文献引用格式：王俊超 . 网络恐怖主义犯罪防控策略研究 [J]. 信息安全与通信保密 ,2020(8):115-121.
WANG Jun-chao.Research on Prevention and Control Strategy of Cyber Terrorism Crime[J]. Information Security and Communications Privacy,2020(8):115-121.

网络恐怖主义犯罪防控策略研究 *

王俊超
（西北政法大学研究生院，陕西 西安 710063）

摘　要：随着互联网技术的更新迭代，传统的恐怖主义犯罪与互联网的结合衍生出网络恐怖主义犯罪，恐怖组织善于运用现代互联网技术扩大开展活动，宣传主张、招募人员、筹集资金、获取信息、协调行动、传播恐怖知识、散布谣言、发布虚假信息，甚至某些恐怖组织将网络作为攻击目标，为各国打击恐怖主义提出了挑战。因此，通过剖析网络恐怖主义的形式多样化、主体的“独狼”化以及犯罪的智能化和隐蔽化，基于网络恐怖主义的治理困境，从而提出加强国际合作、强化科技支撑、强化舆情监管的策略，进而为我国国家安全提供经验。

关键词：网络恐怖主义；涉恐信息；国际合作；舆情监管
中图分类号：D917.6　　**文献标志码：**A　　**文章编号：**1009-8054(2020)08-0115-07

Research on Prevention and Control Strategy of Cyber Terrorism Crime

WANG Jun-chao
（Northwest University of Political Science and Law, Xi'an Shaanxi 710063, China）

Abstract: With the update and iteration of Internet technology, the combination of traditional terrorist crimes and the Internet has resulted in cyber terrorist crimes. Terrorist organizations are good at using modern Internet technology to expand their activities, recruit personnel, raise funds, obtain information, coordinate actions, spread terrorist knowledge, spread rumors, and release false information, even some terrorist organizations also attack the Internet，the network has posed a challenge for all countries to fight against terrorism. Through the analysis of the diversification of cyber terrorism forms, the "lone wolf" of the main body and the intelligence and concealment of the crime, the paper finds out the Governance Dilemma, and puts forward the strategies of strengthening international cooperation, strengthening

* 收稿日期：2020-05-20；修回日期：2020-07-16　Received date:2020-05-20; Revised date:2020-07-16

scientific and technological support and strengthening public opinion supervision.

Key words: cyber terrorism; the information of terrorism; international co-operation; public opinion supervision

0 引 言

没有网络安全就没有国家安全。近些年来随着信息技术的飞速发展，网络已经渗透到我们生活的方方面面，截至 2020 年 3 月我国网民规模已经达到 9.04 亿人次，同时利用网络实施犯罪的比例已经大幅度提高。随之而来的网络空间安全已经成为世界各国面对的难题，网络空间已经成为反恐新阵地。目前，网络恐怖主义主要是指目标型网络恐怖主义，有时也称为对象型网络恐怖主义（以计算机系统或者整个互联网为目标进行攻击）和工具型网络恐怖主义（将计算机作为网络攻击的工具）[1]，从 20 世纪 90 年代中期起，恐怖主义势力就开始利用网络工具开展活动，宣传主张、招募人员、筹集资金、获取信息、协调行动、传播恐怖知识、散布谣言、发布虚假信息等。还有恐怖组织开始尝试将网络或网络设施作为直接攻击目标[2]。随着人工智能和大数据的加速发展，智能机器人、智能医用器材、无人驾驶技术等网络层面变得更加现实化，目标型网络恐怖主义很可能从“神话”转变为现实。美国曾出现攻击伊朗核设施的“震网”病毒，被认为网络武器的开端，该技术一旦被恐怖分子所掌握，其对人类社会的危害将是难以想象的。我国同时也是受到网络恐怖主义危害的国家之一，我国公布的涉恐人员也基本受到网络极端思想和恐怖组织的网络教唆。因此，通过对网络恐怖主义犯罪特征进行分析，准确发现其治理难点，从而为打击网络恐怖主义提供合理建议。

1 网络恐怖主义的概念和特征

1.1 网络恐怖主义的定义

针对某一概念进行准确界定是其研究的逻辑起点，在当下，无论是学术界还是在司法界对网络恐怖主义的概念均没有准确的界定和概括，这对研究世界范围内各国应对网络恐怖主义造成了困境。早在 20 世纪末，美国著名情报研究员就将网络恐怖主义定义为“网络”和“恐怖主义”的结合[3]。联合国反恐工作组将网络恐怖主义概括为四类行为：“第一类是指远程改变计算机系统来实施恐怖袭击；第二类是指利用互联网作为其基本工具使用；第三类是指将互联网作为散布恐怖事件的手段；第四类是指为了支持恐怖活动而利用网络[4]。”我国学者于志刚认为：“网络恐怖主义的概念和范围，是随着网络的演变、网络恐怖活动犯罪的罪情变化而不断发展的过程。在现阶段，网络恐怖活动犯罪是指出于恐怖主义目的，针对计算机信息

