论恐怖组织暗网化趋势

赵　航，曾　帝

（新疆大学 中亚地缘政治研究中心，新疆 乌鲁木齐　830046）

摘　要：随着国际反恐力量不断加强，互联网反恐力度进一步加大，恐怖组织在互联网上的活动逐渐呈现出暗网化趋势。利用暗网去中心化及隐匿性等特点，恐怖组织搭建宣传平台，密谋策划暴恐袭击，互联网反恐进入“深水区”。恐怖组织暗网化趋势是全球反恐取得阶段性胜利的结果，同时也是互联网技术同恐怖主义深度融合的体现。打击暗网恐怖主义已经提上议程，各国需要从技术、立法与合作三个层面，全面清剿恐怖主义在互联网领域的遗毒。

关键词：暗网；恐怖主义；反恐

中图分类号：D55　　**文献标识码：**A　　**文章编号：**1009-9115(2019)01-0114-05

DOI：10.3969/j.issn.1009-9115.2019.01.023

On Hidden Web Trend of Terrorist Organizations

ZHAO Hang, ZENG Di

(Research Centre for Geopolitics Of Central Asia, Xinjiang University, Urumqi 830046, China)

Abstract: With the strengthening of international counter-terrorism force, the internet counter-terrorism efforts have intensified. And the hidden web trend of terrorist organizations' activities gradually appears. Using hidden web, terrorist organizations establish propaganda platforms and plan terrorism attacks. Internet counter-terrorism has entered the “deep water zone”. The trend of the dark net of terrorist organizations is the result of the phased victory of global anti-terrorism, and it is also the embodiment of the deep integration of Internet technology and terrorism. The fight against hidden web terrorism has been put on the agenda, and all countries need to eliminate terrorism in the Internet field from three levels: technology, legislation and cooperation.

Key Words: hidden web; terrorism; counter-terrorism

互联网是一个多层结构，“表层网”处于互联网的表层，能够通过标准搜索引擎进行访问浏览。藏在“表层网”之下的被称为“深网”。深网中的内容无法通过百度、谷歌等常规搜索引擎进行访问浏览。“暗网”通常被认为是“深网”的一个子集，显著特点是使用特殊加密技术刻意隐藏相关互联网信息。

最新的互联网安全研究报告显示，57%的暗网被色情、非法融资、毒品买卖、武器贩运、制造假币、恐怖主义等非法内容所占据[1]。此外，大量受强权压迫的政治团体、维权人士以及调查记者也开始利用暗网进行秘密交流、策划行动。

一、恐怖组织与暗网

自 20 世纪 90 年代末以来，恐怖组织一直活跃在各种网络平台之上[2]。随着互联网反恐力度逐渐加大，恐怖组织在表层网络的活动空间受到挤压，逐渐转向暗网。伦敦奎利姆基金（London-based Quilliam Foundation）发布的资料显示，随着恐怖主义在表层网遭遇重创，恐怖分子开始涌入暗网，更加难以追踪。

特别是对“伊斯兰国”而言，自 2016 年开始在网络空间遭受重创。各大网络公司在打击网络恐怖主义方面的立场日趋相近，并且采取了有

基金项目：新疆维吾尔自治区社会科学基金项目（11BGJ071）
收稿日期：2018-04-27　　修回日期：2018-09-04
作者简介：赵航（1993-），男，回族，河北沧州人，硕士研究生，研究方向为国际政治。

效的反恐措施。以推特为例，作为“伊斯兰国网络圣战”兴起的策源地，“伊斯兰国”利用推特这一社交网络工具在全球范围内宣扬“圣战”思想。随后，推特公司果断采取行动，同政府及其他社交平台合作，利用技术手段对所有账户进行筛选，清除了大量宣扬极端宗教主义思想的账户。仅在 2015 年 6 月至 2016 年 2 月期间，推特就封禁了超过 12.5 万个同圣战组织相关的账户（主要是与“伊斯兰国”相关）[3]。2016 年 1 月至 8 月期间，推特清除 23.5 万个账户[4]。有报告称，仅在 2016 年 6 月至 10 月的短短 4 个月期间，与“伊斯兰国”相关的推特账户大幅下降[5]。此外，推特公司还加强审核制度，缩短响应时间，引入新的信息技术，同执法部门及研究所（如 PAVE、战略对话研究所）合作，共同打击恐怖主义[6]。2016 年 12 月，包括推特、脸书、微软、YouTube 在内的各大互联网巨头联手开发软件工具，用于识别恐怖图像和视频。通过建立共享数据库，及时有效地对暴力图像和恐怖主义视频进行识别并将其从互联网上删除[6]。

