责任编辑:陈烽 邮箱:179652384@qq.com

极端组织“伊斯兰国”(IS)经常使用社交网站、手机应用、电子杂志等互联网手段宣传极端思想,招募成员。在推特等微博客和各种网络论坛中散发文字、图片、视频,不少内容颇具煽动性。针对IS的网络宣传,各国都采取了哪些行动?

欧美打响反IS网络战

2015年1月12日,美国中央司令部推特账户遭到IS袭击

IS每天发9万条信息

IS每天在网络上释放约9万条消息。他们熟练利用社交媒体散播消息招募成员,再转入加密的社交通信软件信息进一步沟通。

IS不仅针对平民发动恐怖袭击,在网络上,他们也频繁向欧美国家机关、大型科技公司发动黑客袭击,并通过网络进行宣传和招募。

今年1月,IS支持者入侵了美国中央司令部的YouTube和推特账户,窃取了大量内部文件并泄露到了网上。IS控制美国中央司令部推特账户长达1个小时,并把美国中央司令部的logo换成了“I love you ISIS”。

3月,IS支持者向推特创始人发出死亡威胁,称将追杀所有推特员工,威胁说“你们针对我们的虚拟战争将会带来一场真正的战争。”在发送给推特创始人杰克·多西的帖子中,还附了一张多西被枪瞄准的合成图片。

4月,法国电视台5台遭到来自IS拥护者、黑客组织Cyber Caliphate的大规模网络攻击。攻击者因不满法国总统奥朗德参加国际反恐行动,入侵了电视台的广播传输渠道。

IS发起的类似网络攻击不胜枚举。实际上,IS迅速崛起与其对网络空间的娴熟利用分不开。IS在网络空间进行大规模宣传、招募,利用网络进行加密通信、策划袭击活动。他们对网络科技的利用已经达到了“专业”水平,要打击IS,网络反恐越来越成为不可忽视的一部分。

2015年出版的反恐书籍《耶稣和圣战者:回应ISIS的愤怒》中披露,IS每天在网络上释放约9万条消息。他们熟练利用社交媒体散播消息招募成员,再转入加密的社交通信软件信息进一步沟通,通过分享网站存储数据,并利用在线文本编辑平台编辑恐怖袭击实时战况。恐怖分子甚至开发了App。

据美国媒体报道,他们还发现IS有一本34页的网络操作安全手册,如教材一般发放给成员学习。美国西点军校反恐中心的研究人员亚伦·布兰特利从IS的论坛和聊天室里发现了这本手册,其原件为阿拉伯文写就。

该手册为IS成员之间的互相通信和策划袭击活动提供了简便易行的指导。比如如何保持通信和定位数据的安全,它还给出了几十个安全应用和服务的链接。

美国整合力量网上反恐

今年2月,英国军方决定建立关于社交媒体的特殊作战部队,又称“77旅”,以应对日益猖獗的IS网络恐怖主义。

随着恐怖分子对网络技术的运用,网络反恐提上议程。

早在2001年9·11恐怖袭击之后,时任总统小布什及其政府便以反恐需要为由,允许NSA(美国国家安全局)在未经特别法庭许可的情况下,对美国境内居民在国际间进行的通信进行窃听。

网络科技的发展令美方认识到,很多在常规军事力量上无法与美国抗衡的敌人,可以派遣手段高超的黑客摧毁美国的金融系统、通信系统和水电基础设施。美方认为,开展此类袭击的成本远远低于建造一架第五代战斗机。五角大楼因此开始大力发展自己的网络攻击能力,并将其应用到实战之中。

2002年12月,美国海军率先成立海军网络司令部,随后空军和陆军也相继组建自己的网络部队。2010年5月,美军建立网络司令部,统一协调保障美军网络战、网络安全等与电脑网络有关的军事行动,其司令部设在华盛顿附近的马里兰州米德堡军事基地,网战部队人数约8.8万人。

美国网络战队重要任务就是在网络战场进行反恐。美国参谋长联席会议称,希望美军的网络战队拥有将对方电脑网络搞瘫痪的能力,中断敌人对关键信息和系统的访问和使用,并且用假信息欺骗对手,让其对现实情况做出误判。今年2月,美国成立了一个新的网络反恐机构——网络威胁情报整合中心(CTIIC)。CTIIC结合多个政府部门,将反恐可疑数据集聚,以促进网络反恐工作协同成效。

英国建“77旅”对抗IS

英国政府高级官员披露,作为新的反恐战略的一部分,英国安全机构正在对极端分子的网站展开一场秘密的网络战。在开办自己网站的同时,政府还对那些监控和堵截网上恐怖分子信息的组织给予支持,以阻止IS等极端组织通过网络对年轻人进行洗脑。

