网络恐怖主义犯罪的现实表现、风险挑战与政策治理

李 恒

（西南政法大学 刑事侦查学院，重庆 401120）

摘要：网络恐怖主义是恐怖主义与互联网相结合的产物，是恐怖主义在网络上的延伸，具体是指恐怖活动组织与人员基于政治目的或意识形态等其他特定目的，通过利用网络作为犯罪辅助载体，或把网络作为实施恐怖攻击的目标对象，从而达到制造社会恐慌、人员伤亡或经济财产损失等严重社会后果的恐怖主义行为，其最终目的是利用网络为实施恐怖主义犯罪提供服务。维护网络安全是促进国家发展的前提和条件，在阐释全球信息化背景下的网络与恐怖主义犯罪结合为逻辑起点的基础上，剖析网络恐怖主义犯罪的新动向、特征及打击难点的现实挑战。目前，世界各国对网络恐怖主义犯罪研究起步较晚，政策治理不够完善，国际社会形成打击网络恐怖主义的合力还未突破技术等现实困境。梳理并提出网络恐怖主义犯罪的政策治理路径，以维护国家网络空间主权安全，全面构建“网络空间命运共同体”。

关键词：网络恐怖主义；暗网；暴恐音视频；政策治理；网络安全；网络空间命运共同体

中图分类号：D815.5 **文献标志码：**A **文章编号：**1002-0292(2020)02-0055-10

一、问题的提出

近年来，网络犯罪比例已大幅提高，开始出现新的攻击方式。例如，通过黑客病毒、植入木马程序、智能远端操控等。随之而来的网络安全问题也相伴而生，世界范围内利用网络作为工具侵害个人隐私信息、侵犯知识产权等网络违法犯罪时有发生，网络电信诈骗、网络恐怖主义（Cyber terrorism）等已成为全球之公害。就如同全球化现象所带给世界各国的正面及负面影响一般，网络虽然让人们的生活更加便利，信息的分享和传播也更加迅速，但潜在的安全危机也不容忽视。网络恐怖主义犯罪是一种高科学技术条件下的新型恐怖主义活动。恐怖分子利用暴恐音视频作为宣传恐怖主义的重要方式，歪曲宗教教义、煽动极端主义思想、鼓吹暴力恐怖意识形态；利用网络转向攻击网络，借助网络等新兴媒体、智能手机APP等现代信息化传播手段，为暴恐思想传播提供了便利条件。

随着科学技术的飞速发展和日益革新，网络空间已形成了一个具有完整社会功能的活动空间。在信息技术蓬勃发展的时代，恐怖主义犯罪已逐渐不受时空条件的限制，恐怖活动组织与人员利用先进的通信科技设备实施恐怖活动，进而危害国家安全、公共安全的事件屡见不鲜。恐怖活动组织与人员将现实中的恐怖主义犯罪不断转移至虚拟的网络社会之中，逐渐将互联网打造成恐怖主义犯罪的一个新的重要平台或工具。任何事物都有其两面性。网络在服务人类社会生产生活的同时，也为恐怖主义这一非传统威胁、人类社会的毒瘤提供了传播扩散的温床，并改变了恐怖主义的组织形态、行为手段和犯罪方式，扩展了恐怖主义的影响范围，形成了网络恐

作者简介：李 恒，男，西南政法大学刑事侦查学院讲师，四川社会治安与社会管理创新研究中心副主任，法学博士，主要研究方向为刑法学、反恐法治理论与实践。

基金项目：重庆市社会科学规划博士项目“总体国家安全观下反恐情报理论与实践研究”（项目编号：2019BS109）；教育部人文社科规划基金项目“国内安全保卫法治化研究”（项目编号：19YJA820030）；四川社会治安与社会管理创新研究中心重大委托项目“中国恐怖主义犯罪防治与对策研究”（项目编号：SCZA19A01）。

怖主义这一具有独立特点的新型恐怖主义。有诸多证据表明，恐怖活动组织与人员已熟练掌握了多种网络技术，并试图培植“圣战”分子的网络专家，包括暴恐音视频在内的多种网络恐怖活动，给全球带来了重大威胁[1]。

网络恐怖主义是在人类进入网络时代后产生的新现象。恐怖主义还在进一步向网络空间渗透，与网络的结合更加紧密，其网络化趋势更加凸显，成为人类社会面临的新的重大威胁。网络恐怖主义煽动在境外、行动在境内；恐怖音视频的制作在境外、传播在境内[2]。因此，要彻底铲除恐怖音视频，就必须坚决打掉境外制作传播的源头和平台。目前，世界各国对网络恐怖主义犯罪研究起步较晚，研究成果相对缺乏，法律应对与政策治理还不够完善，国际社会形成打击网络恐怖主义的合力还未突破技术等现实困境。本文阐释全球信息化背景下网络与恐怖主义犯罪相结合的表现形态，剖析网络恐怖主义犯罪的新动向、特征及打击难点的现实挑战，提出网络恐怖主义犯罪的刑事政策治理路径，以期为国家安全战略构建提供支持。

