基于暗网环境的网络恐怖主义及其治理

黄紫斐[1]，刘洪梅[2]，张舒[2]
（1. 上海外国语大学国际关系与公共事务学院，上海 200083；
2. 中国信息安全测评中心，北京 100085）

[摘要] 恐怖组织及其支持者使用网络作为信息传播工具，已成为网络恐怖主义的常态。随着国际上加大打击恐怖主义，网络恐怖主义转向暗网环境，给国际社会和国家安全带来新的风险。对此，应从网络技术、社会舆论、执法监管、国际合作4个方面提升对暗网恐怖主义的治理能力，应对网络恐怖主义的新威胁。

[中图分类号] D815;TP393.08　　[文献标识码] A　　[文章编号] 1009-8054(2018)12-0050-13

1 网络恐怖主义：信息传播的视角

网络恐怖主义（Cyberterrorism）一词于1997年被学术界提出，是指网络空间与恐怖主义相结合的产物①。它最早仅仅被描述为恐怖分子“对计算机信息系统、程序进行破坏性的攻击”，现在则包括“利用网络散布恐怖信息、组织恐怖活动”②。具体而言，出于恐怖主义目的而进行的下列活动都属于网络恐怖主义研究的对象范围：①使用传统工具，破坏网络系统；②使用黑客工具，入侵或破坏网络系统；③使用网络信息传播工具，如Web网站、社交媒体、组网工具，进行沟通、宣传、招募等。

事实上，恐怖分子破坏、入侵网络系统的行动还只是一种可能的威胁，现实中尚无成功案例。其原因在于：①网络结构本身具有很强的弹性，简单的物理破坏行动不足以对整个系统造成重大的影响；②仅仅破坏部分网络设施不足以实现恐怖主义的最终目的，其效果远远比不上传统的恐怖袭击；③恐怖分子还未获得开展高级黑客攻击行动的能力。目前，使用网络作信息传播工具才是网络恐怖主义的常态③。

互联网是网络恐怖主义滋生蔓延的温床。2013年联合国安理会2129号决议表达了对“恐怖分子及其支持者越来越多使用互联网进行招募、煽动、筹资、策划等活动”的关切，强调“会

① 唐岚. 网络恐怖主义面面观 [J]. 国际资料信息，2003(07):1-7.
② 余硕，刘旭. 网络恐怖主义新动向及其治理分析 [J]. 情报杂志，2018(02):37-44.
③ 郎平. 网络恐怖主义的界定、解读与应对 [J]. 信息安全研究，2016(10):882-887.

万方数据

员国必须协力防止恐怖分子利用技术、通信和各种资源来煽动支持恐怖主义”①。

同时，近年来许多国家都出台反恐怖主义和网络安全法律，实施更严厉的反恐措施，加强对恐怖主义信息内容的追踪和监控，极大地限制了恐怖组织的信息传播能力。涉及恐怖主义内容的网站和社交媒体账号常常在很短时间内就被关闭，并且成为执法安全部门调查恐怖组织的重要线索。

2015 年“伊斯兰国”的数百个网站遭关闭后，该组织发布新的暗网（Darkweb）网址②，表明随着国际网络反恐力度加大，网络恐怖主义开始向暗网寻求信息传播的空间。

2 暗网环境下的信息传播特点

暗网络（Darknet）是一种建立在互联网基础之上的匿名网络。Tor、Freenet、I2P 是 3 种常见的暗网络，用户需使用相应的软件工具连入暗网络，成为其中的节点。同时，用户可以在暗网络上配置 Web 服务，如网页浏览、文件共享、电子邮件等，生成丰富的暗网（Dark web）资源，供暗网络上的其他用户访问。以 Tor、Freenet、I2P 为例，可以概括出暗网环境下信息传播的特点包括：

2.1 通信的匿名性

在基础的互联网环境下，节点之间传输的数据包含有明文格式的源 IP 地址和目标 IP 地址，任何用户都可以对经过其节点的数据包进行解析，从而实现追踪、监控。但 Tor、Freenet、I2P 暗网工具通过非对称加密、P2P 路由、虚拟隧道等技术，实现暗网环境下的匿名通信。匿名性是指除传输路径上的相邻节点以外，其他节点用户无法解析出数据包的真实来源地址和目标地址。当网络节点越多、传输路径越长时，数据包的来源越不容易追踪。

在暗网络中建立网站并不需要在互联网域名管理机构注册域名。在当前的版本下，每个用户都可以在暗网络中配置 Web 服务，建立个人网站，发布信息内容。基于暗网络通信的匿名性，暗网用户在自由发布和接收信息时，可以避免被他人追踪。因此，暗网用户常常可以放心地传递秘密信息，也可能肆无忌惮地发布在明网上不敢发布的内容，如暴力极端、盗版侵权、淫秽色情、虚假谣言等内容。

2.2 跨越地域范围

暗网络由互联网上自愿运行 Tor、Freenet、I2P 工具的节点组成。而如今互联网已经覆盖全球超过 176 个国家或地区、48% 的人口③。因此，暗网也具有跨越国家地域范围的能力。以最大的暗网络 Tor 为例，截止 2018 年 11 月，以直连方式进入 Tor 网络的用户约有 200 万，用户主要分布在美国、俄罗斯、阿联酋、德国等；以桥接方式进入 Tor 网络的用户约 6 万，用户主要分布在俄罗斯、美国、伊朗、印尼等④。

① 联合国安全理事会 . 第 2129（2013）号决议 [EB/OL].(2013-12-17).http://www.un.org/zh/documents/view_doc.asp?symbol=S/RES/2129(2013).
② GabrielWeimann. Terrorist Migration to the Dark Web[J].Perspectives on Terrorism, 2016(03):40-44.
③ ITU.Measuring the Information Society Report[EB/OL].https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf.
④ Tor Metrics. Analysis[EB/OL].https://metrics.torproject.org/userstats-relay-country.html.

