暗网治理需各国执法协同联动

本刊记者 王丹娜

虽然各国网络监视活动已成“常态”，然而，为避免遭到窥探和监测的暗网，却成为非法交易市场、黑市论坛以及网络犯罪的平台。因此，暗网的存在给各国网络空间治理带来更多挑战。

一、多国警方联合实施打击暗网行动

2017 年 7 月，由美国联邦调查局（FBI）、美国缉毒局 (DEA) 与荷兰国家警察总局主导，在英国、加拿大、法国、德国、立陶宛、泰国以及欧洲刑警组织（Europol）协助下采取的联合行动，关闭了全球规模最大从事毒品、武器和其他非法物品交易的暗网平台“阿尔法湾”（AlphaBay）。在荷兰，警方一直秘密收集数据并控制“汉萨”市场（Hansa Market）服务器。也是在 7 月 20 日，欧洲刑警组织和荷兰警方宣布，永久关闭该市场。此外，虽然俄罗斯当局已经在 7 月关闭只面向俄罗斯境内用户、以销售毒品而闻名的 Tor 市场——俄罗斯匿名市场（Russian Anonymous Marketplace，RAMP），但没有公开消息。直到 9 月，俄罗斯内政部官员向塔斯社（TASS）透露，俄罗斯警方已经承认，他们负责除掉了 RAMP。至此，据媒体报道，多国警方联合打击暗网行动的直接结果是，在 Deep Dot Web 网站 7 月 12 日暗网市场排名前 4 的交易市场 AlphaBay、RAMP、“梦幻市场”（Dream Market）和 Hansa Market，都被撤除。

二、各种利益叠加提升暗网治理难度

非营利组织 Tor Project 前执行董事卢曼曾指出，暗网是犯罪孕育之地，黑市交易日益猖狂，网络犯罪分子不断使用 Tor 匿名网络干非法勾当。据美国司法部长杰夫·塞申斯（Jeff Sessions）介绍，被打掉的 AlphaBay 网站上非法药物和有毒化学品销售列表超过 25 万条，偷窃或伪造的身份文件、恶意软件等销售列表超过 10 万条。正是因为有这样的规模和充斥暗网世界的各种违法行为，各国治理暗网的难度可见一斑。

1. 充斥暗网的各种违法行为

暗网世界充斥着军火、毒品、色情和诈骗等非法交易，诸如枪支、毒品、各国伪钞、人体器官等，甚至有恐怖组织招募成员、策划发动恐怖袭击。同时，暗网中同样存在欺诈，每个参与者的每场交易都充满风险，其中包括：直接导致“破财”的交易平台“退场骗局”，或“破财”+“人财两空”的交易平台被执法机构控制。当然，也可能出现暗网中的交易平台被黑客袭击，从而导致用户资金损失的情况。

第一，各种数据信息被出售

各种不同类型的数据在暗网市场出售。根据 2015 年 12 月 Mcafee 实验室发布关于暗网市场出售敏感数据价格的报告，在暗网市场出售的数据类型一般有财物数据、敏感系统访问权限、学校和医院等单位的数据库信息等。在暗网中出售的财务数据主要是信用卡，还包括储蓄卡和借记卡等银行卡信息。仅在 2017 年上半年，“阿尔法湾”就销售超过 500 万个被盗的信用卡号码，平均日交易额约为 80 万美元。在暗网黑市，250 美元可以获得美国社保卡（SSN），再加付 100 美元，可以拿到能够辅助进行身份认证的物业账单，而护照、医院通行证和警察身份证，只需 10 美元左右就能买到。选民和明星、网红信息也是暗网用户感兴趣的内容。2017 年 7 月，威胁情报公司 Looking Glass Cyber Solutions 称，美国

近千万选民记录在暗网仅售 4 美元，包括 9 个州超过 4000 万选民的信息。据苏格兰媒体报道，伦敦数据公司在对黑客在暗网出售逾 11 万条爱丁堡公民信息事件展开调查后发现，与 EH1、EH4 邮编有关的公民身份信息窃取案例共计 115，333 宗，是骗局中受影响程度最为严重的部分。2017 年 9 月，由于社交网络 Instagram 被黑，包括演员、歌手与运动员在内的男女明星、网红信息泄漏，被放置暗网出售。此外，包括窃自中国腾讯、网易、新浪等互联网公司的用户数据也在暗网销售。