网络，或者利用信息网络，或者在信息网络上进行的攻击行为和威胁行为，以及建立恐怖活动组织、宣扬恐怖主义思想的行为[5]。”舒洪水认为网络恐怖主义常出于某种政治目的来威胁政府或民众，通过采用对计算机及其存储信息进行非法攻击的方式，给攻击对象和受害者造成精神上或者财产上的伤害或者损失，以达到扰乱社会秩序、威胁政权稳定和国家安全的目的[6]。高铭暄指出网络恐怖主义属于恐怖主义的类型之一，只是一种新型的“恐怖主义战术”，不是一种新的恐怖主义形式，其在形式上没有变化，只是在形式上有别于传统恐怖主义[7]。但是就目前而言，网络恐怖主义，主要是指以网络作为对象或者目标而进行攻击的行为。根据我国相关法律对恐怖主义做的规定可以将网络恐怖主义解释为：“一种将网络作为工具或者目标的具有政治目的和意识形态的制造社会恐慌、危害公共安全、侵犯人身财产，或者胁迫国家机关、国际组织的主张和行为。”

1.2 网络恐怖主义的特征

（1）活动方式的多样性

随着近年来各国对恐怖主义的镇压和打击，“基地”和“伊斯兰国”恐怖组织线下阵地受到了严重挤压，因此恐怖分子利用网络的开放性、互动性、低廉性将犯罪的魔爪伸向了以网络为媒介的网络空间。其中以工具型网络恐怖主义为典型，包含传播和收集暴恐活动信息、招募成员、非法融资、扩散恐怖气氛等。恐怖组织利用线上快捷性的特点将暴恐活动计划通过网络渠道对其信息做加密处理后传送到组织成员手上，使得其策划暴恐犯罪更加快捷和隐蔽，这为提前预防和打击暴恐犯罪带来了挑战。

资金和人员是恐怖组织的血脉，通过网络遴选恐怖成员和融资的方式突破了传统的方式，不仅扩大了恐怖成员的遴选范围，而且扩大了融资渠道。以招募成员为例，ISIS 组织将激进的和温和的穆斯林全部作为目标人选，更是在无形之中宣扬其行为的正当性。据中国互联网发展统计报告发布，我国 30 岁以下网络用户占 44.7%，青少年群体的高度参与度使恐怖组织将目标转向该群体，恐怖组织通过传播极端思想引诱青少年，进一步激化从而实施“独狼”恐怖主义行为。在融资方面，恐怖组织突破传统的融资手段，与传统网络恐怖主义通过黑客技术套取个人或机构银行卡信息进而窃取资金的行为不同的是，新式网络恐怖主义活动中，恐怖组织在网上筹集资金通过“温和”的形式实现[8]。有研究表明，其通过网上虚假募捐筹集资金或者设置深层次链接给支持者提供捐赠渠道，这种区别于传统的诈骗或者盗窃手段使得恐怖组织获得更方便的融资手段，为切断恐怖组织资金源限制其活动范围带来困难。

与传统恐怖主义相区别，网络恐怖主义一改对传统物理空间的攻击，恐怖分子通过社交媒体和各种形式的 App 传播甚至直播暴恐信息。在新西兰“3·15”暴恐案件中，暴恐分子 Brendon Tarrant 用头戴的 Go-pro 在 Facebook 上进行全过程直播，该视频不但扩大了暴恐案件的恐怖性，更是对公众造成了二次伤害，这种对公众造成的次害也是恐怖分子所追求的既让更多的人受害也让更多的人看见的目的。因此在研究网络恐怖主义犯罪的情况下，了解犯罪