万方数据

互联网的应用具有一定的地域特征，地方监管机构可以通过对电信服务、互联网信息服务等行业的行政管理，实现对非法内容或虚假诈骗信息传播的限制。然而，监管机构很难辨别互联网中的哪些节点组成暗网络，在暗网上设立网站、提供网络服务并不需要实名。在世界某一角落建立的暗网网站可以向任何国家或地区的暗网用户传播信息内容，而监管机构很难追踪网站服务器和访问者的真实位置及身份。在摧毁暗网交易网站AlphaBay的行动中，执法部门跨越美国、加拿大、泰国等地，才确定网站管理者和网站服务器所在的位置[①]。

3 暗网恐怖主义的表现形式

暗网环境下的信息传播具有匿名、跨国的特点，吸引了不同类型的群体使用。记者、线人可以利用暗网放心地传递信息而不暴露身份，军队可以利用暗网隐藏指挥控制系统，执法部门可以在暗网上收集情报、引诱罪犯，个人可以在暗网上讨论敏感话题、共享盗版资料等[②]。对于恐怖组织而言，为实现恐怖主义目的，可将暗网用于以下场景：

3.1 建立信息传播网站

连入Tor、Freenet、I2P网络的节点用户都可以配置Web服务，建立自己的匿名网站。这些匿名网站同样具有“域名地址”，但无需在互联网域名管理机构注册和备案。据不完全统计，3种暗网域名地址的总数比例约为：Tor占80.3%、Freenet占14.9%、I2P占4.8%[③]。可见Tor网络规模较大、开放的资源最多，但Freenet和I2P网络也不容忽视，其中存在许多鲜为人知或仅向好友用户开放的个人站点。

一些不愿被追踪的组织或个人倾向于在暗网上建立网站，将不便于在互联网上发布的内容发布在暗网网站上，如窃取的文件、色情图片、盗版音视频、反社会主张等。但同时，仅仅由业余用户运营的暗网网站通常只有简单的静态网页，内容更新较慢。并且由于内容发布者的身份难以验证，暗网网站上内容的真实性存疑，其中不乏诈骗、虚假信息或恶意程序。此外，也有一些网站是由情报机构建立，用于收集访问数据、分析暗网用户的特征。

2015年巴黎恐怖袭击案发生后，数百个“伊斯兰国”相关的网站被关闭。为此，“伊斯兰国”的传媒组织（Al-Hayat Media）将站点迁移至暗网，并且在Shamikh论坛上发布访问暗网站点的方法[④]。暗网成为“伊斯兰国”传播信息的另一重要平台。2016年4月，又有两个“伊斯兰国”的暗网网站被发现，但页面更加简陋[⑤]。

① The Verge. Dark Web drug marketplace AlphaBay was shut down by law enforcement[EB/OL].(2017-07-14).https://www.theverge.com/2017/7/14/15975140/alphabay-dark-web-drug-marketplace-police-shutdown-silk-road.

② Michael Chertoff, Tobby Simon. The Impact of the Dark Web on Internet Governance ad Cyber Security[EB/OL]. https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

③ 杨溢，郭晗，王轶骏等．基于Tor的暗网空间资源探测[J]. 通信技术，2017,50(10):2304-2309.

④ Krypt3ia. The First Official Da’esh DARKNET Bulletin Board Has Arrived[EB/OL].(2015-11-15).https://krypt3ia.wordpress.com/2015/11/15/the-first-official-daesh-darknet-bulletin-board-has-arrived/.

⑤ Krypt3ia. Two More Da’eshbag Darknet Sites Popped Up[EB/OL].(2016-04-29).https://krypt3ia.wordpress.com/2016/04/.

万方数据

从目前已知的资料来看，恐怖组织建立暗网网站的主要用途是宣传。然而这些网站缺少新鲜内容，且域名地址鲜为人知，因此，与推特、Facebook、Telegram 等社交媒体平台相比，暗网网站的宣传作用极其有限。但不排除有更多尚未被公众知晓的暗网恐怖主义网站。随着暗网用户的增加，暗网恐怖主义网站还可能进一步演变升级。

3.2 组织内部秘密联系

暗网本身具有匿名的基本特性，是进行秘密通信的绝佳工具。暗网上的秘密通信方式主要有：①暗网电子邮件。Tor、Freenet、I2P 网络上都有电子邮件服务，可为用户转发和保存邮件。②暗网聊天室网站。在 Tor 上有许多匿名、实时聊天网站，如 The Hub、OnionChat[①]。③匿名社交媒体平台。暗网上的热门论坛如 Hidden Answer 具有社交功能。2014 年 10 月，Facebook 在 Tor 上建立站点 Facebookcorewwwi.onion[②]，至 2016 年 4 月，该暗网 Facebook 的月访问量达到 100 万[③]。④即时聊天工具。Telegram 支持端到端的秘密聊天模式而深受暗网用户喜爱。而 FireChat 可使手机通过蓝牙、WiFi 连接组成暗网络，用于组织现场行动。

