“伊斯兰国”的暗网攻势及其应对路径

肖 洋
(北京第二外国语学院国际关系学院,北京 100024)

摘 要: 近年来,各国互联网反恐的力度不断加大,暗网成为“伊斯兰国”招募与筹资的避风港。随着熟稔互联网的恐怖分子进入暗网,将引发一场国际联合打击恐怖主义的持久战争。“伊斯兰国”的互联网营销以暗网为平台,借助新媒体工具进行网络动员与网络扩散,里应外合共同制造恐怖案件。恐怖分子利用暗网进行资金转移、内部联系、人员招募、自我宣传、恐怖主义串联等活动,使得各国政府的反恐政策与安全服务面临巨大挑战。“伊斯兰国”的“暗网”转向,是恐怖主义活动蔓延与互联网技术推广相结合的新产物。暗网反恐将成为国际反恐斗争新前线,各国需要构建网络安全综合政策体系以打击暗网恐怖主义。

关键词: “伊斯兰国”; 暗网; 恐怖主义; 比特币
中图分类号:D815.5 文献标识码:A 文章编号:1673-1026(2017)01-0019-06
DOI:10.16147/j.cnki.32-1569/c.2017.01.005

近年来,国际恐怖组织趋向于积极利用互联网开展活动,包括发布信息、自我宣传、筹集资金、招募人员、秘密联络、非法交易等,其借助互联网和新媒体进行跨国动员的趋势,促使各国反恐战略的工作重心从“应急处置”向“反恐预警”转移。2015 年的巴黎暴恐案反映出国际恐怖组织的互联网攻势对各国首都安保工作的巨大威胁,而“伊斯兰国”恐怖分子之间使用暗网加密科技进行暴恐策划与交流,使之在互联网空间能够躲避各国政府的追踪、定位与抓捕。最新互联网安全研究发现,暗网将成为伊斯兰国恐怖分子的避风港。鉴此,本文在解析暗网概念与基本架构的基础上,深入剖析“伊斯兰国”等国际恐怖组织如何利用暗网进行动员活动,成为当前恐怖主义研究的重要议题。

一、暗网的概念与内涵

互联网是一个多层结构 “表层网”(Surface Layers)又称“明网”,指的是通过超链接就可以被常规搜索引擎搜索到的页面集合。“底层网”(Deeper Layers)又称“暗网”,指的是无法被谷歌等常规搜索引擎检索到的、需要严格注册才能浏览的结构化数据集合。[1] 底层网的最底部,包含了故意隐瞒的内容,需要通过动态请求方可进入,并需要借助“洋葱路由”(The Onion Router,TOR)等特定搜寻器才可找到。暗网具有链接简便、高匿名性、金钱交易便捷、意识形态混杂等特点。暗网的体量比明网大得多,明网的数据量只占整个互联网空间的 4%,暗网则占 96%,约 8ZB(1ZB=1 亿 TB)。[2]

暗网并非单一的形态,而是分为三种基本类型。一是 I2P(Invisible Internet Project)匿名网络,采取的是封包交换的方式以实现安全、匿名地聊天与传输文档。二是以“洋葱路由”为代表的 P2P 匿名网络,采取分布式技术,让每个用户的计算机都成为加密的中继连接,用户在访问暗网时,不会留下完整的链接痕迹。三是以 FIRECHAT 为代表的自组织匿名网络。每个节点通过特定的自组织协调机制,以适应包括无线网在内的各种网络条件下的网络通信任务。当前,个人需要使用 TOR 或 I2P 等特殊软件才能进入暗网。在暗网中,一个访问者必须知道在哪里能找到可访问的网站。尽管有少数搜索引擎能够访问暗网,但它们在范围与使用效

收稿日期: 2016-08-26; 收修改稿日期: 2016-11-11
基金项目: 本文系北京市社会科学基金项目“互联网时代国际恐怖组织攻击首都城市的策略及北京应对路径研究”(项目编号: 16ZGC015)、北京市优秀人才培养资助青年拔尖个人项目(项目编号: 2016000026833ZS06)的阶段性成果。
作者简介: 肖 洋(1981-),男,湖南长沙人,北京第二外国语学院国际关系学院副教授、国际问题研究中心主任,博士,研究方向: 网络恐怖主义与国际危机预警。

