“暗网”犯罪及其应对措施

□ 麦 政

随着互联网的不断普及与发展，“国家网络安全”成为公众最关心的问题。尤其是“暗网”犯罪作为目前国家安全潜在威胁之一，不仅对公民的个人隐私、政府的信息安全造成了重大威胁，而且对于政治、军事领域以及社会生活等重要层面也形成了严峻挑战。

“暗网”犯罪

“暗网”称为“黑暗网络”，简称“Dark Web”，其存在于地下网络中的万维网，从本质上来说，它又从属于洋葱网络，通常具有“onion”扩展名，是一种分散性的匿名网络。对于暗网访问，通过百度等常规搜索引擎是搜索不到的，只能通过类似于I2P、自由网以及其他地下网络（Tor）的特殊加密匿名软件的访问才能进行。

“暗网”犯罪又称“crime by dark web”，即使用“暗网”空间的媒介手段进行犯罪，在国内，目前仍归类于“传统网络犯罪”，但实际上其所涉及的范畴却远不止网络，在毒品交易、军火贸易、黑客服务、色情服务等犯罪问题上“暗网”均有涉及。而在国际上，暗网犯罪手段已经非常成熟，并且具有较大的社会危害性，并引起高度关注。

犯罪特点

犯罪主体、犯罪客体多样化 “暗网”犯罪随着互联网的发展普及，成为不可忽视的一个问题。在这期间，犯罪主体平均年龄主要集中在25岁以上，如“丝路”市场创始人罗斯·乌布利希年龄为26岁，“阿尔法市场”创始人亚历山大·卡兹被捕时25岁，拥有高等学历，同时精通互联网技术是他们身上的共同点。此外，犯罪客体多样化指的是“暗网”内容丰富，包含有儿童色情、非法军火交易、恐怖主义、以及个人信息、政府资料的出售等等。

犯罪手段高级化、智能化 掌握Tor的基本配置，以及租用VPS服务器，私人搭建“暗网”获取“onion”的域名，这类看似简单的方法其实要求使用者精通计算机技术，熟练掌握计算机安全领域，同时对“暗网”具备高级专业知识的了解。此外，区别于传统的计算机犯罪，此类犯罪显得更难以侦查取证及追踪，德国警方所摧毁的世界第二大“华尔街市场”就历时4年才最终破获。

犯罪地域全球化 21世纪的互联网发展越来越全球化，更深入世界的各个角落。作为网路虚拟空间，互联网并不像现实中的国界那般清晰，且地域明显，在网络虚拟空间中地域性已被打破，“暗网”犯罪比比皆是。犯罪分子会利用Tor浏览器进行IP隐藏，同时使用VPN进行流量加密，使得在全球范围内对“暗网”犯罪的打击变得更为棘手。此外，根据Tor官方2019年3月至6月所公布的全球十大中继用户的排名来分析，这其中既有发达国家，也有发展中国家；既有欧洲国家，也有亚洲国家。犯罪分子利用“暗网”的特点进行逃避打击，同时使犯罪实施效率提升。

犯罪手段

以Tor浏览器为依托，通过洋葱网络搭建“电商”平台进行交易 同淘宝等购物电商一样，“暗网”也通过构建“电商”平台对各类非法药品、武器以及数据服务等进行公开出售。洋葱网络区别其他网络最大特点是不仅为用户提供匿名，而且也为使用者提供天然的“避风港”。这正是“暗网”犯罪屡禁不止的一个重要因素，从“农夫市场”再到“阿尔法市场”再到“丝绸之路”，每个犯罪市场被捣毁背后都是执法人员夜以继日地付出所得来的成果，但往往一个巨大“暗网”市场倒下以后，接着却是无数“暗网”市场崛起。

以匿名加密货币为交易手段 高度匿名性、隐私性、安全性、无监管性，使得以比特币为代

表的一类加密货币备受青睐，包括比特币在内的各种加密型货币如莱特币、门罗币等构成“暗网”经济的重要枢纽。以比特币为例，作为目前主流的货币，区别于传统的电子货币，它更是一种作为去中心化以及通过区块链作为基础技术的加密货币存储在加密的数字钱包之中，从2009年诞生到目前为止，其发明者至今仍是一个谜。