各互联网公司联合展开的反恐措施取得成效，使“伊斯兰国”在表层网的影响力不断下降。目前，各大社交网络中已经鲜见“伊斯兰国”的宣传信息。即使能够重新创建账户，但是在巨大的压力下，重新构筑网络沟通渠道需要耗费大量时间和精力。虽然该组织仍试图利用社交媒体进行宣传，却收效甚微。

由于恐怖组织在表层网的活动空间日益萎缩，迫使其走向暗网，寻找“网络庇护所”[7]。2015 年 11 月，巴黎暴恐袭击发生后，“伊斯兰国”网络宣传阵地逐渐向暗网转移。“伊斯兰国”宣传机构 Al-Hayat Media Center 发出声明称，这么做的目的在于隐藏其支持者真实身份以及避免遭受黑客袭击[8]。

综上所述，随着世界反恐形势不断演变，恐怖主义活动出现了新的变化，在互联网领域暗网化趋势逐渐加强，标志着恐怖组织对网络的利用更加深入，网络恐怖主义更加难以追踪与监控，国际反恐增添新变数。

二、恐怖组织暗网化趋势凸显

一般而言，恐怖组织暗网化仅仅是活动区域发生改变，其活动内容未发生根本变化。实际上，相较于表层网，暗网的去中心化、隐匿性特点更加突出。此外，据以色列纪录片《暗网深处》称，目前 99%的互联网都无法被常规搜索引擎检索，这 99%即为深网[9]。在数据体量方面，表层网的数据量仅仅是整个互联网空间的 4%，而深网包含的数据体量所占比例高达 96%[10]。值得注意的是，深网并不等同于暗网。即使如此，暗网中的数据流亦不可小觑。高度隐秘性、可观的数据流，加之深网环境下的无政府状态，为恐怖组织提供更多的活动空间进行非法交易、远程指挥、圣战宣传等破坏行动。

1. 比特币成为恐怖主义“流通货币”

随着国际金融体系日趋完善，金融交易逐渐透明化，外汇管制也愈加严格，恐怖组织难以通过表层面实现资金积累与转移，虚拟货币的出现为其提供了新的集资通道，使其能够在暗网的掩护下，将大量资金兑换成虚拟货币，进而实现资金转移。一些影响力较大的虚拟货币，如比特币甚至已经形成一个成熟稳定的产业链。2015 年，美国财政部发表报告称，由于借传统渠道向恐怖分子提供资金援助的渠道被切断，那些资助恐怖分子的人可能转而使用比特币等虚拟货币从事涉恐活动[11]。

暗网中存在大量非法交易平台，最为著名是“丝路网”（Silk Road）。该网站在暗网掩护下，售卖毒品、军火甚至性奴。最终在 2013 年，该网站遭受重创。在技术支持下，美国联邦调查局确认“丝路网”背后老板罗斯·乌布利希（Ross Ulbricht），并最终将其捉拿归案。据统计，在短短两年间，“丝路网”就在暗网中通过比特币交易，获取高达 12 亿美元的收入。在遭到政府查封 8 个月后，丝路网 2.0 出现，再次关闭后丝路网 3.0 上线[12]。在暗网这个无政府的互联网环境中，非法网络交易平台难以彻底断绝，就如希腊神话中的海德拉（Hydra）一般，再生能力极强。类似的非法交易平台还有 Agora、Amazon Dark、AlphaBay 等，无一例外都是在暗网世界中利用安全性相当高的比特币进行非法交易。根据 SurfWatch 实验室搜集的信息，截至 2017 年，仅 AlphaBay 一家就拥有 20 万用户，是当年“丝路网”体量的 10 倍[13]。

因此，恐怖组织能够通过这些非法交易平

台，使用比特币等虚拟货币购置武器、炸药，又能在暗网上贩卖人体器官（往往来自人质、俘虏）、石油、古董等，为“圣战”筹集资金[14]。

根据斯图加特检察官办公室发布的文件称，2015 年巴黎暴恐事件中，恐怖分子所使用的武器正是通过暗网购得的[15]。“奋斗伊斯兰无痕基金”也向“伊斯兰国”支持者提供暗网使用教程，募集“圣战资金”。2015 年，新加坡网络情报公司 S2T 发表声明称，一个盘踞于美洲的恐怖组织通过比特币在深网进行圣战募资，最终这笔资金流向“伊斯兰国”[16]。

