 4 月 28 日访问。

[2] HackRead：《世界最大 BT 服务器本周死了三回，海盗湾要凉凉？》，来源：https://baijiahao.baidu.com/s?id=1595803287405870630&wfr=spider&for=pc，2019 年 4 月 28 日访问。

[3] 肖竟：《全球最大“暗网”黑市被关闭》，载《青年参考》2017 年 8 月 2 日第 6 版。

[4] 姜妹：《黑暗网络勾当被曝光》，来源：http://finance.sina.com.cn/roll/2019-03-13/doc-ihsxncvh2018589.shtml，2019 年 4 月 29 日访问。

[5] FreeBuf：《2018 上半年暗网现状：逐渐成为威胁情报来源》，来源：https://baijiahao.baidu.com/s?id=1607593591955556451&wfr=spider&for=pc，2019 年 4 月 30 日访问。

[6] 柠楠：《新闻周刊：暗网毒品交易网站“丝绸之路”的兴衰》，来源：http://finance.sina.com.cn/stock/usstock/c/20150225/212421592746.shtml，2019 年 4 月 30 日访问。

或个人必须符合国家规定的强制性要求，如若发现网络产品、网络服务存在安全缺陷和漏洞等风险时应当立即采取补救措施，否则将面临法律的惩罚制裁。而对于提供特许进入行业的服务，均需要取得相应的特别许可证。我国《刑法》第二百二十五条中还明确规定，“其他严重扰乱市场秩序的非法经营行为”均构成了非法经营罪。由此可见，一项服务要在暗网中匿名进行，必须严格遵守网络管辖属地的法律法规。暗网，作为网络空间的组成部分，是互联网的一个子集，我国网民在暗网上进行活动和利用暗网的行为必须遵守《网络安全法》等法律法规，否则将会受到法律的严厉制裁。

三、当前暗网的现状分析

暗网虽然给了人们更多的自由，但是秩序价值变得更难以保障，特别是我国与美国等西方国家在暗网的监管和开放程度上存在着明显的差异与不同。

（一）我国暗网的发展现状

2018 年，腾讯守护者计划安全团队对我国暗网的访问和网上数据交易情况进行了分析研究，主要有以下特点：一是我国网民日均访问暗网的用户并不高。据统计，我国网民日均访问暗网的人数与上网人数相比不足 5%，而且在这些访民中直接绕开代理进行访问的也只有一半以上；二是从地域上看广东网民访问暗网的人数最多。我国访问暗网的用户中广东网民占比最大，约达到了 21%左右，其它省份暗网访问用户的人数占比基本平均，最高的省份也不超过 7%；三是从性别上看男性网民访问暗网的人数远远高于女性。统计发现，我国男性网民访问暗网的人数接近 77%，而女性暗网访问者仅占 23%不到；四是从年龄结构上看青少年网民访问暗网的占到八成以上。统计显示，在暗网中 10-18 岁的访问者达到 29.9%，19-27 岁的访问者占比达 52.5%，28-36 岁的访问者达 8.8%，由此可见，30 岁月以下的年青网民最热衷于访问暗网（见图 1）；五是暗网中数据泄露和不法交易比较突出。根据腾讯安全云鼎实验室对 2018 年国内暗网数据交易情况进行梳理统计，不法分子通过暗网进行数据交易的违法行为极为猖獗，特别是倒卖网购和物流数据信息占到了 50%以上，公安机关全年破获通过暗网倒卖个人信息的犯罪案件多达 100 余起（见图 2）[1]。

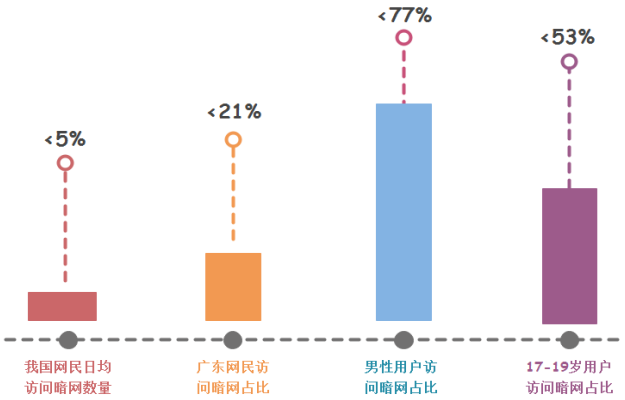

图 12018 我国暗网网民访问情况

[1] 区块链之家：《暗网观察：盘点 2018 热点事件，看网络安全新趋势》，来源：http://www.csunv.com/article-210863-1.html，2019 年 5 月 3 日访问。