的形式对于提出治理对策有重要意义。

（2）犯罪主体的“独狼”化

互联网技术的快速发展使得大量的自媒体出现，恐怖组织更加倾向于利用这种“去中心化”特点进行传播，传统恐怖组织的金字塔式组织结构向平面化转化。这种平面化导致网络中的每一个使用者都可能让恐怖组织所利用，由此而产生的“独狼”式恐怖主义袭击就是基于网络的去中心化所导致，该行为使得零散的组织人员化整为零，增强了组织能力，同时“独狼”恐怖活动的随机性、隐蔽性、突发性等特点给防控工作带来巨大的困难。新西兰“3·15”暴恐袭击则是典型的“独狼”恐怖袭击，“独狼”分子有目的、有计划地对国内清真寺进行袭击造成近百人伤亡；斯里兰卡“4·21”连环暴恐案件同样也是由“独狼”分子发动，每起“独狼”恐怖袭击案件的背后都是网络恐怖主义的直接表现。

（3）犯罪行为日益隐蔽化、智能化

犯罪工具的智能化使得犯罪行为隐蔽化，暴恐犯罪也是随着网络技术的智能化而出现隐蔽化的趋势。智能性是由网络犯罪本身特性所决定，在当下恐怖主义犯罪活动向线上转移的过程中，暴恐分子必须具备先进的网络设备，否则无法实施线上犯罪。

对于工具型网络恐怖主义犯罪而言主要是计算机网络，我们在日常生活中所使用的主要是表层网络，而被暴恐分子所掌握的还有深层次的“暗网”，“暗网”所具有的隐蔽性和匿名性增大了防控的难度，同时随着 WEB3.0 时代的到来，一些列智能软件 App（Skype、Whats App 、Facebook、Viber、Twitter）的发展使得犯罪分子之间的交流更加便捷和隐蔽。据情报显示，一款名为 Bit Torrent Bleep 的即时通信软件被誉为全球无法监控的聊天软件，该软件具有阅后即焚的功能并且具备匿名性的特征，恐怖组织一旦掌握该种软件的开发技术，将在各种网络监管范围之外使用，其无疑会成为网络恐怖主义的助推器。对于目标型网络恐怖主义而言，依然出现智能化和隐蔽化的特征，随着人工智能时代的到来，人们的生活与网络更加紧密地联系起来。随着人工智能时代的到来，人们的生活与网络更加紧密地联系起来，人工智能机器人、无人驾驶、纳米医疗机器人等现代科技的发展使得网络攻击更具物理空间的攻击危害，暴恐分子通过编写计算机病毒植入目标系统，达到控制或者破坏的目的，我国工业系统同样面临恐怖分子的攻击。据情报部分显示，被称为“Stuxnet”的网络病毒可以快速攻击工业系统，2010 年及 2012 年伊朗核电站、石油部门的相关计算机系统被攻击的幕后黑手均是此病毒[9]。同时基于网络本身的隐蔽性使得暴恐分子无论在犯罪预备阶段还是实施或者遂后都能完美逃避侦察机关的侦察。由于上述原因，使得近年来大规模有组织的暴恐犯罪转向“独狼”型和网络型恐怖主义犯罪。

2 网络恐怖主义的治理困境

2.1 国际合作的有限性，难以达成普遍共识

在网络恐怖主义的国际治理层面，虽然联合国对网络恐怖主义的概念进行了界定，通过多种决议，如在 2013 年 12 月通过 2129 号决议强调，各国要打击恐怖分子和组织利用网络的招募、资助等行为；在 2014 年通过 2178 号决议

强调，成员国合力打击网络传播极端言论；同年通过了《联合国全球反恐战略》，呼吁各种灵活应对新型恐怖主义督促各成员国阻止“基地”和“伊斯兰国”的网络恐怖行为，为成员国提供了方向，但是制度的落实情况并不乐观。各国在治理网络恐怖主义的过程中，因治理理念、各国利益的不同导致某些国家在打击网络恐怖主义上出现双重标准。西方发达国家特别是美国推行网络霸权主义，不尊重他国主权，以打击网络恐怖主义为名，利用先进的网络技术窥探他国国家秘密、攻击他国关键性网络，甚至不惜以干涉他国更迭的极端方式消除恐怖主义[10]。在对待“东伊运”的问题上，美国在前期将其确定为恐怖组织后出于某种政治目的将其排除恐怖组织之外，这种行为不但难以根治恐怖主义，甚至为恐怖主义的发展提供土壤。同时在技术、情报方面国际合作并不深入，各国在打击网络恐怖主义方面技术差别悬殊，遭受网络恐怖主义攻击的国家主要因为网络技术不成熟，遭受恐怖组织穿透防火墙攻击重要工业系统，各国在技术层面的交流合作尚待深入。