果方面都极其有限。

“绝对隐形”是暗网的核心特点，这包括网站隐形、用户身份隐形、IP 地址隐形等。因此，暗网通常用来保护数据安全，在军、商两界广泛使用。在军事通信领域，能够有效防止敌方的数据追踪，能够提升军事通信安全。在电子商务领域，既能保护商业信息，同时也可通过建立加密通道来保护云服务使用者的个人隐私。

美军是暗网的最大资助方。以使用最广的 TOR 软件为例，TOR 最初是美国海军研究实验室（U.S. Naval Research Laboratory）研发的一款匿名网上搜索工具。这依赖于一个志愿计算机网络（Network of Volunteer Computers）通过一系列其他用户的计算机来更改某些用户的网络路由，能够有效防止流量分析与监听，从而保护使用者的隐私。虽然并非所有的暗网都使用 TOR 与 ONION 地址，但所有启用 TOR 的浏览器能够访问任何网站而不会泄露访问者的信息，也正因为如此，TOR 面临被犯罪分子滥用、情报机构监控的风险。如今，TOR 在互联网中的中继节点为 4000 个，大多位于美、德、法等国，日常用户已过百万，因此被称为“暗网之基”。为了控制这一新兴的网络阵地，其运作资金的 60%仍来自美国政府。

二、恐怖分子对暗网的利用

一般而言，恐怖分子在暗网的活动，都被描述为“与在表层网的活动相似，只是更加隐秘而已”。然而，这只说对了一半。恐怖分子虽然使用了几十年的表层网，但暗网为他们提供了新的互联网生存机遇。在 WEB3.0 时代，恐怖分子常常在表层网发布招募信息、激进宣传信息、募资信息、开展恐怖袭击的协调信息等。然而，在各国政府加强互联网监管的背景下，恐怖分子所有这些活动都开始转入互联网的更深层面。例如恐怖分子的宣传材料，已经存储在了暗网。由于暗网基本处于无人监管的状态，因此恐怖分子常常利用暗网的匿名性进行非法金融交易、内部联系、恐怖宣传、反政府串联等破坏活动。

（一）恐怖分子广泛利用虚拟货币进行资金转移

随着各国对现金出境和明网金融交易的监管日益严格，使得恐怖分子难以通过常规方式进行资金积累与转移，暗网的虚拟货币运行模式为恐怖分子打开了募资新渠道，使其能够将法定货币与虚拟货币在暗网中进行兑换与转移，甚至在影响力较大的论坛自助生产加密的货币，从而形成稳定的资金链。互联网虚拟货币分为集中型虚拟货币，即由单一实体管理运营的“网络货币”（Web Money）和“完美货币”（Perfect Money）；以及没有实体进行管理的分散型虚拟货币，如“比特币”（BitCoin）和“黑币”（Black Money），通过网络中分散的用户节点进行交易，汇款人与收款人的交易信息都被隐藏起来。当前暗网中使用量最大、美誉度最高的比特币被称为“暗网美元”，也最受恐怖分子青睐。如今，57%的暗网空间充斥着色情、非法融资、贩毒、武器交易、假币贩卖等非法信息。[3] 其中最臭名昭著的例子就是“丝路网”（Silk Road）利用暗网的隐匿用户身份，从事着上述所有的违法行为，“丝路网”在两年内就赚了价值 12 亿美元的比特币。2013 年 10 月，美国联邦调查局关闭了这家毒品贩卖网站，并逮捕了其幕后老板罗斯·乌布利希（Ross William Ulbricht）。然而，暗网的匿名性使得网络勾连、秘密交易更加难以监管，使之逐步成为“密买密卖”的金融黑市平台。