Telegram 是最受“伊斯兰国”组织及其支持者青睐的通讯工具，它可以用于传播恐怖主义内容、散发培训资料、招募恐怖分子等。2015 年 11 月巴黎恐怖袭击事件后，Telegram 公司关闭 78 个与“伊斯兰国”相关的公共频道，这些公共频道被“伊斯兰国”用于传播非法内容。但 Telegram 的私密聊天模式仍然能够为恐怖分子的秘密联络提供支持。与此同时，媒体公布的一份“伊斯兰国”行动安全手册显示，除推荐 Tor 浏览器上网以外，该组织还建议使用 FireChat、Hushmail、Telegram 私密模式、阅后即焚的 Wickr 等实现安全的通信联系[④⑤]。

3.3 使用暗网秘密市场

在 Tor 或 I2P 网络中，有一些网站专门为买卖违禁药品、武器、被盗财物和个人信息的商贩提供平台，这类网站被称为暗网秘密市场（Cryptomarket）。此外，还有更多商贩单独在暗网建立个人商品展示网站，或者直接在暗网社交平台上发布商品出售信息，进行秘密交易活动。

2013 年以来，美国政府执法部门牵头发起多次打击 Tor 网络上秘密交易市场的跨国联合行动，先后摧毁了 SilkRoad（2013）[⑥]、SilkRoad

① Congressional Research Service, Kristin Finklea. Dark Web[EB/OL].(2017-03-10).https://fas.org/sgp/crs/misc/R44101.pdf.
② Wired. Why Facebook Just Launched Its Own 'Dark Web' Site[EB/OL].(2014-10-31).https://www.wired.com/2014/10/facebook-tor-dark-site/.
③ Quartz.A Million People Now Access Facebook on the "dark web" every month[EB/OL].(2016-04-22).https://qz.com/667880/a-million-people-now-access-facebook-on-the-dark-web-every-month/.
④ Wired.Several Cyber Security to Protect your Account in the Social[EB/OL].(2015-11-19).https://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf.
⑤ Wired.Security Manual Reveals the Opsec Advice Isis Gives Recruits[EB/OL].(2015-11-19).https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.
⑥ TheGuardian.FBI Claims Largest Bitcoin Seizure after Arrest of Alleged Silk Road Founder[EB/OL].(2013-10-02).https://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin.

万方数据

2.0（2014）、Hydra（2014）、Cloud 9（2014）[①]、Hansa（2017）、AlphaBay（2017）[②]六个运营在Tor网络上的交易网站，并且扣押了其服务器。此外还有Atlantis（2013）、Agora（2015）、Evolution（2015）等网站的匿名管理者主动关闭了其交易平台。

上述暗网交易网站主要用于违禁药品交易，使用数字加密货币（如比特币）作为支付工具。根据FBI探员的报告，截至2013年9月，有将近1.3万件违禁药品出现在SilkRoad网站上，秘密探员在调查中验证了部分毒品交易的实现。此外，SilkRoad上的商家还列出电脑黑客服务、黑客工具、武器弹药、职业杀手等项目[③]。

除了毒品外，小型轻武器（Small Arms and Light Weapons）是暗网市场上的另一个主要的交易项目。2016年9月的数据显示，在当时的12个暗网秘密市场上共有16.7693万件交易物品，其中武器相关的物品总数为811件，占4.8%。而AlphaBay网站上就含有414件武器相关的交易物，是最大的暗网武器交易平台[④]。

在巴黎恐怖事件中，恐怖分子使用的武器被疑为从暗网上一名叫DW Guns的德国商贩处购买[⑤]。也有报告指出一些恐怖组织使用暗网交易市场出售人体器官、被盗的石油、文物等物品[⑥]。而为了在暗网秘密市场上活动，恐怖组织首先需要筹集、使用数字加密货币（Cryptocurency）。一名“伊斯兰国”支持者曾在社交网络上发布筹集资金指南，建议建立“比特币”钱包为恐怖组织在暗网上的交易提供帮助[⑦]。这表明，加密数字货币和暗网秘密市场的结合，已经带来新的恐怖主义筹资、洗钱威胁。

4 暗网恐怖主义风险及治理

叙利亚内战爆发以来，“伊斯兰国”迅速崛起。该组织善于运用互联网[⑧⑨]，代表着网络恐怖主义的发展趋势[⑩]。以2015年11月巴黎恐怖袭击事件为转折点，国际上开始加强对互联网上“伊斯兰国”相关内容的监控和打击力度，各国政府、科技公司、黑客组织等纷纷对网络恐怖主义发起进攻，主流网络上的恐怖主义由盛转衰。然而，暗网的兴起为网络恐怖主义生存提供良好的环境，比特币、秘密市场、社交