2.2 网络监管落后，涉恐信息难以有效甄别、阻断

网络恐怖主义犯罪的智能化和隐蔽化使得涉恐信息难以有效甄别和预判。在当下网络进入 WEB3.0 时代，恐怖组织传递暴恐信息不断更新迭代，单个恐怖组织使用传播媒介竟达到几十个，其中不乏恐怖组织自己开发的秘密软件，在传播涉恐信息时，使用加密语言并且加上涉恐信息类型众多，难以有效甄别。以“纳希德”为例，其更多描绘“圣战”内容，在诸多网络媒体上用多种语言和代码表达思想，导致负责反恐信息侦察的人员也难以应对。网络恐怖主义逐步进入“暗网”化加大了反恐部门的侦察难度。“暗网”普遍采用多层加密、多重跳转代理节点、随机变换信息传递路径等隐蔽措施，确保无论是从普通的互联网上，还是从“暗网”的用户端、目的服务器端、中途跳转节点以及任何第三方，均无法监控网络通信活动[11]。网路恐怖主义与互联网的结合使“暗网”成为恐怖组织进行资金转移、人员招募、秘密通信、理论宣传的掩体，使得诸多涉恐信息难以有效甄别和阻断，恐怖组织利用“暗网”的特性进行宣传，使得大批潜在暴恐分子从事“独狼”恐怖活动，为我国反恐工作带来诸多难题。

2.3 网络媒体报道不当，扩大恐怖效应

恐怖组织在利用网络媒体进行意识形态渲染的同时，将暴恐犯罪的结果进行扩大化宣传也是其行动目标之一。便捷的社交媒体向来是“基地”和“伊斯兰国”重点关注的目标，其不仅仅通过暴恐事件制造物质损失、残害无辜群众，更希望通过网络的无地域性放大恐怖效果，制造社会恐慌达到政治目的。基于当下网络传播的互动式模式，自媒体的发达性使得世界范围内任何了解网络的人都能在毫不费力的情况下观看甚至间接传播恐怖视频、音频，这种恐怖后果的蔓延性无疑会扩大恐怖事件的影响范围。2015 年 11 月 13 日在巴黎市内发生的暴恐事件造成 132 人死亡的恐怖后果，随后 ISIS 组织宣称对该暴恐案件负责，并且在 Twitter 上发文嚣称，伦敦将是下一个目标，罗马与华盛顿也在劫难逃。此次事件除造成严重人员伤亡和经济损失外，还造成巨大的社会恐慌，恐怖的氛围

再次在全球范围内引爆[12]。需要重视的是部分新闻媒体为追求点击量和收视率在报道过程中故意夸大事件影响效果，使用不恰当词汇恶意制造恐慌，同样在巴黎恐怖袭击案件中部分媒体使用“滴血的塞纳河右岸”“歌剧院大屠杀”等词汇，显然会强化社会恐慌 。因此，无论是恐怖组织本身还是大众媒体在暴恐犯罪发生后通过网络媒体进行肆意传播的行为，都需要进行有效遏制。

3 网络恐怖主义的治理对策

3.1 加强国际合作，拒绝双重标准

和平与安全是世界各国共同追求的美好愿望，治理网络恐怖主义这一非传统安全需要各参与主体之间相互合作、共享信息、共定标准。面对网络恐怖主义这一世界公敌，各个国家应该摒弃“双重标准”，唯有如此，方可有效打击恐怖主义。因此，首先应该坚持联合国在反恐国际合作中的中心地位和主导作用，争取达成对网络恐怖主义标准的认同，主张各国相互尊重、平等合作，反对“双重标准”，推动落实联合国《全球反恐战略》及安理会反恐决议，建立以合作共赢为核心的国际反恐体系[14]。坚持反恐不与特定民族、宗教、国家挂钩，推动不同文明的对话交流，积极发展区域性合作组织的作用，为打击恐怖主义创造大环境。其次，要加强情报之间的合作共享，情报是预防恐怖主义的前沿，加强国家间、区际间、全球范围内的情报合作，把握网络恐怖主义发展趋势，为预防网络恐怖主义提供先导性情报。同时要加强人才的合作培养，增强反恐的智力建设。