“伊斯兰国”恐怖分子能够使用暗网进行融资、转移财产和非法购买武器炸药、使用比特币等虚拟货币和其他加密货币。例如，“奋斗伊斯兰无痕基金”（Fund the Islamic Struggle without Leaving a Trace）是“伊斯兰国”将“圣战”募捐资金转化为比特币的深层网镜像，在网页中出现 PDF 的操作教程，标题为“比特币与暴力抗争的福音”（Bitcoin and the Charity of Violent Physical Struggle）①，这事实上是指导如何使用暗网进行秘密金融交易。例如，“伊斯兰国”进行巴黎暴恐案的武器就是通过暗网购买的，通过斯图加特检察官办公室（Stuttgart Prosecutor's Office）的官方文件，枪械贩卖方是德国暗网销售商“DW Guns”。[4] 一些报告研究发现，暗网已经成为恐怖分子出售人体器官（往往来自伊斯兰国的俘虏）、石油（盗窃而来）、古董（从古城洗劫而来）的在线黑市。[5]

2015 年 1 月，大本营在新加坡的网络情报公司 S2T 发现了确凿的证据，一个自称与“伊斯兰国”有关的美洲恐怖分子小组，将收集比特币作为募资方式。[6] 其在线募资的负责人阿布-穆斯塔法（Abu-Mustafa）声称“人们不可能将一家银行转移给‘圣战组织’，在异教徒政府统治下的圣战者应该意识到，一个可能的方式就是使用比特币进行匿

① 关于此教程的网页链接详见：https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf.

名捐助，这能够为‘圣战’提供价值数百万美元的比特币财富，每一个圣战者口袋里的每一分钱，都将化为支持圣战的不竭动力。”[7] 另一个例子来自于印度尼西亚的恐怖组织“伊斯兰祈祷团”(Jemaah Islamiyah)，无论是国内国外捐资者，都是通过在暗网的比特币交易平台对其进行资金捐赠。甚至，通过从暗网中盗取的身份信息，该组织攻击了一个外汇交易网站，募集了近百万美元。

(二) 恐怖分子利用暗网科技进行内部联系

如今，恐怖分子使用暗网进行交流，比以前任何时候都更加安全。虽然人们常常认为恐怖分子以秘密网络进行恐袭协调，但获得确凿的证据却在2013年8月，美国国家安全局(U. S. National Security Agency，NSA)破译了基地组织领导人Ayman Al-Zawahiri和基地组织也门分部领导人Nasir Al-Wuhaysi的加密通信。美国国家安全研究所(Institute for National Security Studies)揭示说：在十年里，全球范围的基地组织网络领导人之间的交流，已经转入到暗网之中。

如今，“伊斯兰国”和其他吉哈德组织主要使用Telegram等在线应用工具，这使得应用方通过加密移动电话可以向海量用户发送信息。自从2013年8月14日Telegram被创造出来就获得极大成功，不管是最初的使用者还是恐怖分子都对其予以一致好评。随着Telegram在2015年9月赶走了“Channels”后，“恐怖主义研究分析联盟”(Terrorism Research & Analysis Consortium)见证了大量的社交媒体如推特(Twitter)开始向Telegram转移。[8] 2015年9月26日，即Telegram击垮Channels的4天后，“伊斯兰国”在推特上开始宣传自己的官方频道“发布者”(Nashir)。最近，国际反恐中心(International Center for Counter-Terrorism)关于Telegram的特别报告揭示说“自从2015年9月至今，我们发现伊斯兰国和基地组织大幅使用Telegram软件(可即时发送匿名信息)。仅2016年3月一个月，‘伊斯兰国’就开放了700个新频道。”[9]

另一个被“伊斯兰国”恐怖分子使用的安全通信应用程序是TrueCrypt。2015年8月，一名被法国警方逮捕的“伊斯兰国”成员供述了这一程序的相关细节。Reda Hame是一位巴基斯坦IT专家，他在叙利亚加入“伊斯兰国”，在接受了短暂培训之后赴法国准备实施爆炸活动。Hame供述了他被培训使用TrueCrypt的细节。TrueCrypt是一款加密软件，在Hame准备返回法国之前，被给了一个存有TrueCrypt驱动程序的U盘。“伊斯兰国”的软件工程师还告诉Hame一到达欧洲，就安装TrueCrypt软件以保持与“伊斯兰国”技术人员的联系。TrueCrypt出现于2004年，互联网罪犯Paul Le Roux曾在菲律宾的基地里，操作该程序进行全球贩毒、地下军火贸易、洗钱等犯罪活动。2012年9月，Paul Le Roux在利比亚进行毒品交易时被捕，但TrueCrypt仍然活跃，且后门进入免费(backdoor-free)，这就解释了为什么“伊斯兰国”恐怖分子仍然能使用它进行加密通信与文件共享。