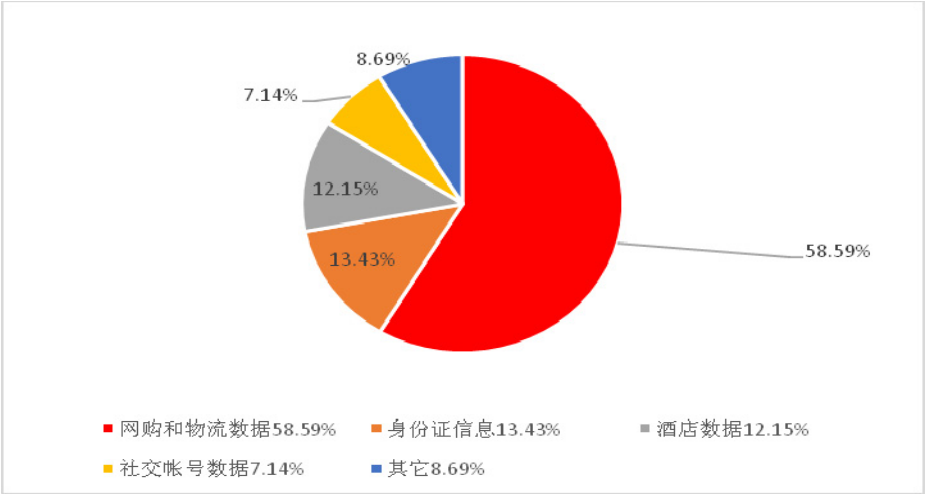

图 2　暗网数据交易类型分布统计

（二）我国对暗网的管制及要求

由于暗网的去中心化、匿名性、不可控性以及暗网网站建立的随意性等特点，与我国对于互联网建设、使用、运营和维护的基本要求存在差异，特别是在《中华人民共和国计算机信息网络国际联网管理暂行规定》中第六条明确规定要求，“计算机信息网络直接进行国际联网，必须使用电信部门的国家公用电信网提供的国际出入口信道，任何个人不得自行建立或者使用其他信道进行国际联网”。我国类似于暗网的管理和管控上也有明确的规定和要求，在 2017 年实施的《网络安全法》中明确规定，建设、运营、通过网络提供服务应当遵循法律法规及强制性规定，各级司法机关要采取必要的措施，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。而且我国在司法解释中也明确要求，任何在互联网上从使非法经营性活动的行为都构成违法犯罪。同时，更加明确的强调国家网信部门和有关单位负有网络信息安全的监督管理职责，其管理的对象体现为网络运营者、任何使用网络的个人和组织。因此，暗网的连接、浏览和进入必须严格遵守国家的法律法规和相关要求，坚决打击一切通过暗网实施违法犯罪的行为[1]。

（二）国外对暗网的管控与策略

以美国为首的西方国家对暗网的管控基本上是采取宽严相济的政策，特别是美国对暗网的管控相对宽松，目前尚未禁止人们对暗网的使用，且很少过滤暗网上的内容，他们比较关注的是对暗网通信的监听，其目的是保证政府能够接触到所有点对点的通信领域，但这种强制监听的治理方式被诟病威胁隐私与通信自由，受到了部分法律人士的批评和指责。在“9·11”之后，美国的《爱国者法案》中增强了监督信息安全的能力，比如授权有关部门截获恐怖主义信息，计算机欺诈、滥用和攻击的通信信息权力，提高了侦听、揭发通信信息的底线，还可以随时查看公民的上网记录、私人信件、电子邮件甚至监视公民的阅读情况。美国联邦调查局（FBI）还不断深入暗网卧底打击非法活动，使用特殊技术手段进行暗网监控监测，美国法院在审判案件中支持并依法授予其使用网络调查技术 NIT 的权力[2]。而与我国的友好邻邦俄罗斯则在暗网的管控上有锁紧的趋势，特别是在中俄达成网络空间

[1] 马可：《暗网法律治理思路探究》，载《中国信息安全》2017 年第 11 期。
[2] 智妍：《9.11 事件后美国反恐立法分析》，载《法制与社会》2009 年第 11 期（下）。

密切协作之后，两国在打击互联网违法犯罪方面取得了积极进展，并且达成了一定的共识。尽管各国在暗网的监管与执法方向上存在隐私、自由与保障网络空间合法性的争议，但是以美国为首的西方国家未来可能更倾向于允许用户使用 Tor 网络，但更会对利用 Tor 进行违法活动的行为设置独立责任[1]。

四、暗网犯罪的趋势特点

当前，通过暗网实施违法犯罪的形式复杂多样，趋势与特点比较明显，特别是以毒品交易、杀人越货、武器贩卖、物品销赃、色情服务、个人信息和数据倒卖、实施恐怖主义为主的违法犯罪活动在暗网中更加肆意猖獗。

（一）数据泄露占据暗网犯罪首位

按照国际权威机构波耐蒙研究所与 IBM Security 对 2018 年数据泄露研究发现，通过暗网进行数据泄露事件造成的损失仍在不断增长，且消费者个人记录丢失或被盗的情况仍在年复一年的持续增加。尽管安全与防御水平皆有所提升，但各国在对抗暗网攻击的战斗中仍处于下风。暗网，基本上一直以恶意倾向于散布个人、财务、物联网以及技术性数据信息为主要的犯罪攻击目标。据 FreeBuf 报道，2018 年 8 月 28 日，暗网中文论坛中出现一个帖子，声称售卖华住旗下所有酒店数据，数据标价 8 个比特币，约等于人民币 37 万人民币，数据泄露涉及到 1.3 亿人的个人信息及开房记录。泄露的数据包含华住酒店集团旗下拥有的汉庭、美爵、禧玥、漫心、诺富特、美居、CitiGo、桔子、全季、星程、宜必思、怡莱、海友等多个酒店的开户信息，信息内容还包括姓名、手机号、身份证号、登录密码等。此事件曝光后在中国大地一片哗然，社会议论纷纷、反响激烈，众多网民发问，个人信息的保护，路在何方？目前此事件仍在调查中[2]。