① Wired. Not Just Silk Road 2: Feds Seize Two Other Drug Markets and Counting[EB/OL].(2014-11-06).https://www.wired.com/2014/11/dark-web-seizures/.
② Europol. Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation[EB/OL].(2017-07-20).https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.
③ FBI. Ulbricht Criminal Complaint[EB/OL].https://assets.documentcloud.org/documents/801103/172770276-ulbricht-criminal-complaint.pdf.
④ GiacomoPersiPaoli. The Trade in Small Arms and Light Weapons on the Dark Web: A Study[EB/OL].(2018-10-22).https://www.un.org/disarmament/update/the-trade-in-salw-on-dark-web/.
⑤ GabrielWeimann.Terrorist Migration to the Dark Web[J].Perspectives on Terrorism,2016(03):40-44.
⑥ Andreas Wimmer. Darknet, Social Media nad Extremism: Addressing Indonesian Counterterrorism on the Internet[EB/OL].https://www.academia.edu/20813843/Darknet_Social_Media_nad_Extremism_Addressing_Indonesian_Counterterrorism_on_the_Internet, 2015.
⑦ Business Insider. Supporter Of Extremist Group ISIS Explains How Bitcoin Could Be Used To Fund Jihad[EB/OL].(2014-07-08).https://www.businessinsider.com/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7.
⑧万婧.“伊斯兰国”的宣传[J].新闻与传播研究,2015(10):96-110.
⑨思思.“伊斯兰国”的互联网攻势及其影响[J].现代国际关系,2016(02):32-39.
⑩马国春,曹君.网络恐怖主义中的“伊斯兰国”[J].上海公安高等专科学校学报,2015(03):90-96.

万方数据

论坛、匿名通信等组成一个适合恐怖主义的理想生态系统[①]。

但暗网环境并不是专门为恐怖主义生存而设计的保护伞，它也并非绝对安全：①与互联网的节点数相比，暗网络上的节点数目极少，且暗网节点本身也是互联网的节点，使用 Tor、I2P 等暗网应用软件的监管者可以通过在网络层监测数据包，分析暗网主要节点的位置和传输路径，进而控制暗网线路并追踪暗网用户。②暗网资源不易搜索，且暗网上的活跃用户很少，恐怖分子首先需在明网上传播暗网使用方法和暗网网站资源的地址，从而暴露位置。③情报机构也在暗网上以匿名身份活动，或建立钓鱼网站，或建立收集暗网数据包的中继节点，更方便地打击恐怖组织。

针对暗网环境下网络恐怖主义的风险和特点，政府和科技行业已开始研究和实施应对策略。美国国防部于 2014 年 2 月发起 Memex 项目[②]，针对暗网内容不被标准商业搜索引擎索引的问题，试图通过个体间互动和信息共享的方式，实现对暗网网站的搜索能力[③]。亚利桑那大学则建立暗网研究项目，包括收集圣战网站、抓取论坛数据、分析暗网内容中情绪、链路和来源分析等[④]。也有报告提出对暗网实施监控的策略，包括绘制暗网域名服务节点的目录、监测用户数据、扫描明网社交网站上的暗网信息、分析暗网市场等[⑤]。

我国近年来加强打击网络恐怖主义。2015 年出台的《反恐怖主义法》在第 19 条规定电信业务经营者、互联网服务提供者以及网信、电信、公安、国家安全等主管部门对“含有恐怖主义、极端主义内容信息”的监管措施和责任[⑥]。2016 年出台的《网络安全法》在第 12 条规定任何个人和组织不得利用网络“宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视”等[⑦]，明确网络恐怖主义的非法性质。此外，由外交部和国家互联网信息办公室共同发布的《网络空间国际合作战略》提出“深化打击网络恐怖主义和网络犯罪国际合作”的行动计划[⑧]。随着网络恐怖主义向暗网转移，我国反恐怖主义工作面临新的挑战，需要综合各方面资源，对暗网恐怖主义问题进行治理。

4.1 网络技术方面

暗网是建立在互联网应用层之上的网络，

① Beatrice Berton. The Dark Side of the Web: ISIL’s One-stop Shop?[EB/OL].(2015-06).https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf.

② FBO. DARPA-BAA-14-21: Memex[EB/OL].(2014-02-04).https://www.fbo.gov/index?s=opportunity&mode=form&id=426485bc9531aaccba1b01ea6d4316ee&tab=core&_cview=0.

③ DARPA. Memex[EB/OL]. https://www.darpa.mil/program/memex.

④王琳，杜雪．暗网项目：美国网络反恐情报研究的典范 [C].(2017-12-24).2017 3rd International Conference on Humanity and Social Science（ICHSS 2017).

⑤ Michael Chertoff, Tobby Simon. The Impact of the Dark Web on Internet Governance ad Cyber Security[EB/OL].https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

⑥中国人大网．中华人民共和国反恐怖主义法 [EB/OL].(2018-06-12).http://www.npc.gov.cn/npc/xinwen/2018-06/12/content_2055871.htm.

⑦中国人大网．中华人民共和国网络安全法 [EB/OL].(2016-11-7).http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm.

⑧中共中央网络安全和信息化委员会办公室中华人民共和国国家互联网信息办公室．网络空间国际合作战略 [EB/OL].(2017-3-1).http://www.cac.gov.cn/2017-03/01/c_1120552617.htm.