(三) 暗网已经成为恐怖分子的重要宣传平台

从20世纪90年代起，恐怖分子就已经活跃在各大互联网在线平台。然而，表层网很难实现匿名化，恐怖分子很容易被监控、追踪并最终被找到，很多位于表层网的恐怖分子网站和社交媒体都被反恐部门密切监控，并且常常被关闭或入侵，因此在明网实施恐怖信息传送与串联的风险极大。例如“伊斯兰国”在表层网的一举一动都受到各国的密切关注，各国屏蔽或过滤极端主义内容，使得吉哈德主义者不得不寻找新的在线安全天堂。[10] 相反，在暗网，非聚集化(decentralized)和匿名性使得这些恐怖主义平台避免被锁定和关闭。通过伦敦服务器Quilliam Foundation，恐怖分子的宣传与招募材料会很快在网络上重现，这推动恐怖主义狂热分子利用暗网肆无忌惮地进行活动，丝毫不顾忌被政府部门抓获的风险。甚至，一些伊斯兰极端主义的英语和法语论坛与聊天室仍然被广大用户使用。如今，绝大多数的极端伊斯兰组织的推送信息都转移进了暗网。例如，由于“伊斯兰国”在表层网“#Caliphate_Publications”的活动受阻，任何新的域名刚被注册就被删除，因此在2015年11月15日，即巴黎爆炸案发生的两天后，“伊斯兰国”发布其进行互联网宣传与招募的重要阵地——官方网站Isdarat的暗网转移信息，并包含了一个“伊斯兰国”在洋葱网隐藏网址的链接，暗示着“伊斯兰国”开始全面转向暗网来推广信息和自我宣传，这显然是为了保护该组织拥护者的身份，同时避免其宣传内容被各国政府黑客攻击。

在巴黎暴恐案发生后，最大的政治黑客联盟“匿名者”(Anonymous)对数百个与“伊斯兰国”有关的网站进行了密集攻击。随后，“伊斯兰国”的宣传阵地就进行了这场大转移。“伊斯兰国”的媒体终端——哈耶特媒体中心(Al-Hayat Media Center)，已经列出了如何在暗网联系“伊斯兰国”的方法与镜像。这种地址变更的说明还用开放式源代码软件Telegram进行内部通报，该软件具有“阅后自毁”的特点，具有较高的反追踪能力，成为

“伊斯兰国”等恐怖组织在互联网隐身的绝佳工具。Telegram 能够在安卓、IOS 和 Windows 系统中传送文本与多媒体文件。此外，Telegram 的加密法极其复杂，且不会把网络通信的内容存储在服务器中，因此安全性颇高，甚至扬言对第一个能够破解其密码的人奖励 30 万美元。“伊斯兰国”通过在暗网的洋葱网地址加密服务来传递宣传材料，例如纪录片《战火》(Flames of War)。此外，网站中还包括联系“伊斯兰国”成员的通讯门户。巴黎暴恐案发生后不久，各国在线反恐监控就发现在 Telegram 上至少有 78 个伊斯兰群组，而 Telegram 公司拒绝与安全部门合作。因此，“伊斯兰国”仍然可以在明网和暗网进行游击战，对各国安全构成了极大威胁。

其他恐怖组织也都效仿“伊斯兰国”的暗网宣传。其中，包括阿拉伯半岛基地组织(Al-Qaeda in the Arabian Peninsula)、利比亚圣战组织(Ansar al-Sharia in Libya，ASL)、努斯拉阵线(Jabhat al-Nusra，JN)、伊斯兰军(Jaysh al-Islam)。基地组织也门分部(Al-Qaeda's Yemeni branch，AQAP)在 2015 年 9 月 25 日开通了自己的 Telegram 频道，第二天利比亚圣战组织也在 Telegram 开通了自己的频道，每一个频道的用户订阅量极其惊人。仅仅一周的时间，伊斯兰国 Telegram 频道的成员就从 5000 人上升为 1 万人。[8] 当被问及此事时，Telegram 的首席执行官帕维尔·杜罗夫(Pavel Durov)承认了“伊斯兰国”的确使用 Telegram 以确保其通信安全。但是随后又补充道“我认为与我们所重视的隐私权相比，那些令人恐惧的灾难，如恐怖主义更值得关注。”[11] 国际恐怖主义的在线图书馆设置“吉哈德维基”(Jihadwiki)，进行吉哈德主义宣传。