此外，在暗网中“Blockchain”的出现使得比特币流通更加正式化以及规范，它是目前最受欢迎的在线钱包。根据相关的数据统计其被开挖的数量为2100万个，而其最基础的单位为聪。作为一种去中心化的货币，其不需要一个政府或银行去管制和发行，而通过一种区块链交易记录方式在人与人之间转账，只要通过互联网，就没人能阻止这笔交易。因此，基于这种优势使得其在“暗网”中成为通用货币。

以发达国家为主要阵地，正向中国逐渐蔓延　“暗网”的发展，离不开美国等主要国家的支持。作为西方大多数人眼中的自由天堂以及理想境地，“暗网”这片领域充满了自由，同时成为天然犯罪的集中地。目前，主要犯罪阵地仍集中于欧美等发达国家，这是基于互联网技术的领先以及技术成熟，同时从政策层面来看，对于暗网的管理并没有形成统一明确的合作体系，在政府层面监管缺位是导致其犯罪上升的一个重要因素。

根据国内某网络安全公司提供的“暗网”节点数据显示，在全球17635个中继节点里，北美与欧洲的中继节点占据了75%。而语言使用方面，英语所占比例高达80%，仍是“暗网”主流语言。但是，随着“暗网”版“维基百科”的发展，其搜索引擎功能正逐步得到完善，并出现了相当数量的“中文暗网”，这点值得警惕。

犯罪危害

军火交易以及枪支泛滥问题严重　根据兰德公司一项研究表明，“暗网”的枪支主要来源于美国，并占据了黑暗市场份额的60%，欧洲国家占据了25%，其他国家为15%。黑市价格与“暗网”价格相差无异，相比于黑市交易，不法分子更加青睐于隐匿性更高的“暗网”进行交易。这是基于美国各州枪支管控制度不一，为枪支的非法流通埋下了安全隐患。此外，兰德公司以及曼切斯特大学专家的联合研究报告也表明，50余家不同的供应商在“暗网”上提供各类枪支武器以及配件销售。其中，在贸易清单中枪支占据了40%，而且欧洲俨然成为“暗网”枪支最大的流通市场。

与枪支市场相辅相成的是，“暗网”市场中提供的各类非法教程，包括3D枪支打印图纸，爆炸物制作等，也极大增加了恐怖袭击隐患。源于“暗网”的匿名性及复杂性，各国对枪支管控都面临了巨大的挑战。

“暗网”为恐怖主义发展提供温床　英国政府通信总部前负责人戴维·奥德曼曾强调：“恐怖分子和犯罪团伙会运用他们可接触到的最新技术且实时跟进，整个过程就犹如军备竞赛”。2014年，极端组织伊斯兰国的迅速崛起震惊世界。虽然国际反恐联盟介入，以及俄罗斯高调亮剑，使得伊斯兰国在战场上迅速溃败，但是其组织构架并未溃散，其媒体宣传员依然活跃在各个网络社交媒体以及社交平台上进行宣传及招募新人。根据Telegram官方公布的数据显示，2015年，其关闭约78个与恐怖主义有关的公开频道；2016年，每月还屏蔽将近2000个与之相关频道。同时，Twitter官方也宣布关停12.5万相关账户，Google以及Facebook官方宣布将采用版权扫描工具对极端主义内容进行识别，及时作出下线调整。

面对世界对恐怖主义打击力度的加大，极端组织开始把阵地转向高度匿名性的“暗网”。2017年，联合国负责政治事务部副秘书长费尔曼就曾指出，随着伊斯兰国在战场的溃败，恐怖组织将采取更多隐蔽匿名方式招募新成员以及联络，以分散目前军事压力，伴随暗网不断发展，这也为恐怖主义提供了新的活动场所。2018年，伦敦某男子因涉嫌在“暗网”购买非法物而被捕，警方在搜查时发现了其使用匿名加密工具进行联络。

敏感信息泄露　售卖敏感信息在“暗网”中占据了很大市场，包括个人、政府机密、军事等信息。2013年，“暗网”版的“维基百科”出现，起到了推波助澜的作用。在“暗网”版“维基百科”中大量敏感信息可以通过洋葱网络进行访问，大大提高了访问效率。与此同时，也出现了数个中文网站。尽管目前没有公开数据资料显示其为何时成立，但其中售卖的个人信息足以令你大开眼界。