万方数据

它仍然遵循互联网数据通信的技术规范。暗网恐怖主义问题在很大程度上也就是技术问题。有研究认为，国家有关部门需牢牢把握技术根本，组织国内重点网络安全研究所，展开暗网治理技术专项工程攻关研究，尽快形成适应中国网络空间治理需求的暗网管控技术能力[①]。治理暗网恐怖主义的技术路径主要在于减少暗网通信的匿名性，如：①识别互联网中的暗网络节点，特别是中继节点、目录节点、出入口节点等；②解析暗网节点上的数据流量，绘制暗网结构图；③遍历暗网网站资源，建立暗网资源数据库。④改进互联网结构，使运行其上的暗网更易于识别，等等。

4.2 社会舆论方面

“暗网”一词出现在公众视野中时，被渲染神秘、惊悚的色彩。类似于《暗网：一个比你想象恐怖 100 倍的互联网世界》《暗网，一个千万不要沾上的网络，也不要试图访问的罪恶网络》的文章广为流传，这类文章都夸大暗网的功能和作用，吸引了更多人接触暗网。事实上，暗网因缺乏身份验证、信任机制，任何人都可以在其中发布大量煽动、虚假、诈骗的内容。普通网民接受暗网上的煽动、虚假信息，或者有意或无意地将暗网上的内容带入明网，反而污染互联网舆论环境，甚至助长恐怖主义的发展。而加入暗网的用户节点本身也容易成为暗网数据包中转接力的工具，加大监管部门管控暗网恐怖主义的难度。因此，相关部门应加强宣传引导，充分揭示暗网的危险性质，减少暗网滋生发展的民众土壤。

4.3 执法监管方面

暗网作为一种匿名通信工具，既可以用于合法目的，也可以用于违法犯罪、恐怖主义等非法目的。美国执法部门摧毁 SilkRoad、AlphaBay 等大型暗网秘密市场后，一系列小型暗网交易网站也主动关闭，表明监管活动有助于遏制暗网非法活动的发展。同时也可以看出，虽然暗网具有匿名特点，但执法部门仍然可以对非法活动进行管控：

（1）监管暗网相关的线下活动。在暗网秘密交易中，物品的线下交付环节存在身份暴露的机会，线下暴露的信息又可以成为追查暗网活动的线索。在 SilkRoad 关闭前，美国邮政局检查员以及海关边境保卫局调查人员曾扣押至少 3000 个相关的可疑包裹[②]。为此，暗网用户开始使用“秘密传递点”（Deaddrops）的方式交付物品[③]，但其实仍然处于执法部门的密切监视之下。

（2）监管明网上谈论的暗网内容。有的暗网用户会将暗网内容转移到明网，或者将暗网的网址发布在明网上。例如，Telegram 是“伊斯兰国”支持者常用的信息共享和发布平台，其中包括暗网信息资源；Reddit、Pastebin、推特则是挖掘暗网资源地址的重要渠道[④]。此外，其

① 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):88-93.

② Wired. How the Feds Took Down the Silk Road Drug Wonderland[EB/OL].(2013-11-18).https://www.wired.com/2013/11/silk-road/.

Aldridge J, Askew R, Delivery dilemmas. How Drug Cryptomarket Users Identify and Seek to Reduce their Risk of Detection by Law Enforcement[J]. International Journal of Drug Policy, 2017, Vol.41:101-109.

④郭晗 , 王轶骏 , 薛质 . 基于 Freenet 的暗网空间资源探测 [J]. 通信技术 ,2017,50(09):2017-2023.

万方数据

他明网平台上也可能出现暗网相关的信息。执法部门可以收集这些信息，从而追踪暗网非法活动，并且及时阻止暗网内容流入明网产生社会影响。

（3）使用暗网，收集情报，引诱潜在的违法犯罪人员。执法部门、军队、情报机构也是暗网的主要用户之一[①]，其中，执法部门通常使用暗网实施在线监控、诱捕违法者、联系秘密线人[②]。此外，通过新的网络技术、政企联合行动等措施，执法部门可以追踪暗网上的非法内容、切断暗网链路等。

4.4 国际合作方面

暗网具有跨地域范围的性质，只有同时控制住跨地域的多个节点，才能准确追踪暗网非法活动。建立高效的国际合作机制，有助于获取和分享情报信息，提高联合行动效率，极大地促进打击暗网恐怖主义活动。在打击 Hansa 暗网秘密市场的联合行动中，美国联邦调查局、美国毒品管理局、荷兰国家警察局在欧洲刑警组织的支持下，最终在德国逮捕了 Hansa 网站的管理员，在荷兰、德国和立陶宛查封网站服务器。而查封服务器上获得的订单信息又被分发给 37 国执法情报部门，以便进一步调查暗网活动[③]。在这个案例中，多国执法部门、私企、外事部门、国际组织之间的国际合作至关重要。

网络恐怖主义也是国际公共威胁。中国在制定完善网络安全、反恐怖主义法制的基础上，可充分发挥上海合作组织以及其他双边、多边执法安全合作框架的作用，建立打击网络恐怖主义的国际合作机制，应对暗网环境下网络恐怖主义的新威胁。