（二）色情犯罪问题异常突出严重

暗网中色情服务犯罪极为恶劣，特别是儿童色情问题更加猖獗、惊骇全球。2016 年，4 名德国人架设、营运儿童色情平台“极乐空间”，其平台应用程序就属于隐密度极高的“黑暗网络”也即“暗网”，平台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。截止 2017 年 6 月，该网站在全球共有 11 万会员，地域之广、规模之大以及人数之众，立刻惊骇全球。2019 年 3 月，德国林堡地方法院对此案作出判决，网站 4 名创办经营者因“建立、经营儿童色情平台，持有并传播儿童、甚至婴儿的性虐影像”，分别被判处 4 至 10 年有期徒刑。而“极乐空间”暗网平台只是德国儿童色情网络的冰山一角。根据德国警方统计，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。据世界卫生组织估计，全球范围内的网络色情受害者人数多达 100 万人，而在这类犯罪人群中极大部分的恋童癖好者，都是通过“暗网”来躲避追查，观看、交流儿童色情影像，甚至进行儿童性虐待的犯罪行为[3]。

（三）暗网恐怖主义活动十分猖獗

近年来，随着世界各国反恐力度的不断加大，恐怖分子公开进行网络恐怖活动受到了

[1] 马可：《暗网法律治理思路探究》，载《中国信息安全》2017 年第 11 期。

[2] FreeBuf：《程序员炫技引发的惨案：华住旗下酒店上亿条用户数据在暗网售卖》，来源：https://www.freebuf.com/company-information/182637.html，2019 年 5 月 3 日访问。

[3] 姜妹：《黑暗网络勾当被曝光》，来源：http://finance.sina.com.cn/roll/2019-03-13/doc-ihsxncvh2018589.shtml，2019 年 4 月 29 日访问。

极大地打击和限制，于是一些恐怖组织和恐怖分子逐步转向了互联网的“地下世界”，不断利用暗网进行恐怖主义宣扬的迹象越来越明显，有机构研究表明，暗网已经渐渐成为恐怖分子的“避风港”。据媒体报道，在 2011 年发生的“阿拉伯之春”中，埃及的革命者正是通过在暗网上的串联活动，成功躲避了政府的追踪，最终导致推翻前总统穆巴拉克下台[1]。2013 年 8 月，美国国家安全局（NSA）截获并破解了基地组织领导人艾曼·扎瓦希里和也门分部一名领导人之间的加密通信，这是恐怖组织的秘网通信首次为官方所掌握。美国国家安全研究所指出，在最近十年内，恐怖组织领导人之间的网络联系已经逐步转入暗网中[2]。而国际恐怖组织 ISIS 的网站几乎全部建立在暗网之上，其目的就是为了躲避世界各国的打击，并持续招募成员。此外，恐怖组织也在不断利用暗网筹集资金和洗钱，这一迹象通过各种反恐情报信息得到了证实。因此，尽管巴黎恐怖袭击发生后，世界各国加强了对暗网中私密信息传输的监管，如中国、美国、法国、英国等国家完善了相关的反恐立法，加大了打击力度和反恐资金的投入，但是“暗网”仍然具有极强的隐蔽性和市场需求，恐怖组织和恐怖分子通过“暗网”实施恐怖活动的概率仍在进一步放大。

（四）加密货币占据暗网的主战场

根据 Recorded Future 在 2018 年初发布的报告显示，短短几年内，暗网交易所使用的货币中仍然是比特币占主导，但更方便、更安全的莱特币乃至门罗币等加密货币也逐渐开始风靡暗网[3]。一方面，加密货币以其加密、安全性而受到暗网交易者青睐，为暗网交易带来便利，催生了更多犯罪或洗钱活动；另一方面，暗网又为加密货币相关的犯罪行为提供了洗钱或销赃平台，让加密货币越来越不安全。所以，当加密货币与暗网混迹在一起，便成了罪恶的恶性循环。2013 年 10 月，臭名昭著的暗网丝绸之路创始人罗斯，被美国联邦调查局（FBI）、国土安全调查局（HIS）和缉毒局等多部门联合逮捕。由于“丝绸之路是创建于美国，隐藏了大量毒品交易、性奴、儿童色情以及暗杀等犯罪线索的网络世界。它之所以受到加密世界的关注，是因为一直以来为了逃避银行和政府监管，它的所有交易是以比特币和加密货币为主[4]。因此，暗网既是比特币和加密货币的大型交易场，更是充满着黑色恐怖与幽灵的黑暗地带。

（五）暗网信息售卖更加泛滥猖獗

5900 美元可以获得包括美国护照、身份证、驾照等全套的证件。伪造的英国护照价值 2000 英镑，卖家还会承诺把你的个人信息添加到官方数据库之中，保证你的护照可以走遍世界。一把沙漠之鹰手枪，1450 欧元；一个新鲜出炉的用户信用卡信息(账户、密码、CVV 码)需要 14 美元，可以随意消费。如果你缺钱，可以花很低的价格买到伪钞[5]。截至 2018 年 7 月，暗网英语网站上的信息买卖从价值 1 美元的社会安全账号到价值 100 美元的毕业证书不等，基本是应有尽有，成套的信息售价更贵（见图 3）[6]。