2. Telegram 逐渐取代 Twitter

随着世界互联网巨头对恐怖主义打击进一步加强，恐怖组织越来越难以在传统社交网络中活动。暗网为他们提供了新的沟通渠道。美国国家安全研究所表示，近十年间，“基地”组织位于全球各地的分支组织领导人之间交流逐渐从传统方式转向通过暗网进行[17]。

除了继续在 Facebook、Twitter 等社交媒体上活动以外，“伊斯兰国”“基地”等恐怖组织开始使用一些具备一定安全性和隐私性的在线通讯程序进行圣战招募，比如 Skype、Signal、Whatsapp、SnapChat 及 Telegram[18]。其中，Telegram 凭借其优秀的加密算法，赢得了恐怖组织的青睐。恐怖主义分析研究分析联盟表示，大量宣传极端恐怖主义的社交媒体开始向 Telegram 转移[19]。国际反恐中心也在关于 Telegram 的报告中表示，自 2015 年 9 月，Telegram 涌入大量“伊斯兰国”相关账户。仅 2016 年 3 月，“伊斯兰国”就开放了 700 个宣传频道[20]。

实际上，Telegram 软件不仅被恐怖组织用于发布信息，同时也成为恐怖主义用于串联各地反政府主义者的工具。该软件具有超强的隐秘性，同时呈蛛网连接，每个用户都是信息传播的节点，可以实现大规模数据流的传播。在 2017 年末伊朗政治骚乱中，反政府主义者正是利用这一软件，迅速在伊朗全境煽动反政府游行，最终迫使伊朗政府不得不暂时屏蔽 Telegram。

3. 极端思想宣传平台

同表层网相比，进入暗网需要一定的技术，因而恐怖组织在暗网进行的宣传难以直接影响互联网受众人群，引发“雪球效应”。但是，暗网去中心化程度更高，隐秘性更强，能够帮助恐怖组织网络宣传平台避过监测和封禁。如今大多数极端伊斯兰组织的宣传信息都逐渐转向暗网，大量极端思想宣传资料在暗网涌现。由于缺乏监管，恐怖主义迅速蔓延，俨然已经成为伊斯兰极端思想传播的据点。

在“伊斯兰国”的影响下，阿拉伯半岛基地组织、利比亚圣战组织、努斯拉阵线、伊斯兰军、基地组织也门分部等恐怖组织也开始将其宣传平台转向暗网及在线通讯程序。

恐怖组织在暗网建立极端主义的数据库，如“圣战维基”（Jihadwiki），进行圣战思想宣传。巴黎暴恐事件发生后，仅在 Telegram 上就至少存在 78 个伊斯兰群组，人员还在不断增多。

为了加大宣传效应，恐怖组织在表层网发表相关制作教程，指导他们的支持者应用暗网探查这些组织的发展境况。2015 年，“伊斯兰国”宣传部门在相关网站上列出在暗网联系“伊斯兰国”的方法和镜像。同年 12 月，“基地”组织也发布暗网使用教程，确保其支持者能够通过暗网获取与“圣战”相关的信息。该指南不仅包括相关软件下载和使用教程，还教授使用者如何避免被安全部门定位或识破身份。

三、暗网化趋势带来的挑战及应对措施

暗网已经成为全球恐怖组织和跨国犯罪的主要平台。2016 年 4 月，美国时任总统奥巴马在同 50 个国家元首及外交部部长会晤时指出，恐怖分子试图通过暗网购买铀和钚等核材料，通过无人机投放放射性物质。同年，法国时任内政部长贝尔纳·卡泽纳夫表示，在欧洲制造暴恐袭击的恐怖组织大都是利用暗网，通过加密信息进行密谋策划。尽管各国都加强了对网络平台的监管力度，但是随着恐怖组织内部越来越多的人掌握 IT 技术，在互联网空间，政府难以彻底掌握其踪迹。根据美国国土安全部的报告，仅 2014 年就有超过 64 万起针对美国政府机构的网络袭击[21]。恐怖组织“明暗游击”的网络策略，使得各国安全部门难以有效应对。

1. 暗网化趋势为全球反恐带来技术和法律障碍

暗网是一个类似于蜂巢形状的组织结构，由多个网络互连的网桥搭建而成，存在数以万计的网络节点，可供恐怖分子隐藏。在无政府状态的暗网中，各个节点甚至可以实现自行组网，形成巨大的信息流，在遭遇各国政府打击时，能够迅速隔离被打击的节点，因而难以追踪打击。就如“丝路网”的案例一样，安全部门即使成功拔除一个网点，其他网点也能在短时间内搭建相同的组织网络。暗网之下，毒品贩运、器官买卖、军火交易等非法交易如同野草一般盘根错节，难以彻底铲除。