附件

1、维基百科关于暗网的定义

暗网络（Darknet）是指一种使用互联网的上层网络（overlaynetwork），但需要特定软件、设置或授权才可接入。它包括：①小众型暗网络，如 f2f、p2p 网络；②大众型暗网络，如 Tor、Freenet、I2P、Riffle 等。

明网络（Clearnet）是指未隐秘、非暗网、非 Tor 的互联网。

暗网（Darkweb）是指存在于暗网络上的万维网（WorldWideWeb）内容。

深层网（DeepWeb），又称不可见网、隐藏网，是指未被标准 Web 搜索引擎建立索引的万维网（WWW）内容。

表层网（Surfaceweb），又称可见网、可索引网，是指便于普通公众访问并且可被标准 Web 搜索引擎搜索的万维网（WWW）内容。

2、一些暗网平台

（1）Tor（https://www.torproject.org）

Tor 网络由一组自愿运营的服务器组成。Tor 用户通过一系列虚拟通道连接，组织和个人在

① Congressional Research Service, Kristin Finklea. Dark Web[EB/OL].(2017-03-10) . https://fas.org/sgp/crs/misc/R44101.pdf.

② Michael Chertoff and Tobby Simon. The Impact of the Dark Web on Internet Governance ad Cyber Security[EB/OL]. https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

③ Europol. Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation[EB/OL].(2017-07-20).https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

万方数据

公共网络上分享信息时不会暴露其隐私。

Tor 软件用于接入和研究 Tor 网络，包括 Tor、Tor 浏览器、Nyx、MetricsPortal 等。个人可使用 Tor 软件访问普通网站，网站无法追踪到此人的真实地址；同时，个人还可以使用 Tor 软件的“洋葱服务”（onionservices）发布自己的 web 站点或其他服务，而不用公开其站点的位置。

TorProjectinc. 建立于 2006 年，是位于美国马塞诸塞州的一家非营利组织，负责开发和维护一系列 Tor 软件。海军研究实验室、电子前沿基金会是该组织的早期出资人，近年来，国家科学基金会、人权观察、出版自由基金会、谷歌公司、美国国务院等都曾向其提供资助。

Tor 的用途：记者可以使用 Tor 与爆料人或异见人士进行安全的联络。美国海军某部门使用 Tor 进行开源情报收集，其中一支小队在被派往中东后使用了 Tor。执法部门使用 Tor 访问、监测网站，而不会暴露政府所属的 ip 地址，或者保证诱捕行动时的安全。

（2）Freenet（https://freenetproject.org）

Freenet 是一个可绕过审查进行通信和发布信息的 p2p 平台，与其他暗网平台相比，其显著特点是去中心化。用户需贡献出自己电脑上的部分硬盘空间作为“分布式数据存储”，用以保存和传递网络上流转的加密文件片段。Freenet 平台上有一系列第三方开发的程序或插件，可实现在“分布式数据存储”上建立网站、聊天论坛以及搜索文件等功能。

在 0.7 版本后，Freenet 支持“暗网”（darknet）和“明网”（opnennet）两种连接方式。“明网”模式是指所有开启明网模式的节点将自动连接。“暗网”模式是指仅仅在相互认识和信任的用户之间手动连接。

伊恩·克拉克（IanClarke）是 Freenet 的创始人和 Freenet Project Inc. 协调人。DuckDuckGo、Web Hosting Search、谷歌公司以及 JohnPozadzdes、JohnGilmore 等个人为其提供资助。Freenet 的文化强调信息自由流动和言论自由的重要性。

（3）I2P（http://www.i2pproject.net/en/）

I2P 即“不可见互联网项目”（Invisible Internet Project），项目团队由一些分布在世界各地的匿名人士组成。2003 年项目组推出 I2P 软件测试版，取得初步成功，如今该软件已经更新至 0.9.37 版。

每个 I2P 客户端同时都是一个路由器。这些 I2P 路由器以“大蒜路由”方式组成匿名网络，在该网络上所有的通信都是端到端加密的。

I2P 网络上可以运行许多应用程序，目前可用的 I2P 程序如 I2PTunnel、SAM、BOB、BitTorrent、I2P-Messenger、Susimail、Syndie 等，可实现 E-mail、Web 浏览器、博客和论坛、匿名建站、实时聊天、去中心化存储等功能。

I2P 用户可以使用 I2PTunnel 程序建立匿名网站（eepsite），网址以 .i2p 结尾，如 ugha.i2p、forum.i2p 等。任何运行了 I2PTunnelHTTP 代理的用户通过普通浏览器就可以访问此类网站。

（4）Telegram（https://telegram.org）

Telegram 是由 TelegramMessenger 公司于 2013 年推出的即时消息软件，主要运行在手机端。该软件默认使用客户端到服务端 / 服务端到

万方数据

客户端加密的“云聊天”模式，但也可以启动客户端到客户端加密的“秘密聊天”模式。在“秘密聊天”模式中，只有双方同时开启“秘密聊天”功能才可以访问传输的加密消息。并且发送过的消息可以远程删除和定时自毁。

（5）FireChat（https://www.opengarden.com/firechat/）

FireChat 是由 OpenGarden 开发的一款手机即时消息软件，于 2014 年首次推出。该软件无需接入互联网，仅仅通过 p2p 蓝牙或 WiFi 连接，就可以在运行 FireChat 的手机设备之间传送消息。此外，每台手机设备相互接力，可以在一定范围内组建协作网络。2015 年 FireChat 宣布使用端到端加密保护消息。当外界网络被切断时，FireChat 可被用于社区组织、应急响应等。在一些抗议活动中，参与者也可能使用 FireChat 联络，避免电信和互联网上的监测。