(四)利用暗网进行网络攻击成为恐怖分子反政府串联的重要途径

恐怖分子与持不同政见者、社会活动家和自由记者沆瀣一气，使用暗网进行非法信息传送和秘密结社，还采用匿名的 SMTP 软件发送大量宣传邮件，与政府部门争夺互联网舆论引导权。例如，在香港“占中”事件中，FireChat 软件一天之内被下载 10 万次，该软件呈现中心节点、网状链接的特点，在人口密集区可实现自行组网，实现大规模的信息推送，成为反政府组织开展群众动员与信息传播的工具。而这些反政府活动的幕后组织者，往往具有光鲜的身份，为了隐匿操纵政治运动的信息，这些幕后黑手开始使用加密功能强大的 Telegram 软件。2012 年 12 月，一些反政府黑客通过 TOR 匿名网络控制僵尸网络 Skynet，随后对多个政府网站发动攻击。2015 年 12 月，基地组织 al-Aqsa IT 团队发布“TOR 安全浏览指南”(Tor Browser Security Guidelines)手册，以确保在线匿名浏览者能够使用 TOR 软件。该指南详细教授网民从下载到安装浏览器的全过程，以及如何防范反恐部门的地理定位与身份确定。

三、暗网恐怖主义带来的挑战及其应对

越来越多的证据表明，暗网已经成为全球恐怖组织和跨国犯罪的主要平台。2016 年 3 月，法国内政部长贝尔纳·卡泽纳夫(Bernard Cazeneuve)在国民议会上声称“伊斯兰国”恐怖分子已经广泛使用了暗网，近期欧洲暴恐案负责的恐怖组织都使用了深层网，并通过加密信息进行联系。2016 年 4 月，美国总统奥巴马在华盛顿对来自 50 个国家的元首和外交部长致辞中，描述了恐怖组织如何在暗网上购买铀和钚等核材料，而恐怖分子通过无人机对平民区散播放射性物质，则是美国最大的反恐噩梦。尽管各国都加强对暗网搜索平台的监管，但成效并不明显，面临着来自技术和法律的双重挑战。

(一)暗网恐怖主义带来的挑战

一是暗网的开发者利用云服务运行多个网络互连的网桥，从而形成数以万计、可供恐怖分子藏匿的虚拟点，使得各国政府在暗网追踪恐怖分子更加困难。二是隐私保护成为暗网反恐的难解之题。暗网代表了部分网民匿名上网以保护隐私的合理需求，但这也使得恐怖分子能够大肆散布极端意识形态、进行犯罪交易。由于保护个人隐私在互联网治理立法过程中尚存在漏洞，各国也没就访问暗网的个人隐私保护问题提出明确的法律约束条款。三是暗网的接口隐蔽性高，恐怖分子经常变动信息发布地址，且采取“一对一”私聊的方式传播，文件下载常常通过具有暗网接入软件的 BT 和网盘等方式，使得反恐部门难以摸清上传者与使用者的身份。此外，智能手机移动终端的大幅增多，也使得暗网接入软件的使用更为频繁，提高了追踪成本。

由此看来，恐怖分子使用暗网为各国政府的反恐政策与安全服务带来新的挑战，这急需发展新的方法和标准来剖析恐怖分子使用暗网的举动。

(二)应对暗网恐怖主义的对策

笔者认为，可从以下三个方面进行思索。

第一，完善对暗网涉恐信息的监测科技。美国国防部高级研究项目局(American Defense Advanced Research Projects Agency)认为可以通过 MEMEX 软件找到恐怖组织隐匿在暗网的账号与交易平台，