互联网用户同网络反恐之间的症结难解。暗网的产生正是在互联网用户希望确保其隐私的基础上产生的。匿名性成为暗网的一大特征。恐怖组织正是利用这一点，在暗网大肆传播宗教极端主义思想，进行器官买卖、毒品交易等非法活动。目前，各国在互联网反恐上并未形成统一的法律条款，整个暗网，甚至是互联网都基本处于无政府状态。自互联网产生之初，“黑客理论”就已经诞生，自由联通成为互联网的显著特点，政府任何干涉行为都会引发民众的强烈反弹。最具代表性的例子是，2016 年苹果公司拒绝协助 FBI 破解手机密码，获取用户信息。随后，谷歌、脸书、微软等公司对苹果公司这一决定表示支持。因此，如何把握平衡，在有效保护公民隐私的情况下，完全清除网络空间内极端主义遗毒成为当前网络反恐不得不面对的难题。

一对一的交流方式加大了网络反恐的难度。出于隐蔽性考虑，当前恐怖组织开始减少在表层网直接发布暴恐信息，逐渐转入暗网。在暗网世界里，通过动态地址实现一对一地交流，最具代表性的就是 Telegram 通讯软件。该软件具有“阅后即焚”的特点，反追踪能力极强，使得反恐部门难以掌握通讯者信息。此外，随着智能手机普及，接入暗网的应用软件大量出现，如 ORBOT 等，特别是对安卓系统而言，开放性的系统使其更容易摆脱反恐部门的监管。

2. 全面应对恐怖组织暗网化

暗网产生的最初目的在于通讯加密。对暗网下恐怖主义及其他犯罪的打击也应当从技术层面出发，寻找解决途径。作为暗网的创造者，美国国防部高级研究项目署（DARPA）认为可以通过相关软件对暗网进行监控。早在 2002 年，美国联邦调查局就开始在暗网中使用网络调查技术（Network Investigative Technique，NIT）锁定暗网上的匿名用户。网络调查技术旨在提供互联网用户的真实 IP 地址，无论他们是否进行代理设置，其目的是访问计算机，获取系统相关信息或计算机中包含的数据[22]。随着相关技术的成熟，将进一步加强在网络空间对恐怖组织的打击力度。

建立完善的管控措施。恐怖组织之所以会出现暗网化趋势，最大的原因在于国际社会对暗网缺乏管控，相较于表层网，暗网无政府状态更加明显。为了有效应对这一趋势，各国政府已经开始立法，加强对暗网进行管控。美国成立“网络威胁情报整合中心”，出台《网络安全法》。中国实行的《中华人民共和国网络安全法》及《中华人民共和国反恐怖主义法》将落实网络安全明确写进法律条文。英国则通过“调查权力法草案”，授予安全部门更大网络调查权，并且建立网络安全部队。法国也自 2015 年开始实施《反恐情报监控法》。俄罗斯政府甚至要求日访问量在 3 000 以上的网站向政府报备，放弃匿名权，且政府有权关闭网络[23]。

借助大数据分析，加强网络合作。通过大数据建立有针对性的监控机制，随时对网上暴恐信息进行搜索分析。此外，对移动终端上监管工作也需加强。各大应用商应随时检查上线应用，及时阻挡所有涉及暴恐的应用程序传播。其中，应给予安卓手机更多的关注。

恐怖组织暗网化是世界反恐战争取得的阶段性的结果。当前，互联网反恐随着暗网化趋势已经进入“深水区”，需要尽早制定全面打击互联网恐怖主义的战略，进一步加强网络管控力度，消除来自网络的威胁。网络恐怖主义更像是传统恐怖主义在互联网时代延伸出来的分支，其根源还在于恐怖组织实体。因此，在加强网络管理的同时，应当加强对恐怖组织的物理打击，从根源上消除网络恐怖主义。

[参考文献]

[1] Daniel Moore, Thomas Rid. Cryptopolitik and the Darknet[EB/OL]. http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085, 2016-02-01/2017-7-23.

[2] Weimann, Gabriel. Terrorism in Cyberspace: The Next Generation[M]. Columbia University: Woodrow Wilson Center Press, 2015: 7.

[3] Twitter Blog. Combating Violent Extremism[EB/OL]. https://blogs.kingston.ac.uk/twitter/, 2016-1-5/2017-7-25.