3、一些暗网网站

（1）Tor 平台

http://darkdirmpmoq3uur.onion

http://zlal32teyptf4tvi.onion

http://msydqjihosw2fsu3.onion

http://grams72tru2gdpl2.onion

http://xmh5752oemp2sztk.onion

http://hss3uro2hsxfogfq.onion

http://sinbad66644fr5lq.onion

（2）I2P 平台

http://direct.i2p

http://0thers.i2p

http://btdigg.i2p

http://echelon.i2p/

http://abhishek.i2p

http://identiguy.i2p

http://diftracker.i2p/

http://closedshop.i2p

http://cokeandcoffee.i2p

http://themarketplace.i2p

http://darkhardwarelab.i2p

http://tracker2.postman.i2p/

（3）Freenet 平台

Enzo Index：http://localhost:8888/freenet:USK@XJZAi25dd5y7lrxE3cHMmM-xZ-c-hlPpKLYeLC0YG5I,8XTbR1bd9RBXlX6j-OZNednsJ8Cl6EAeBBebC3jtMFU,AQACAAE/index/711/

YAFI：http://localhost:8888/freenet:USK@yET8IzHqEXMLhzIJuIl1aO7aXx0tPEzh4JldQXx5las,xc1XLpeP9QiE1br5En~HcfwraeugGEwEc5TBKTjkjgE,AQACAAE/YAFI/3/

Freenet Message System：http://localhost:8888/USK@0npnMrqZNKRCRoGojZV93UNHCMN-6UU3rRSAmP6jNLE,~BG-edFtdCC1cSH4O3BWdeIYa8Sw5DfySV-TKdO5ec,AQACAAE/fms/147/

Sone (Social Chat)：http://localhost:8888/USK@nwa8lHa271k2QvJ8aa0Ov7IHAV-DFOCFgmDt3X6BpCI,DuQSUZiI~agF8c-6tjsFFGuZ8eICrzWCILB60nT8KKo,AQACAAE/sone/76/

TV Episodes：http://localhost:8888/freenet:USK@E5W70UxbeLAguZTR2t936phv4EWQoaqn7-WZOLqXFsk,pv2wNA~8BVNPuGgPX2LbesXss2rwsrGgvuLCU57uHgE,AQACAAE/tvtorrents/1192/

万方数据

参考文献

[1] 郭晗，王轶骏，薛质．基于 Freenet 的暗网空间资源探测 [J]. 通信技术，2017,50(09):2017–2023.

[2] 郎平．网络恐怖主义的界定、解读与应对 [J]. 信息安全研究，2016(10):882–887.

[3] 柳思思．“伊斯兰国”的互联网攻势及其影响 [J]. 现代国际关系，2016(02):32–39.

[4] 马国春，曹君．网络恐怖主义中的“伊斯兰国”[J]. 上海公安高等专科学校学报，2015(03):90–96.

[5] 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):88–93.

[6] 唐岚．网络恐怖主义面面观 [J]. 国际资料信息，2003(07):1–7.

[7] 万婧．“伊斯兰国”的宣传 [J]. 新闻与传播研究，2015(10):96–110.

[8] 王琳，杜雪．暗网项目：美国网络反恐情报研究的典范 [C].2017 3rd International Conference on Humanity and Social Science（ICHSS 2017), 2017–12–24.

[9] 杨溢，郭晗，王轶骏等．基于 Tor 的暗网空间资源探测 [J]. 通信技术，2017,50(10):2304–2309.

[10] 佘硕，刘旭．网络恐怖主义新动向及其治理分析 [J]. 情报杂志，2018(02):37–44.

[11] 联合国安全理事会．第 2129（2013）号决 议 [EB/OL].（2013–12–17）.http://www.un.org/zh/documents/view_doc.asp?symbol=S/RES/2129(2013).

[12] 中国人大网．中华人民共和国反恐怖主义法 [EB/OL].(2018–06–12).http://www.npc.gov.cn/npc/xinwen/2018–06/12/content_2055871.htm.

[13] 中国人大网．中华人民共和国网络安全法 [EB/OL].(2016–11–07).http://www.npc.gov.cn/npc/xinwen/2016–11/07/content_2001605.htm.

[14] 中共中央网络安全和信息化委员会办公室中华人民共和国国家互联网信息办公室．网络空间国际合作战略 [EB/OL].(2017–03–01).http://www.cac.gov.cn/2017–03/01/c_1120552617.htm.

[15]Aldridge J, Askew R, Delivery dilemmas. How Drug Cryptomarket Users Identify and Seek to Reduce Their Risk of Detection by Llaw Enforcement[J].International Journal of Drug Policy, 2017, Vol.41:101–109.

[16]Gabriel Weimann. Terrorist Migration to the Dark Web[J]. Perspectives on Terrorism, 2016(03):40–44.

[17]ITU. Measuring the Information Society Report[EB/OL].https://www.itu.int/en/ITU–D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf.

[18]Tor Metrics.Analysis[EB/OL].https://metrics.torproject.org/userstats–relay–country.html.