第二，各种恶意软件和漏洞信息在售

2017 年 2 月，黑客在某暗网市场以 40 比特币价格出售针对 Mac OS 设备的新型远控木马“Proton”。其开发者宣称，这款恶意软件属于远程管理工具（RAT），无法被检测发现，且能够通过绕过反病毒软件检测以实现 Mac OS 设备全面控制等多种功能。2017 年 10 月，卡巴斯基研究人员在地下论坛发现一个售卖恶意软件的广告帖，售卖一整套 ATM 偷钱方案。这款名为 Cutlet Maker 的软件于 2017 年 5 月开始在 AlphaBay 销售，因为 AlphaBay 在 7 月中旬被关闭，软件经营方新建一个独立网站 ATMjackpot 专门销售该软件。根据广告，工具包整体打包售价 5000 美元，使用手册相当详细，包括作案需要的软件设备、可攻击的 ATM 机型，以及软件操作方法和偷窃小技巧，还附有操作演示视频。如果还看不懂，对方可以提供一对一在线解答，包教包会。反病毒服务提供商 Carbon Black 的威胁分析研究人员发现，从 2016 到 2017 的一年时间，暗网市场勒索软件的销量增加了 2502%。

第三，网络犯罪与恐怖活动

据媒体报道，2017 年初，AlphaBay 市场有 122 个供货商兜售芬太尼，238 个供货商叫卖海洛因。2017 年 8 月，暗网药头 Gal Vallerius 在前往美国参加世界胡子锦标赛后被捕，并被指控担任 Dream Market 的管理员、高级主持人和供应商，访问这个市场的人可以购买从海洛因到财务数据等各种违法信息和物品。然而，最恐怖的还是通过暗网匿名雇佣杀手谋杀。2016 年 10 月，美国新泽西警方破获一起在暗网提供杀手谋杀服务犯罪未遂的案件。此外，暗网也已成为恐怖分子宣传、招募、融资和策划活动的重要平台，助长网络恐怖主义的发展。联合国一个专家组在 2016 年向联合国安理会提交的报告中警告，“伊斯兰国”、“基地”等组织使用暗网招募外国成员，策划发动袭击，其加密信息即便水平最高的安全机构也无法破解，各国政府应对此保持警觉。

2. 黑产链条经济效益的驱动

有评论说，“网络犯罪生态系统历来都是由网络黑市数据的价值驱动的”。随着成功的网络攻击数量增多，网络罪犯的业务模式也正在发生转变，评估数据的价值成为一个重要维度。在被关停之前，AlphaBay 网站规模是“丝绸之路”的 10 倍。自 2014 年投入运营以来，该网站的交易额保守估计达 10 亿美元。据卡耐基梅隆大学教授 Nicolas Christin 的研究显示，AlphaBay 每日交易额约在 60–80 万美元，是当时“丝绸之路”的两倍。这样的用户和交易规模，能够带来的经济效益可想而知。在关闭 AlphaBay 后，“美国执法当局与多方国外合作伙伴一道冻结并没收了价值数百万美元的加密商品，而根据起诉书所言，这些加密商品的没收理由为——其代表了 AlphaBay 组织非法活动的收益。”从警方对捕获的暗网人员调查可以获知其经济收益情况：曾兜售专门攻击英国及其他欧洲国家服务器和网站的男子 Grant Manser，其在暗网销售的攻击工具价格从 4.99 英镑到 20 英镑不等，支付通过 PayPal 完成，几年时间总共获利 5 万英镑；被认为是 AlphaBay 联合创始人之一的加拿大人 Alexandre Cazes，被指控积累价值超过 2300 万美元的比特币（Bitcoin）、门罗币（Monero）、以太坊（Ethereum）、零币（Zcash）以及估值约为 1250 美元的汽车和房产，其现金分布在泰国、列支敦士登、瑞士、圣文森特和格林纳丁等国家的银行账户。

3. 不断出现的“继承者”