[1] 黎晓珊：《警惕暗网演进的四大趋势》，来源：http://tech.huanqiu.com/internet/2019-04/14741820.html?agt=9054，2019 年 5 月 4 日访问。

[2] 杨亚强：《暗网恐怖主义应对路径探析》，载《江西警察学院学报》2017 年第 4 期。

[3] FreeBuf：《2018 上半年暗网现状：逐渐成为威胁情报来源》，来源：https://baijiahao.baidu.com/s?id=1607593591955556451&wfr=spider&for=pc，2019 年 4 月 30 日访问。

[4] 柠楠：《新闻周刊：暗网毒品交易网站“丝绸之路”的兴衰》，来源：http://finance.sina.com.cn/stock/usstock/c/20150225/212421592746.shtml，2019 年 4 月 30 日访问。

[5] 严言：《暗风是一个怎样的世界》，来源：https://new.qq.com/cmsn/20151221/20151221038533,2019 年 4 月 30 日访问。

[6] FreeBuf：《2018 上半年暗网现状：逐渐成为威胁情报来源》，来源：https://baijiahao.baidu.com/s?id=1607593591955556451&wfr=spider&for=pc，2019 年 4 月 30 日访问。

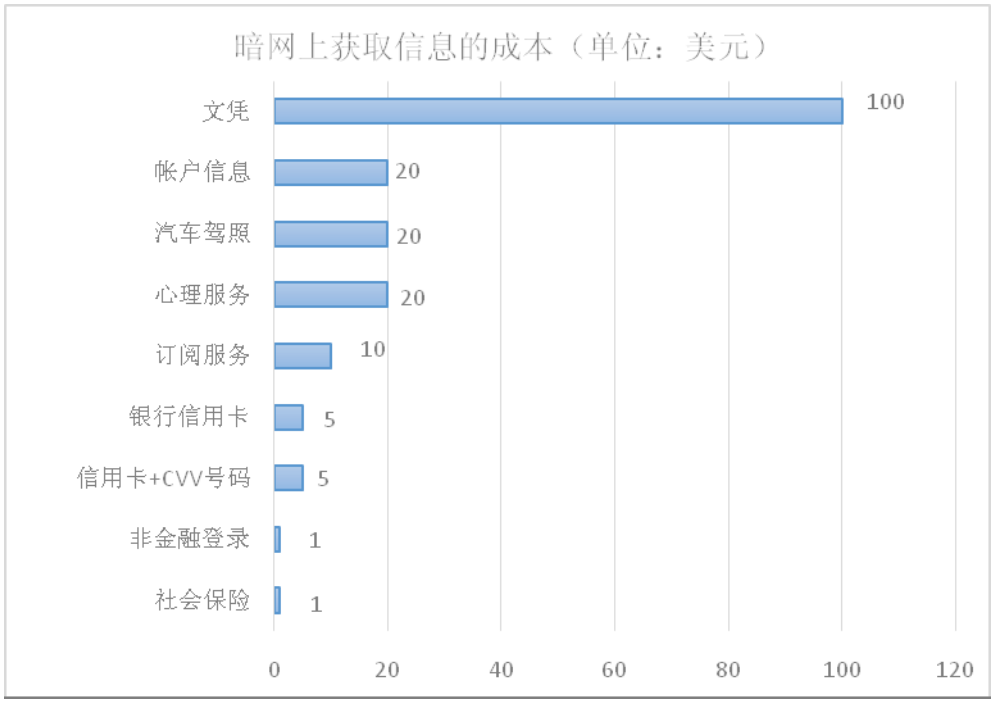

图 3 暗网上获取信息的成本（单位：美元）

而对于受害者来说，一旦个人信息流失到暗网，损失的不仅仅是金钱，他们还可能无法再借款、需要日积月累地工作甚至要变卖家产来堵上信息被卖所造成的财物损失，还有的甚至要背负高利借贷，完全被毁掉整个人生。2019 年 3 月 17 日，巴基斯坦黑客 Gnosticplayers 在全球最大的暗网市场 Dream Market 出售 2700 万用户信息，出售的信息来自六个网站的数据库，总价值为约合 5000 美元，据称这已经是该黑客出售的第四轮个人信息（见图 4）[1]。