该软件能够对深层网进行更好的编目。MEMEX 最初被用来监控暗网中的人口贩卖信息，但也可用于暗网中几乎所有的非法活动。2015 年 2 月，一篇名为《暗网对互联网治理的影响与网络安全》(The Impact of the Dark Web on Internet Governance and Cyber Security) 的特别报道提出了若干应对暗网犯罪的建议。[12] 2015 年 2 月，美国联邦调查局使用 NIT(网络调查技术) 的工具成功破解了 TOR 网站，NIT 是迄今为止最复杂的网络检测工具，能够破解 TOR 所提供的所有隐匿保护，一次可在暗网探索 1300 个真实 IP 地址，然后顺藤摸瓜地找到真实使用这些网址的人。不仅如此，用户电脑的操作系统与用户名、MAC 地址、主机名都能被捕获。这对打击恐怖组织的互联网营销起到非常大的作用。

第二，建立对暗网的规管措施。2015 年 2 月，美国成立“网络威胁情报整合中心”(Cyber Threat Intelligence Integration Center)，能够开展部际合作，集聚整合反恐数据，协调互联网反恐工作。2015 年 12 月 18 日，美国出台《网络安全法》，将“网络威胁指标”与“防御性指标”作为网络安全信息共享的范围，重点审查互联网的信息共享方式、组织机构、责任豁免、隐私保护规定等。2015 年 8 月 5 日，中国政府公布《中华人民共和国网络安全法(草案)》，规定网络产品和服务提供者不得设置恶意程序，明确赋予有关主管部门处置阻断违法信息传播的权力。2015 年 11 月 4 日，英国通过“调查权力法草案”(Draft Investigatory Powers Bill)，赋予警方和安全部门更大的网络调查权，并于 2015 年 2 月成立互联网反恐作战部队“77 旅”，专门打击“伊斯兰国”的网络恐怖主义。法国于 2015 年 3 月起实施《反恐情报监控法案》，赋予法国政府无需经过法律程序就可限令互联网供应商在 24 小时之内关闭涉恐网站。俄罗斯强制要求日均访问量超过 3000 人的网站必须向政府报备，且放弃匿名权，俄罗斯政府有权关闭全国网络。[13]

第三，加强国际互联网反恐合作。网络无国界与互联网科技有国界的现状，使得恐怖组织能够借助互联网技术精英实施跨国攻击。因此，打击国际恐怖组织在暗网的活动，不仅要增强国内的科技力量，更要推动国际合作，尤其是与那些具有网络科技优势的国家进行情报合作与沟通。在互联网反恐的技术支撑、情报分享与司法管辖问题上，发达国家与发展中国家都应发挥积极作用，推动高透明度、多边参与的互联网治理机制，加快制定互联网行为准则，优化暗网反恐的国际环境。

综上所述，如今“伊斯兰国”的互联网营销以暗网为平台，借助新媒体工具进行网络动员与网络扩散，里应外合共同制造恐怖案件。可以说，“伊斯兰国”的暗网转向，是恐怖主义活动蔓延与互联网技术推广相结合的新产物。为了构建网络安全综合政策体系，就需要去洞悉互联网发展的最新进展——暗网。虽然暗网相对于表层网来说缺乏广泛的应用人群，但其隐藏的网络生态系统有利于宣传、招募、融资和计划，并为犯罪分子所喜爱，这是因为，暗网本身就是一个不受监管的空间。

参考文献：

[1] 赵兵，郭才正.深网和搜索引擎[J].情报探索，2016(1)：90.

[2] 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.

[3] Daniel Moore，Thomas Rid. Cryptopolitik and the Darknet[J]. Survival Global Politics & Strategy，2016，58(1)：7-38.

[4] Germany arrests man reportedly suspected of selling guns to Paris attackers[N/OL].2015-11-27[2016-07-26] http://www.foxnews.com/world/2015/11/27/germany-arrests-man-reportedly-suspected-selling-guns-to-paris-attackers.html.

[5] Andreas Wimmer，Aulia Nastiti. Darknet，Social Media，and Extremism：Addressing Indonesian Counterterrorism on the Internet[J]. Deutsches Asienforschungszentrum Asian Series Commentaries，2015，30.

[6] Danna Harman. U.S.-based ISIS Cell Fundraising on the Dark Web，New Evidence Suggests[N]. Haaretz，2015-01-29.

[7] Supporter of Extremist Group ISIS Explains How Bitcoin Could Be Used To Fund Jihad[N/OL].2014-07-08[2016-07-12] http://www.businessinsider.com/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7.