儿童色情肆意传播　2016年，北京警方通过技侦手段，打掉国内利用“暗网”传播儿童色情的首个犯罪团伙，这也意味着目前国内已经存在

利用“暗网”犯罪的利益集体。通过前期的研究过程中也发现“暗网”中儿童色情的传播发达国家数量大于我国。在欧美一些国家定义中，儿童色情通常泛指“儿童虐待”。

“暗网”治理

加强国际间立法合作

2015年，习近平总书记在世界第二届互联网大会上提出了构建“网络空间命运共同体”的概念，为世界互联网的安全以及治理提供了新的方向；2016年，《国家网络空间安全战略》出台；2017年，我国正式颁布实施了《中华人民共和国网络安全法》，这不仅为我国网络安全治理提供强有力的法律保障，同时也为互联网安全治理提供了中国方案。

在“网络空间命运共同体”的概念提出后各国的网络安全法案也相继出台。如2017年新加坡的《网络安全法案2017》、2018年南非的《网络犯罪以及网络安全法案》、美国的《网络安全法案》、2019年欧盟也出台《网络安全法案》等，全球各国的法案中都提到了网络信息安全，标志着全球范围对网络空间安全的重视。

“暗网”犯罪的全球化，凸显出了国际间互联网治理的重要性。我国在治理方面不仅应加强与国际间的合作，同时应积极借鉴各国出台关于互联网的法律法规，在相应的层面上还应明确监管部门职责范围，规范网络服务供应商，以及用户的使用规范。此外，加强与国际间的网络安全交流，积极探索和构建新型国际互联网安全体制对于“暗网”空间的治理显得尤为迫切。

多国联合治理应对

暗网犯罪并不是单个国家的问题，而是全球所必须面临的问题，它的危害已经波及全球，产生了巨大影响。2019年1月初，欧洲执法机构联合加拿大、美国的执法部门开展了对“暗网”市场联合打击行动，在行动中执法部门共逮捕61人，并关闭10余个用来非法活动的账户，而仅在2018年欧洲刑警组织协调的网络巡逻周行动中，来自19个国家的60位专业人士确定了247个高价值的“暗网”目标并进行了立案调查，以及采取相关行动，效果显著。这不仅凸显了联合行动的优势，同时也为跨境犯罪打击以及合作提供长效机制。我国在这一阶段中应该积极学习国外先进治理经验，同时在警务合作方面加强与国际间的合作，积极推动多边合作机制。

加强加密货币的金融监管

“暗网”犯罪发展的根本原因在于，加密货币的流通。以比特币为主的一类去中心化加密货币不仅为“暗网”犯罪提供极为有效的经济支撑，同时也对加密货币管理提出了挑战。

以比特币为例，它是基于密码学的一种货币，其不需要政府或银行去管制和发行，通过一种区块链交易记录方式进行转账，只要通过互联网，就没人能阻止这笔交易。因此，基于这种优势使得其在暗网中成为通用货币。央行等五部委在2013年发布《关于防范比特币风险的通知》并宣布对比特币流通纳入监管范围。2018年日本金融服务局（FSA），做出对数字货币进行反洗钱监管的决定。此类监管手段以及做法为净化金融市场提供了保障，同时也对数字加密货币犯罪监管起到了积极作用。

加强技术投入，提升治理成效

根据欧洲刑警组织最新的“互联网有组织犯罪威胁评估”结果显示，“攻击性”“对抗性”是网络犯罪趋势且逐步上涨。“暗网”犯罪之所以棘手，包括三个方面。第一，“暗网”信息及其内容均经过Tor的层层加密，使得监管以及取证变得尤为困难。第二，洋葱浏览器中继节点众多，犯罪IP地址不断变化，犯罪地域确定非常困难。第三，国际间的合作以及协同缺乏，造成了对“暗网”空间治理的真空区域[1]。

“暗网”区别于互联网中的表网，必须依托Tor等加密软件的使用，才能进行访问。因此，对于“暗网”的技术治理应该从源头上加强治理，以技术制衡技术。美国国家安全局就通过利用Tor的技术原理漏洞进行侦查以及追踪犯罪嫌疑人。根据洋葱（Tor）的技术原理，跟踪其通信隧道，其通信隧道，依靠着全球志愿者的节点构成，而如果从该节点入手可以进行对其网关流量的分析进行追踪，这也是Tor的弱点所在。

参考文献：

[1]汤艳君，安俊霖．暗网案件的爬虫取证技术研究［J］．中国刑警学院学报，2018（5）：115-118.

（作者单位：南京森林警察学院）

责任编辑：王　楠