英国建立的安全与反恐办公室(OSCT),主要使命就是协调反“基地”组织及其支持者的行动。它一直受命采取先发制人的行动,破坏恐怖分子的网络,并在英国年轻人中展开“争取情感上支持”的运动。反恐办公室隶属英国内政部,它与英国警方和军情五处合作紧密。

今年2月,据英国《卫报》报道,英国军方决定建立关于社交媒体的特殊作战部队,又称“77旅”,以应对日益猖獗的IS网络恐怖主义。

11月4日,英国通过了“调查权力法草案”,给予警方和安全部门更大的监管权力:网络公司需存数据一年、严禁通信公司点对点加密传输。

法国议会也在今年通过了反恐新法,包括对网络平台进行更加严格的监控,对涉嫌恐怖主义信息宣传予以惩罚。

(据《新京报》)

网络战场成反恐前线

如今,一些非传统网络通信方式也正在被ISIS利用,一切连接人类的虚拟联网方式都有可能被渗透。比利时内政部长让邦在巴黎袭击前曾向媒体警告,索尼PlayStation 4游戏主机(PS4)可能会被恐怖分子利用秘密通信。事实上,根据英国《每日邮报》报道,比利时布鲁塞尔警方在搜捕流窜恐怖案嫌疑人的过程中至少发现了一个PS4主机等证物。

“包括微软Xbox等知名游戏主机也存在着不同程度的监管难度和漏洞。”北京邮电大学一位不愿具名的安全专家向界面新闻透露。他进一步介绍说,加密的VoIP网络语音通信,利用P2P模式,不但难以监听且政府疏于管理,用户可以非常容易地注册新用户名以逃避监管。如果恐怖分子利用PS4,一是从PSN在线游戏服务发送消息,二是语音,三是在游戏里沟通。

“也许在网络平台上召唤玩家的同时,另一场恐怖袭击可能即将发生。”他说。

此外,知名网游如暴雪旗下魔兽世界(WoW)等也都被确信存在网络安全隐患,据《福布斯》报道,2013年爱德华·斯诺登泄露的文件显示,美情报机构国家安全局(NSA)和中央情报局(CIA)确实潜入了WoW等网游监听恐怖分子的虚拟会议。据业内游戏开发者介绍,凡是带组团、公会,语音聊天功能的网游都有漏洞,且各网游的通信协议都不一样,大多数都使用私有协议,这对政府监控是一大难点。

人们从美剧《纸牌屋》中熟知了深不可测的暗网(Darknet),它恐怕也已经成为恐怖分子的避风港。所谓“暗网”,并不是真正的“不可见”,对于知道如何访问这些内容的人来说,它们是可见的。暗网使用非常规协议、端口和可信节点进行匿名数据传输。暗网中存在大量非法网站,比如,人气颇旺的TOR(The Onion Router,洋葱网络)上甚至存在毒品、武器弹药和杀人交易。

ISIS“明暗游击”的网络策略,让世界各地安全部门头疼不已。美国中央情报局局长布伦南称,仅去年一年,即有超过64万起针对美国政府机构的网络事件。他指出,如今恐怖分子已经学会了相关新技术,他们的安全网络通信能力显著提升。

(据新浪网)

黑客团体自发扮演网络“独行侠”

黑客团体GhostSec宣布攻破了IS的暗网宣传网站,用广告替换其网站原来的宣传内容。这是IS第一次在暗网中受重创。

IS等极端组织策划的一系列袭击事件也刺激了民间黑客的反恐行动,尤其是巴黎恐袭事件发生后,多个民间黑客组织宣布与IS开战。

在巴黎恐袭案发生后的第二天,“匿名者”就立即在推特上线#OpParis标签活动,展开一场旨在限制和打击IS等恐怖组织使用互联网应用的行动。11月17日,#OpParis行动推特账号宣布,他们已经让5500多个支持IS的推特账户瘫痪。“匿名者”在推特上针对IS的清理采取了较为合法的途径,并没有私自动用技术手段来亲自黑掉这些账号,而是筛查发现IS相关人员账号后,经正规渠道举报由推特等社交网站来出面封号。

11月18日,“匿名者”的分支组织RedCult还发布了一份公开名单,这份名单中包含了1000个左右的脸书和推特账号,以及已经在今年2月曝光的邮箱地址和IP地址。他们还公布了一批IS成员的名字和个人信息。业内专家分析,IS的招募十分依赖网络,“匿名者”针对IS的黑客攻击能从根本上扰乱这个武装集团的招募机制。

(据《新京报》)