[19]The Verge. Dark Web Drug Marketplace AlphaBay was Shut Down by Law Enforcement [EB/OL].(2017–07–14).https://www.theverge.com/2017/7/14/15975140/alphabay–dark–web–drug–marketplace–police–shutdown–silk–road.

[20]Michael Chertoff, Tobby Simon. The Impact of the Dark Web on Internet Governance ad Cyber

万方数据

Security[EB/OL].https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

[21]Krypt3ia. The First Official Da’esh DARKNET Bulletin Board Has Arrived[EB/OL].(2015-11-15).https://krypt3ia.wordpress.com/2015/11/15/the-first-official-daesh-darknet-bulletin-board-has-arrived/.

[22]Krypt3ia. Two More Da’eshbag Darknet Sites Popped Up[EB/OL].(2016-04-29).https://krypt3ia.wordpress.com/2016/04/.

[23]Congressional Research Service, Kristin Finklea. Dark Web[EB/OL].(2017-03-10).https://fas.org/sgp/crs/misc/R44101.pdf.

[24]Wired.Why Facebook Just Launched Its Own 'Dark Web' Site[EB/OL].(2014-10-31).https://www.wired.com/2014/10/facebook-tor-dark-site/.

[26]Wired. Several Cyber Security to Protect your Account in the Social[EB/OL].(2015-11-19).https://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf.

[27]Wired. Security Manual Reveals the Opsec Advice Isis Gives Recruits[EB/OL].(2015-11-19).https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.

[28]Wired. Not Just Silk Road 2: Feds Seize Two Other Drug Markets and Counting[EB/OL].(2014-11-06).https://www.wired.com/2014/11/dark-web-seizures/.

[29]Wired. How the Feds Took Down the Silk Road Drug Wonderland[EB/OL].(2013-11-18).https://www.wired.com/2013/11/silk-road/.

[30]The Guardian. FBI Claims Largest Bitcoin Seizure after Arrest of Alleged Silk Road founder[EB/OL].(2013-10-02).https://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin.

[31]Europol. Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation[EB/OL].(2017-07-20).https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[32]Quartz.A Million People Now Access Facebook on the "dark web" Every Month[EB/OL].(2016-04-22).https://qz.com/667880/a-million-people-now-access-facebook-on-the-dark-web-every-month/.

[33]FBI. Ulbricht Criminal Complaint[EB/OL].https://assets.documentcloud.org/documents/801103/172770276-ulbricht-criminal-complaint.pdf.

[34]GiacomoPersi Paoli. The Trade in Small Arms and Light Weapons on the Dark Web: A Study[EB/OL].(2018-10-22）.https://www.un.org/disarmament/update/the-trade-in-salw-on-dark-web/.

[35]AndreasWimmer. Darknet, Social Media nad Extremism: Addressing Indonesian Counterterrorism on the Internet[EB/OL].(2015).https://www.academia.edu/20813843/Darknet_

万方数据

Social_Media_nad_Extremism_Addressing_Indonesian_Counterterrorism_on_the_Internet.

[36]Business Insider. Supporter Of Extremist Group ISIS Explains How Bitcoin Could Be Used To Fund Jihad[EB/OL].(2014-07-08).https://www.businessinsider.com/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7.

[37]BeatriceBerton. The Dark Side of the Web: ISIL's One-stop Shop?[EB/OL].2015-06）https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf.

[38]FBO. DARPA-BAA-14-21: Memex[EB/OL].(2014-02-04).https://www.fbo.gov/index?s=opportunity&mode=form&id=426485bc9531aaccba1b01ea6d4316ee&tab=core&_cview=0.

[39]DARPA. Memex[EB/OL].https://www.darpa.mil/program/memex.

[40]Michael Chertoff,Tobby Simon.The Impact of the Dark Web on Internet Governance ad Cyber Security[EB/OL].https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

[41]Congressional Research Service, Kristin Finklea. Dark Web[EB/OL].(2017-03-10).https://fas.org/sgp/crs/misc/R44101.pdf.

作者简介

黄紫斐，上海外国语大学国际关系与公共事务学院 2017 级博士研究生，研究方向为公共安全、国际关系。

刘洪梅，中国信息安全测评中心副研究员，研究方向为信息安全态势与战略研究。

张舒，中国信息安全测评中心副研究员，研究方向为信息安全态势与战略研究。

Cyber Terrorism and its Governance based on Darknet Environment

HUANG Zi-fei[1], LIU Hong-mei[2], ZHANG Shu[2]

（1.Shanghai International Studies University, School of International Relations and Public Affairs, Shanghai 2000083,China；2. China Information Technology Security Evaluation Center, Beijing 100085,China）

[Abstract] The use of the Internet by terrorist organizations and their supporters as a means of information dissemination has become the norm of cyber terrorism. As the international fight against terrorism has intensified, cyber terrorism has turned to the Darknet environment, posing new risks to the international community and national security. In this regard, we should enhance the governance capacity of Darknet terrorism from four aspects, namely, network technology, public opinion, law enforcement and supervision, and international cooperation, so as to cope with the new threat of cyber terrorism.

[Keywords] Darknet; Cyberterrorism; Cyber Communication; Cyberspace Governance

万方数据