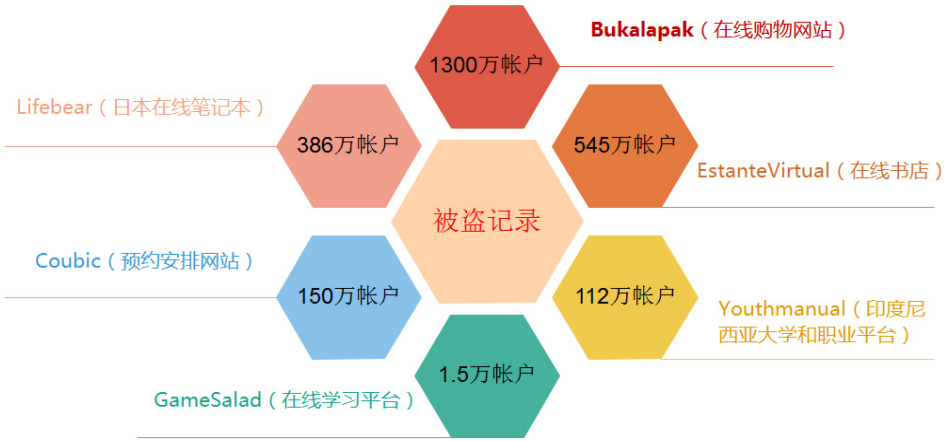

图 4 黑客 Gnosticplayers 出售的第四轮个人信息

[1] ghcoxx:《黑客在暗网上出售第四批数据涉及 6 个网站 2600 万新账户》，来源 https://www.t00ls.net/articles-50334.html，2019 年 5 月 3 日访问。

2018 年 11 月，湖北武汉一家汽车金融平台发现自家网站上的 30 多万条用户个人资料在暗网上被明码标价，个人资料内容包括姓名、电话号码、身份证、住址、银行卡号比特币，在当时相当于 4 万元。卖家还晒出了该平台的业务管理后台等，叫价一个界面截图，显示自己是以“超级管理员”身份登录。此事件被媒体披露后引发社会高度关注。武汉警方接报后通过对海量数据的追踪、分析、碰撞与比对，发现网名为“孤狼”的黑客是四川省成都市双流区华阳镇 22 岁的男子吴某，专案组迅速在成都警方的配合下将嫌疑人吴某抓获归案。据吴某交待，他利用软件以暴力破解手段入侵该汽车金融平台的后台，找到服务器的用户注册信息，盗取大批量、多维度的用户数据，共计 30 余万条，然后在暗网上叫卖。因为不了解进入暗网的相关技术，还花 180 元“学费”向网友请教，目前此案仍在调查中[1]。据美国司法部 2017 年发布的报告称，个人信息被窃取后，受害者的平均金钱损失在 1343 美元左右，而时间损失和精神损失则无法计算。据身份威胁情报公司“4iQ ”于 2018 年发布的报告显示，2016 年到 2017 年期间，其研究团队发现身份信息泄露事件迅猛增长达 182%[2]。当前，暗网中信息贩卖违法行为更加日益猖獗，特别是儿童受害者的个人信息损害数量更在不断成倍数的增长。

五、暗网治理的困境难点

近年来，随着暗网的匿名性和私密性特点不断显现，越来越多的网络犯罪活动逐渐转移其中，因此，暗网违法犯罪越来越猖獗，治理与打击越来越困难。

（一）暗网犯罪追踪溯源打击更艰难

由于暗网使用门槛越来越低，使用方式越来越简便，甚至还有了暗网浏览器、导航和搜索引擎，不需要复杂的安装操作就可以进入暗网，特别是境外进入暗网的工具逐渐倒灌进入我国普通网民中，致使暗网获取信息逐渐平民化，也导致暗网内鱼龙混杂，违法犯罪现象比比皆是。特别是暗网的服务器是用私钥解密信息，获得汇合点 IP 和 cookie，之后通过 Tor 路由与汇合点建立连接，并回传 cookie，用户收到 cookie 之后确认已经和站点建立了连接，之后开始正式访问该站点，最终在用户和暗网服务器之间形成六个中继节点，也就是用户的入口节点、中间节点、汇合点，服务器的出口节点、中间节点、入口节点，并且其上游的通信全都是 TLS 加密的，这样就同时保障了用户的匿名访问和站点服务器 IP 的隐藏[3]，导致 IP 地址的追踪溯源十分困难。因此，各级执法监管部门对暗网的监管和打击难度进一步加大，特是犯罪线索发现难，犯罪证据收集难，犯罪案件定性难。

（二）加密货币诱发的暗网犯罪激增

犯罪嫌疑人用数字虚拟货币进行洗钱和不法交易，网络黑产人员频频利用非法挖矿、勒索、盗窃等威胁网络安全的手段，大肆攫取数字虚拟货币，反过来应用在暗网交易中牟取暴利。暗网和加密货币的结合，使暗网有了更独立、更安全的支付系统，因其进一步增强了暗网交易的隐匿性，导致暗网犯罪的数量在不断增长。据 360 安全团队对暗网中一个

[1] 凌姝，白杰戈：《30 多万条个人资料在暗网上售卖嫌疑人已被控制》，来源：https://baijiahao.baidu.com/s?id=1629037203901577723&wfr=spider&for=pc，2019 年 5 月 3 日访问。

[2] FreeBuf：《2018 上半年暗网现状：逐渐成为威胁情报来源》，来源：https://baijiahao.baidu.com/s?id=1607593591955556451&wfr=spider&for=pc，2019 年 5 月 3 日访问。