[4] Anthony Cuthbertson. Hackers hijack ISIS Twitter accounts with gay porn after Orlando attack[EB/OL]. https://www.newsweek.com/nisis-twitter-accounts-gay-porn-orlando-attacks-anonymous-470300, 2016-06-14/2017-07-23.

[5] J. M. Berger, Heather Perez. The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters[EB/OL]. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf, 2016-02-24/2017-7-24.

[6] Facebook. Partnering to Help Curb Spread of Online Terrorist Content[EB/OL]. Facebook Newsroom, 2016-12-5/2017-7-23.

[7] Berton Beatrice. The dark side of the web: ISIL's one-stop shop?[EB/OL]. http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf, 2015-06-23/2017-07-23.

[8] 新华网.国际黑客组织"匿名者"向"伊斯兰国"宣战[EB/OL].http://news.xinhuanet.com/world/c_128438829.htm, 2015-11-18/2017-7-24.

[9] 以色列时报.暗网深处——互联网的另一个世界[EB/OL].http://cn.timesofisrael.com/暗网深处-互联网的另一个世界,2016-7-20/2017-7-23.

[10] 姚华.追踪隐藏在暗网深处的匿名者[J].计算机与网络,2015,(13):36-37.

[11] 网易科讯网.恐怖组织被指用社交媒体和比特币来募集资金[EB/OL].http://tech.163.com/15/0613/10/AS00SFS H000915BF.html, 2015-6-13/2017-7-23.

[12] TECH2IPO.拥有不死之身的网络交易黑市 Silk Road[EB/OL].http://www.chinaz.com/start/467839.shtml, 2015-11-09/2017-07-23.

[13] 搜狐网.史上最大规模"暗网"市场被打掉[EB/OL]. http://www.sohu.com/a/159864125_166723,2017-7-25/2017-07-25.

[14] Andreas Wimmer, Aulia Nastiti. Darknet, Social Media, and Extremism: Addressing Indonesian Counterterrorism on the Internet[EB/OL]. https://www.academia.edu/20813843/DARKNET_SOCIAL_MEDIA_AND_EXTREMISM_ADDRESSING_INDONESIAN_COUNTERTERRORISM_ON_THE_INTERNET,2015-07-02/2017-7-23.

[15] Fox News. Germany arrests man reportedly suspected of selling guns to Paris attackers[EB/OL]. http://www.foxnews.com/world/germany-arrests-man-reportedly-suspected-selling-guns-to-paris-attackers.html, 2015-11- 27/2017-7-23.

[16] Haaretz-Isreal News. U.S.-based ISIS Cell Fundraising on the Dark Web[EB/OL]. http://www.haaretz.com/middle-east-news/premium-1.639542, 2015-01-29/2017-07-23.

[17] The Institute for National Security Studies. Backdoor Plots: The Darknet as a Field for Terrorism[EB/OL]. http://www.inss.org.il/index.aspx?id=4538&articleid=5574, 2013-09-10/2017-07-23.

[18] Anna Erelle. Skyping with the enemy: I went undercover as a jihadi girlfriend[EB/OL]. The Guardian, https://www.theguardian.com/world/french-journalist-poses-muslim-convert-isis-anna-erelle, 2015-03-26/2017-7-23.

[19] Fitnaphobia. Terrorism Research & Analysis Consortium. Massive Terrorist Migration to Telegram, the new Jihadist Destination[EB/OL]. http://fitnaphobia.com/2015/11/massive-terrorist-migration-to-telegram-the-new-jihadist-social-media-destination, 2015-11-04/2017-07-24.

[20] Michael Barak. The Telegram Chat Software as an Arena of Activity to Encourage the "Lone Wolf" Phenomenon[EB/OL]. www.ict.org.il/Article/1673/the-telegram-chat-software-as-an-arena-of-activity-to-encourage-the-lone-wolf-phenomenon, 2016-07-10/2017-07-23.

[21] 新浪网.恐怖组织ISIS转入暗网网络战场成反恐前线[EB/OL].http://gd.sina.com.cn/sztech/hlw/07563350.html, 2015-11-20/2017-7-23.

[22] 搜狐网. FBI 使用 NIT 技术将性诈骗犯抓捕归案存争议[EB/OL].http://www.sohu.com/a/163543023_257305, 2017-08-10/2017-07-24.

[23] 赵志云,张旭."暗网"应用情况及监管方法研究[J].知识管理论坛,2016,(2):124-129.

（责任编辑、校对：孙尚斌）