3.2 强化科技支撑，阻断涉恐信息传播

网络恐怖主义的传播始终无法脱离互联网的依托，恐怖组织和恐怖分子依靠互联网，甚至在“暗网”中进行传播，网络恐怖主义不同于传统的恐怖主义，其利用网络的虚拟性、匿名性、跨界性等特性，导致网络恐怖主义难以应对，比起其他犯罪更难于发现，因此，为了应对网络恐怖主义犯罪应该加大技术研发，培养高水平侦察人员。一方面，应该推动打击和识别网络恐怖主义工具智能化，恐怖组织利用互联网平台传播暴恐信息时通过多种语言，甚至将信息通过汇编成暗号、编码和符号进行传播，而囿于多种语言的障碍导致该方面的监管处于薄弱领域，因此应着力开发多语言智能识别工具，培养专业化人才，不仅抓住网络平台上的暴恐信息，更要关注深层次连接和暗网的管理，夯实反恐工作中的每一步骤。另一方面，应构建大数据网络平台反恐控制机制。在传统的数据分析理论框架指导下，反恐信息系统控制模式缺乏准确性和高效性，利用大数据网络平台基于大数据平台、云计算、关联的情报线索等创新性分析理论的建设，及时采取手段对网络恐怖主义进行防范和打击。

3.3 加强舆情监管体系建设，引导正确舆论

网络媒体的不当报道和传播渲染了恐怖氛围，对用于传播、集资、宣传暴恐信息的社交媒体和一系列的直播平台进行重点监管和管控，及时切断恐怖组织的传播渠道，加强社交媒体的监管，提高预防性监管能力具有重要意义。首先，应建设健全暴恐信息核查预警机制，依靠大数据和人工智能，针对不同部门、不同数据，

如金融、交通、住宿、医疗等方面数据进行收集和分析，从而减弱甚至消除恐怖组织的网上传播阵地。同时，国家层面应该加强网络舆情队伍建设，网络恐怖主义犯罪涉及法学、民族学、宗教学、外交学、犯罪学、国家关系和传播学等多学科，这说明网络恐怖主义治理的难度，加强舆情队伍建设，推动跨学科人才培养，为打击网络恐怖主义提供智力支撑。其次，加强民企之间的合作。目前的反恐宣传工具比较单一，官方媒体的宣传固定单一，因此，应根据媒体的不同性质分层次进行理论宣传。充分发挥传统媒体和网络新媒体的功能，在官方媒体的引导下发布信息，充分体现反恐信息的可靠性。

4 结 语

网络恐怖主义是恐怖主义的变形，其本质并没有发生改变，虽然网络恐怖主义在我国并没有产生大的影响，但是随着信息化的发展，网络恐怖主义逐渐成为我国反恐的重点。防患于未然是治理恐怖主义犯罪的最好方式，应充分了解网络恐怖主义的现状和特征，把握网络恐怖主义的治理困境，结合我国具体情况，加强国际合作，谋求共同发展，强化科技支撑，加强舆情监管体系从而将网络恐怖主义的火焰湮灭在萌芽阶段，实现国家的长治久安。

参考文献：

[1] 舒洪水，王刚．对我国网络恐怖主义的探讨 [J]. 山东警察学院学报 ,2016(1):68-74.

[2] 朱永彪．网络恐怖主义对各国安全日益构成威胁 [J]. 世界知识 ,2019(10):68-69.

[3] Collin,B.,1997.The Future of Cyberterrorism, Crime and Justice International[J].Crime and Justice International,1997(3):15-18.

[4] See United Nations Counter—Terrorism Implementation Task Force Working Group[N]. R eport on Countering the Use of the Internet for Terrorist Purposes,2009:5.

[5] 于志刚，郭旨龙．网络恐怖活动犯罪与中国法律应对——基于 100 个随机案例的分析和思考 [J]. 河南大学学报（社会科学版）,2015(1):11-20.

[6] 舒洪水，党家玉．网络恐怖主义犯罪现状及防控对策研究 [J]. 刑法论丛 ,2017(3):395-416.

[7] 高铭暄，李梅容．论网络恐怖主义行为 [J]. 法学杂志 ,2015(12):1-6.

[8] 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(2):41-42.

[9] 李涛．总体国家安全观视角下网络恐怖主义犯罪防控研究 [J]. 中国刑警学院学报 ,2019(5):5-11.

[10] 苏红红，郭锐．网络恐怖主义国际治理的制度困境与优化路径 [J]. 情报杂志 ,2020(2):20-25.

[11] 李恒．网络恐怖主义犯罪的现实表现、风险挑战与政策治理 [J]. 宁夏社会科学 ,2020(2):55-64.

[12] 李涛．网络恐怖主义的传播机制及应对策略研究 [J]. 学海 ,2019(2):82-88.

[13] 黄昊．恐怖阴云笼罩巴黎 [N]. 光明日报 ,2015-11-15(005).

[14] 王毅．打赢网络反恐战需要各国同舟共济 [J]. 人民论坛 ,2016,35,(12):6-7.

作者简介：

王俊超（1993—），男，硕士，硕士在读，主要研究方向为刑法学、反恐法学、网络安全法。