[3] 编辑部：《暗网的养成：Tor（洋葱路由）的故事》，载《中国信息安全》2017 年第 11 期。

活跃的中文交易论坛长期进行监测和统计，该交易论坛的活跃程度从 2017 年开始迅速增长，截止 2018 年底暗网的交易贴发布数量总体上升趋势明显，全年达到 3000 人次，特别是从 2018 年 8 月份开始发帖数量激增，11 月份达到峰值，当月发帖数量达 791 人次[1]。而在这些发帖交易的内容当中，所有交易内容都是以加密货币成交计算，涉及的犯罪内容更是包罗万象。

（三）暗网导致网络犯罪更趋平台化

随着暗网的逐渐大众化，网络违法犯罪开始朝向平台化、服务化的趋势发展。比如，可以在暗网上购买整套的勒索软件服务，有的平台直接提供勒索服务指引，你只需要告知要勒索谁，平台会去主动实施勒索攻击，并从勒索得来的收入中获得提成。平台中暗网成员的相互联络更具有极端私密性，导致公安机关在平台中的暗网环境下立案后取证更加困难，特别是平台中的网络犯罪具有动态页面、难以溯源等特征明显，增加了执法部门对此类犯罪方式的打击难度。

（四）数据储存加大了暗网反恐难度

随着数据储存交换的云服务在互联网普遍应用，促使暗网上的不法行为更为隐蔽，也导致相关职能部门追踪起来更为其难。例如，美国亚马逊公司开发了一款名为 EC2 的弹性计算云，该软件能够支持虚拟计算机，可以运行网桥（不同网络之间的互联设备或秘密网络的虚拟点），如果用户加入这一服务，那么其通信就可以沿网桥所连接的路径进行，即可以利用秘密网络进行联络，其中也包括暗网。因此，TOR（洋葱路由）的开发者们极力号召客户大量加入 EC2，因为这样可以催生更多的藏匿地点[2]，也就是说暗网的通信将无所不及、无所不从，更加安全隐蔽。导致恐怖组织和恐怖分子更加无孔不入，打击暗网恐怖主义的难度越来越大。

（五）隐私保护成为暗网被滥用的理由

暗网的出现不断满足了部分网民保护隐私的合理需求，但科技发展往往伴随着不可预知，暗网已逐渐成为违法犯罪和恐怖分子的“避风港”。“棱镜门”事件发生后，网民对隐私的保护意识进一步增强，也导致隐私保护成为打击暗网违法犯罪和反恐的难题。特别是当执法部门因为案件的需要，要求网络公司给予配合调查时，有的公司经常以隐私保护为由予以拒绝。因此，如何处理暗网犯罪与隐私保护之间的关系，已经成为执法机关棘手的问题。特别是我国法律在个人隐私保护方面存在争议，因此法律法规还未完全对“暗网”访问与隐私保护之间的问题作出明确的规定要求。

（六）暗网接口的隐蔽性提高了执法成本

暗网的访问者为了逃避执法监管和打击，主要采取点对点的方式传播违法犯罪信息内容，利用网盘分享下载文件，导致执法部门很难摸清用户的真实身份与活动轨迹。尤其是智能、隐形技术在移动终端的使用，暗网中犯罪证据的提取更加困难繁锁，大大提高了执法机关的追踪追查的成本。有的暗网通过境外跳转，尽管有互联网作为依托，但隐蔽性能极高，无能犯罪嫌疑人是否留下蛛丝马迹，但执法部门受各种技术制约基本上很难掌握暗网使用者的访问动向。

[1] 张厚为：《360 智库：警惕暗网演进的四大趋势》，来源：http://finance.ce.cn/home/jrzq/dc/201904/17/t20190417_31880144.shtml，2019 年 5 月 4 日访问。

[2] 杨亚强：《暗网恐怖主义应对路径探析》，载《江西警察学院学报》2017 年第 4 期。

六、打击暗网犯罪的对策

习近平总书记在第二届世界互联网大会上提出构建“网络空间命运共同体”的设想，强调“网络空间是人类共同的活动空间,网络空间命运应由世界各国共同掌握，各国应该加强沟通、扩大共识、深化合作”,这无疑为暗网治理提供了中国思路[1]。在全球互联网信息快速发展的背景下,以“网络空间命运共同体”的理念为指导,对加大暗网的治理具有非凡的历史意义。但是，由于暗网隐匿性强、变化快、危害性大等特点显著,世界各国虽已采取强有力的治理打击措施,但收效甚微，困难重重，打击与治理暗网犯罪迫在眉睫。