有专家认为，各国执法的打击和媒体的报道加剧了暗网发展。在一个又一个暗网平台被关闭的同时，

又有多个暗网平台“接替”发展，结果是暗网用户持续不断寻找合适的平台继续各种非法交易。在2013年曾经规模最大的暗网市场“丝绸之路”服务器被迫关闭后，AlphaBay随即于2014年崛起，并很快成为暗网市场的最大规模者。根据SurfWatch Labs从暗网收集到的情报，截至2015年10月，AlphaBay已经积累了20万名用户。2016年4月，在Nucleus Market关闭后，AlphaBay更是成为最热门的市场，成为“丝绸之路”的“继承者”。同样的情况出现在俄罗斯，在RAMP网站关闭后，暗网中出现了一个自称为RAMP 2.0的新网站。有报道称，在RAMP被关闭后的几周内，向俄罗斯用户出售违禁药品的暗网市场数量激增，这很可能因为RAMP的突然关闭推动了暗网出售非法药品新市场数量的增长。此外，还有报道称，一个叫RuTor的新市场进行大量宣传，俨然成为RAMP的接替者。从AlphaBay和RAMP被撤掉后的情况看，暗网市场并没有因为执法部门的打击行动而销声匿迹，用户的需求正通过平台转移，持续着这个产业生态链条的发展。

4. 虚拟货币交易的便捷

由于比特币经常“参与”暗网交易、敲诈勒索、僵尸挖矿等活动，被视作网络犯罪分子的专利。曾素有“黑市亚马逊”之称的“丝绸之路”官方指定唯一交易货币即是比特币。有报告显示，印度人使用暗网订购非法药品（主要是毒品），而且印度供应商在一些暗网市场上扮演重要角色。谷歌搜索数据显示，印度的比特币搜索几乎呈指数式增长。在类似Quora和Reddit这样的网站上，很多印度人讨论关于如何购买迷幻药和其他非法毒品的问题，但是暗网处在印度警方的掌控之外。比特币的快速发展已引起国际社会高度关注，各国陆续出台监管措施。2017年8月，美国国家税务局宣布与比特币安全公司Chainalysis联合发明一种工具，可以获知比特币钱包的所有者并监测洗钱活动。由于执法部门的大力打击，以及比特币交易变得更容易追踪，犯罪分子使用比特币交易的数量大幅减少。AlphaBay关闭后，其他数字货币，如以太币和门罗币等，已成为犯罪分子的新选择。根据Chainalysis公司在2017年8月发布的报告，以太币的网络犯罪正在快速增加；2017年，其网络犯罪营收已达到2.25亿美元。

虽然各国网络监视活动已成“常态”，然而，为避免遭到窥探和监测的暗网，却成为非法交易市场、黑市论坛以及网络犯罪的平台。

三、暗网治理需要多层设计和多元手段

欧洲刑警组织执行主任罗伯·温莱特指出，2017年“这次由欧洲及美国当局组织的缜密联合行动取得了巨大成功，在对世界各国的毒品贩运者以及其他重度罪犯分子施以有力打击之后，恶意活动目前已经得到有效控制。”虽然各国执法机构越来越关注对暗网的监控以及对暗网上各类非法交易的打击，但是依然没能够从根本上打破暗网的生态系统。在执法部门高调采取打击行动之后，很多暗网运营者也加强其自身安全，包括“必须通过审查才能进入论坛”。因此，暗网治理需要更多元的治理方法。

1. 加强传统侦查方式与现代信息技术的结合

从2017年各国执法机构的联合行动看，打掉AlphaBay和Hansa等市场的行动是基于警方传统的侦查方式与利用现代信息技术的结合。之所以FBI能够攻破AlphaBay，是因为AlphaBay管理员不小心泄露个人电子邮箱地址，正是因为Alexaandre Cazes的这个错误导致其真实身份被曝光，并最终被捕。根据法庭提供的资料，针对AlphaBay的调查开始时，调查人员通过传统侦查方式：伪装成卧底在AlphaBay购买商品，试图通过追踪邮件包追索到AlphaBay供应商。然而，这种方式基本上无效。后来，调查人员从邮件消息中检索到AlphaBay管理员的个人邮箱地址和几个PayPal账户，并最终确认邮件所有者身