[8] Terrorism Research & Analysis Consortium. Massive Terrorist Migration to Telegram，the new Jihadist Destination[EB/OL].2015-11-03[2016-07-12] http://fitnaphobia.com/2015/11/massive-terrorist-migration-to-telegram-the-new-jihadist-social-media-destination/.

[9] Michael Barak. The Telegram Chat Software as an Arena of Activity to Encourage the “Lone Wolf” Phenomenon[EB/OL].2016-05-24[2016-06-20] https://www.ict.org.il/Article/1673/the-telegram-chat-software-as-an-arena-of-activity-to-encourage-the-lone-wolf-phenomenon.

(下转第 37 页)

[18] Tajikistan Brushes Off Talk of Islamic State at the Border [N/OL].2015-11-06 [2016-06-20] http://www.eurasianet.org/node/75956.
[19] Tajiks Increasingly Turning To Shari'a To Resolve Disputes, Family Affairs [N/OL].2010-09-14 [2016-6-20] http://www.eurasianet.org/node/61914.
[20] 文丰.十字路口上的塔吉克斯坦:世俗化还是伊斯兰化[J].新疆师范大学学报,2011(6).
[21] Remittance flows from Russia to Tajikistan reportedly declined 65.1% [N/OL].2015-12-18 [2015-12-22] http://www.asiaplus.tj/en/news/remittance-flows-russia-tajikistan-reportedly-decline-651.
[22] Tajikistan: Fashion at Heart of Anti-Islamic Culture War [N/OL].2016-4-11 [2016-06-20] http://www.eurasianet.org/node/78241.
[23] As Tajikistan Limits Islam, Does It Risk Destabilization? [N/OL].2015-12-01 [2016-06-20],http://www.eurasianet.org/node/76361.
[24] 约翰·埃斯波西托,达丽亚·莫格海德.谁为伊斯兰讲话?——十几亿穆斯林的真实想法[M].晏琼英,王宇洁,李维建,译.北京:中国社会科学出版社,2010:221.

On the Countermeasures of Tajikistan to Religious Extremism

ZHANG Wei-wei
(School of Marxism, Chinese Academy of Social Sciences, Beijing 102488, China)

Abstract: The religious extremism activities in Tajikistan takes on features like plural subjects, internationalized modes and intensified threats. And Tajikistan has taken multiplied countermeasures including strict law enforcement, strengthened governance of religious affairs and social life and expanded international cooperation. However, the severe social-economic problems and side effect of policies have restricted the results. The counter measures have failed to restrain the expansion of religious extremism in the country.

Key words: Tajikistan; Extremism; Countermeasures

责任编辑:陈丙纯

(上接第23页)

[10] Ghaffar Hussain, Erin Marie Saltman. Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter It [R]. Quilliam, May 2014.
[11] Sarah Kaplan. Founder of app used by ISIS once said 'We shouldn't feel guilty.' On Wednesday he banned their accounts. [N]. Washington Post, 2015-11-19.
[12] Michael Chertoff, Tobby Simon. The Impact of the Dark Web on Internet Governance and Cyber Security [R]. Global Commission on Internet Governance, Paper Series: No.6. February 2015.
[13] 赵志云,张旭,等."暗网"应用情况及监管方法研究[J].知识管理论坛,2016(2):126-127.

ISIS's Dark Web Offensive and the Preventive Solution Concerned

XIAO Yang
(School of International Relations, Beijing International Studies University, Beijing 100024, China)

Abstract: With intensified anti-terrorism efforts online among countries, the deep web has become the haven for ISIS' recruitment and financing. The emergence of Internet-savvy terrorist in the deep web will bring a lasting war against terrorism. ISIS takes the deep web as a platform for marketing and the new media as a tool to attract members, spread terrorism and launch activities. The counter-terrorist policies and security service of governments are facing big challenges since terrorists are using deep web for capital transfer, internal relation, recruitment, self-promoting, terrorist-corporation, etc. ISIS' new strategy in the web is the production of the combination between terrorism and Internet technology, which makes deep web a new front for international anti-terrorism. It is imperative for countries to establish an integrated policy system of cyber security.

Key words: ISIS; Dark Web; Terrorism; Bitcoin

责任编辑:陈丙纯