（一）深化技术创新，挤压暗网生存空间

针对变化莫测和来势汹汹的暗网，永久性的封堵并非治本之策，必须做到“魔高一尺，道高一丈”，不断深挖严查暗网中的一切违法犯罪行为。一要努力将暗网变为我所用。虽然暗网极易成为犯罪的“温床”，但并不意味着暗网“一无是处”，事实上暗网可以应用于很多领域，尤其是对数据安全和通信安全要求较高的军事通信、电子商务等领域，想要从技术层面应对暗网违法犯罪，最重要的是能及时发现暗网上的犯罪信息，这就需要完善针对暗网的科技监测和技术应用。2015 年，美国国防部发布了一款名为 MEMEX 的搜索引擎，该引擎可以深度“挖掘”暗网中的各种信息，可以获取谷歌等常规搜索引擎检索不到的私密信息，还能够对深层网络进行编目编程。该软件最初被用来监测暗网上的人口贩卖信息，后来逐渐可监测其他违法犯罪活动。DARPA（美国国防部高级研究计划局）认为可以通过 MEMEX 引擎找到暗网中的涉恐账号和违法犯罪交易平台，进而以此给予深度精准打击。二要加强针对暗网的技术研究与开发。美国联邦调查局（FBI）使用 NIT（一种网络检测工具）成功破解了“洋葱路由”网站，导致他们随时可以监测掌控暗网中的通信信息。据专家介绍，NIT 是一种极为复杂的网络调查工具，可以识别并破解“洋葱路由”的加密机制，还可一次搜索 1300 个暗网 IP 地址，然后顺藤摸瓜地找到使用这些地址的上网客户，除 IP 地址外，MAC 地址、用户名、主机名都能被 NIT“捕获”[2]。我国政府应加大相关技术的研发力度，力争破解在暗网中的一切违法犯罪活动和恐怖信息，同时也可应用于军事等其它领域。三要加强政府与企业在暗网技术上的合作。要充分发挥腾迅、360 公司、百度、美亚、烽火等我国知名互联网安全企业的优势作用，不断研发阻拦和破获暗网中违法犯罪信息追踪查源的难点，重点加强暗网中匿名违法信息的拦截与破获研究，在保护个人匿名信息合法性的同时，力争做到点对点的精准发现信息，不放过任何违法犯罪、涉恐和颠覆国家政权的信息，真正在暗网中让犯罪分子无机可乘。

（二）加强源头治理，铲除暗网滋生链条

对于暗网犯罪，需要从治理宏观环境开始，斩断黑灰产业链条，从严打击公民个人信息的泄露源头，截断个人信息贩卖的渠道，严打黑卡黑账户买卖等灰产业行为。只有将网络灰黑产业的土壤铲除干净，犯罪分子自然无所遁形。一要健全完善一案双查制度。要督促联网单位和企业落实安全管理责任制度及应急响应措施，对拒不履行互联网安全的单位和企业要依法从严查处。对发生的暗网犯罪既要查案件的本身，更要查联网责任平台和相关互联网企业。要以防范利用暗网进行人口贩卖、毒品交易、淫秽色情和侵犯公民个人信息等犯罪为重点，全面整治网络运营秩序，打击暗网中的黑产黑市，不断净化网络环境。

[1] 周琳娜,高存：《暗网治理思路》，载《信息安全研究》2018 年第 9 期。
[2] 杨亚强:《暗网恐怖主义应对路径探析》，载《江西警察学院学报》2017 年第 4 期。

二要进一步加强信息的治理与管控。各地要借助“净网 2019”专项行动，加大暗网中违法信息的清理清查，坚持边清理边打击。要将违法信息清理工作与打击惩处同谋划、同推进、同落实，全力遏制黄赌毒、枪爆盗、个人信息贩卖、数据泄露等违法信息在暗网中滋生蔓延的高发势头。三要解决底层最根本的问题。打击暗网犯罪需要高科技投入，更要解决最底层的根本性问题。要全面落实《网络安全法》，严格保障公民个人信息的安全，重拳打击“撞库”、假身份证、黑电话卡、虚假 ID、假冒银行账号等网络黑灰产业链，从根本上限制暗网中的肆虐空间。2019 年 2 月，广东警方破获系列电话“黑卡”案，抓获犯罪嫌疑人 190 余人，打掉一批“卡商”“号商”“接码平台”，缴获黑卡 290 余万张(主要为物联网卡)、猫池 2520 余套、公民个人信息 6000 万余条[1]。此案中电话“黑卡”是庞大的“暗网”下层物料基础,由于手机黑卡可变成暗网中犯罪分子最热衷的作案工具,很多犯罪分子隐藏在手机黑卡背后肆意在暗网空间作恶多端，即使办案机关追踪到手机号码，也难以追踪到犯罪者本人。此案的成功告破，说明公安机关有能力、有决心铲除一切与暗网犯罪有关的滋生土壤。

（三）强化侦查打击，遏制暗网高发势头

一要加强打击暗网犯罪的组织领导。各级职能部门要高度重视打击暗网犯罪工作，要成立打击暗网犯罪的专门组织和机构，公安机关要主动作为，亲自抓、主动抓、靠前抓。要不断完善打击暗网犯罪的工作措施，精准提前谋划，通过强组织、强制度、强有力地把暗网犯罪的新势头打下去，以新担当、新作为的精神，奋力开创打击治理网络犯罪工作的新局面。二要加大犯罪团伙的打击力度。各级公安机关要结合当前开展的“扫黑除恶”专项斗争，要将暗网中的暴力犯罪行为列为扫黑除恶的重点内容，严加打击，决不手软。要坚决打掉暗网犯罪中的“团伙”“钉子”，彻底摧毁暗网犯罪活动中的团伙组织，彻底打掉暗网犯罪中的黑社会成员，彻底打掉为暗网犯罪提供保护保障的“保护伞”，彻底铲除此类违法犯罪滋生的土壤。三要加强联合侦查打击的效果。公安机关要充分发挥打击暗网犯罪的主力军作用，及时开展精准研判，创新打法战法，主动出击，将打击延伸到省外、境外，真正对暗网违法犯罪形成强有力的震慑。公安、法院、检察院、工信部门、市场监督管理局等部门要严格按照最顶层的打击理念进行设置，做到不辱使命，勇于担当，不断加大和推进打击网络犯罪的纵深度，进一步彰显打击的威慑力和铁力。