份。此外，荷兰警方的做法是，调查 Dream 市场和 Hansa 市场上具有相同名字的账号，分析重合的账号是否使用相同密码。如果供应商在 Dream 上使用与 Hansa 平台一样的用户名和密码，同时又没有激活双因子认证（2FA），警方就会修改密码并锁定店铺。同时，荷兰警方采用的另一个方式是锁定带有跟踪功能的 Excel 文件。基于上述方式，荷兰警方在打掉 Hansa 市场时，收集了暗网中很多“重要人物”和大量供应商和买家的身份、登录和交易信息。

2. 利用机器学习等新技术手段进行监控

不断发展的信息技术为监控暗网提供了可能。一方面，可以利用大数据、机器学习等技术。2015 年 2 月，微软 Windows 操作系统的漏洞被曝光，虽然微软及时发布补丁修复，但是很快这个漏洞就在黑客社区传播。4 月，网络安全专家发现基于这个漏洞的 exploit 已经在暗网市场公开出售，要价 15,000 美元左右。7 月，基于这个漏洞开发的恶意软件 Dyre Banking Trojan 目标针对全球用户，可以从被感染的计算机上盗取用户信用卡相关信息。Eric Nunes 以及他所在的亚利桑那州立大学（Arizona State University）受此事件启示，利用爬虫技术抓取信息，监视黑客在暗网的活动，并使用机器学习研究黑客论坛及其交易市场。另一方面，可以建立低成本、高回报的暗网情报运营平台。软件即服务创业公司 Sixgill 开发网络情报平台，通过分析“大数据”连接暗网站点，创建暗网用户及其藏身的社交网络模型，找到网络罪犯所在位置，并攻破其技术防御设施。也有专家建议，某些机构和企业可以利用暗网收集更多情报数据。例如，软件供应链管理公司 Sonatype 的核心资产是 120 多万个开源数据包，一旦数据被泄漏，对公司将是致命打击，所以 Sonatype 对网络信息严密监控以便于及时感应到敏感数据泄漏或共享问题，其监控的对象就包括暗网。SurfWatch 实验室的创始人和首席架构师 Jason Polancich 指出，“对大多数企业而言，建立一个低成本、高回报的暗网情报运营平台的资源是充沛的，公司内部的 IT 和专业安全团队就可以完成这项任务”。从技术上看，专业的安全情报厂商会可以采用专业的工具，挖掘暗网中的数据，跟进暗网最新动向，解析暗网市场的变化趋势。

3. 制定有效防御战略提高态势感知能力

监控暗网的活动，可以在提高态势感知能力的同时，为各国制定有效防御战略提供必要视角。因此，有专家建议，在收集和存储感知信息过程中，应提高对暗网犯罪论坛的可视化能力，并限制重复的、低价值的任务，更多增加分析工作。而且，随着网络罪犯主体心态和能力的改变，决策者和防御者应该及时调整防御暗网违法行为的战略。

以英国为例，英国国家犯罪局（National Crime Agency, NCA）在 2017 年积极招募网络专家和暗网分析师，关注暗网市场的非法药物交易和其他违法行为。NCA 专门成立了暗网情报部门，并与其他网络情报和执行部门合作，共同打击暗网中的犯罪活动。根据 2017 年 6 月发布的全球毒品调查报告，高达 25% 的英国吸毒者通过暗网市场获取非法药物，排名在挪威和芬兰之后。随后，英国政府及其执法机构，包括国家反恐警务网（National Counter Terrorism Policing Network，NCTP）宣布针对全国暗网用户的警告。NCTP 进一步强调，单纯的访问暗网市场也可能被执法机关视为恐怖主义的标志。英国政府和执法机构的目标也是与世界各国的其他执法机构合作，彻底消除暗网中的网络犯罪组织。

然而，即便媒体报道美国国防部技术部门将会对暗网搜索引擎 Memex 进行优化和性能提升，可将适用范围将扩大到毒贩、恐怖分子、恋童癖者等，以及用于灾区救援等活动。但是，根据斯诺登曾泄露的一份美国国家安全局 2012 年 6 月的文档，国家安全局在摧毁某些暗网过程中遭遇种种困难，并明确表示，“我们将永远无法破解所有‘洋葱暗网’用户的真实身份。”可见，在这个问题上，国际社会还有很长的路要走。