（四）加强国际合作，推动打击成果效能

一是强化国际合作机制建设。各国要在国际框架的范围内加强网络安全犯罪打击的密切协作配合，不断强化和扩大打击暗网犯罪的纵深度，更加有效地防控和打击暗网中的违法犯罪行为。要加强和改进国际合作的方式方法，共同携手并进，不断强化合作，深化扩大惩治暗网犯罪的成果。要加强联动，标本兼治，健全行之有效的打击地下黑市、震慑暗网交易合作机制，彻底铲除暗网犯罪的生存空间，共同维护本地区繁荣稳定，全力推动构建人类命运共同体[2]。二是构建国家之间的引渡机制。2015 年，美国《网络安全法》规定通过引渡或无合作情况下的磋商等方式打击国际网络犯罪,中美在打击暗网犯罪活动方面,已经有了执法协作实例。因此，各国要在互信互利的基础上，建立网络犯罪的信息交流机

[1] 张毓琪：《广东警方缴获近 300 万张“黑卡”！铲除背后黑灰产团伙》，来源：http://shenzhen.news.163.com/18/0819/18/DPJG1Q7G04178D6R.html,2019 年 5 月 2 日访问。

[2] 杜晓,史欣伟：《开展国际合作打击网络犯罪已成共识》，来源：http://www.legaldaily.com.cn/index/content/2018-09/20/content_7650101.htm?node=20908,2019 年 5 月 6 日访问。

制，不断加强网络犯罪嫌疑人的引渡机制建设，相互之间要摒弃在打击与惩处网络犯罪分子中的误差，提供在本国法律框架范围内的支持。要加强打击暗网犯罪中的情报交流共享，特别是突出反恐情报信息的相互交流，不断健全和完善打击暗网犯罪的国际联动机制，共同联合打击和消灭暗网中的一切违法犯罪。三是加强暗网国际规则约束制定。无论是发达国家还是发展中国家，都应该本着“人类命运共同体”的基本理念，共同携手建立民主透明、多边参与、权责一致的暗网犯罪治理和打击模式。要加快制定互联网行为准则，优化暗网治理的国际环境和行为准则。特别是在国际形势错综复杂的今天，我们更加亟须尽快制定国际规则，不断约束暗网滥用技术优势的行为，明确强调国家无大小、无强弱，切实避免少数技术大国对网络安全的私用与滥用。只有通过各国的共同努力，暗网的生存空间将会进一步收窄。

（五）加强立法管制，提升打击的纵深度

由于各国在暗网治理和打击的目的、方法、手段、包括意识形态各不相同，加上暗网治理本身的技术难度很高，因此如何建立健全有效的法律法规，是目前困扰世界各国在暗网治理上的难题。一要加强暗网安全的立法规制。解决暗网安全问题除了强有力的技术支撑外，更要加强顶层法规设计。为了有效应对暗网给网络安全带来的挑战，在全面落实《网络安全法》的同时，建议国家立法机关和执法部门要加快推进暗网安全的立法规制，明确通过暗网犯罪的社会危害性，不断在法律法规上卡住暗网违法犯罪的脖子。二要加大对暗网匿名服务的监管。相关业务职能部门要专门制定暗网信息安全监管方面的规定准则，明确监管的主体责任，明确网络服务商的权力和义务，明确用户的访问权限，真正落实暗网安全的主体责任要求。三是强化对暗网加密服务的制约。要借鉴美国、德国等西方国家在暗网治理上的先进经验，用制度和规定明确要求加密服务提供商开放监管接口，不断满足政府执能部门的合法需求。同时明确规定加密服务商建立留档备案制度，努力为侦破暗网犯罪提供强有力的法律保障。四要建立个人隐私保护制度。加强暗网立法规制的同时，要尽快建立健全我国公民个人隐私保护制度的落实，合理处置和应对政府监管与隐私保护之间的关系，力求在二者之间保持相对平衡公正。与此同时，更要根据网络安全形势的变化和反恐斗争的需要，随时不断调整两者之间的关系，切实做到既要保护公民的合法权益，更要坚决打击一切网络违法犯罪。

暗网隐藏着违法犯罪已是不争的事实，且有愈演愈烈之势。各级政府职能部门要紧紧围绕新中国成立 70 周年大庆安保维稳这条主线，从严、从实、从细抓好打击整治暗网工作的落实，加大对“暗网”犯罪的打击纵深度，彻底截断暗网地下灰色犯罪链条，不断将“暗网”的黑暗勾当暴露在光天化日之下。要建立健全网络综合治理的防控体系，以专项行动为抓手，打击与整治相结合，坚持以打促管、以打促建，全面提升网络空间的治理能力水平，努力建设更高层次、更高水平的平安网络空间，努力以网安天下的奋斗精神迎接新中国成立 70 周年。

（责任编辑：廖根为）