二、现实表现：网络与恐怖主义犯罪相结合

（一）网络与恐怖主义的纠合

以互联网为代表的新兴技术，已对人类生产生活和社会经济产生了深远影响。由于网络活动具有隐密性、匿名性、跨越时空等特性，以致网络成为重要的犯罪通道。1996年，斯里兰卡武装组织“塔米尔猛虎组织”针对驻外使馆发动电子邮件病毒攻击，被视为最早有记录的网络恐怖主义事件。随着社交媒体的广泛运用，其互动密集、成本廉价、传播广泛的特征日益凸显，在为用户提供沟通便利的同时，其匿名、复杂、快捷的本质属性也为恐怖主义带来了可乘之机。网络技术赋予了恐怖主义现代化特征，科技的变更迭代也是网络恐怖主义衍化的关键因素和直接动因。在信息网络技术飞速发展的今天，网络恐怖主义犯罪随之在全球范围内呈现出日益高发之态势并衍变出新形态[3]。

当今世界，人们的生活重心已由单一的现实空间，转变成现实空间与网络虚拟空间各占一半。人们可以通过网络信息平台和社交媒体轻松地获得各类恐怖主义信息，在恐怖活动组织与人员的眼中，这些信息正是搜集和利用的目标。一方面，恐怖分子利用网络的开放性、跨国性、隐秘性等特点，将恐怖活动不断转移到网络空间，使网络逐渐成为恐怖主义犯罪的工具和平台。特别是网络的无疆界性和高科技性，恐怖主义犯罪活动也随之跨越了历史疆域。另一方面，恐怖分子开始利用网络技术的隐蔽性和便捷性，将对激进分子的招募、对恐怖分子的管理以及对恐怖活动的策划由现实空间转为网络空间。从某种程度上讲，网络恐怖主义是计算机网络与传统恐怖主义紧密结合的最终产物，而网络恐怖主义犯罪就是恐怖分子将网络和恐怖主义相结合的必然结果[4]。

目前，恐怖活动已脱离使用“冷”“热”武器进行破坏的阶段，开始与互联网、机器人、核武器、基因生化等高科技紧密联系。尤其在信息技术进入网络3.0时代后，Facebook、Twitter、Instagram、YouTube、Telegram等国际社交媒体的兴起，使得网络空间活动的参与主体变得更加多元，普通公众也从网络信息的“被动接收者”转变为“主动发布者”。例如，网络暴恐音视频已成为恐怖活动组织与人员向境内传播恐怖思想的主要渠道、煽动境内暴恐分子行动的重要工具、境内人员组织暴恐团伙的思想基础和暴恐分子实施暴恐活动的“精神支柱”。国际社会还注意到，恐怖活动组织与人员开始将目光从封闭式的普通网络论坛转向开放的社交平台。社交平台已成为恐怖分子实施网络恐怖主义犯罪的最好工具，催化了网络恐怖主义的滋生与蔓延，网络恐怖活动已成为恐怖主义犯罪的重要发展方向。

（二）网络成为恐怖主义犯罪的助力平台

网络恐怖主义是时代的产物。随着信息技术的快速发展，网络为恐怖活动组织与人员提供了新的活动工具和犯罪平台，恐怖主义正由物理空间延伸到信息空间，与传统的恐怖活动相比，网络恐怖活动更加“无形”。尤其当网络犯罪与恐怖主义结合在一起时，网络恐怖分子即可能成为继经济驱动、黑客攻击和间谍行为之后的第四种互联网攻击发动者，恐怖主义可能成为实施网络攻击的动机和目的。

恐怖主义相比于其他非传统安全威胁，具有“根深、枝广、嬗变”等特点。如果把恐怖主义比作是当今全球之“瘟疫”，那么网络恐怖主义就是该“瘟疫”的幕后推手。为了增强恐袭的隐蔽性，恐怖活动组织与人员或匿名登录、或使用隐藏身份、或用暗语交流，已经由起初的依托互联网进行联系、策划恐怖袭击，拓展为依托互联网进行人员招募、培训恐怖分

子、宣扬“圣战”极端主义思想、发布并传播暴恐音视频、传授武器装备技术或制爆等特殊技能。可以看到，网络恐怖主义是助推恐怖活动大幅增多的主要原因。网上传播宗教极端思想、制爆技术和反宣渗透活动不断增多，“世维会”等“东突”组织、敌媒借网络媒体滋扰煽宣活动频仍，恐怖分子不断提升极端信息发布的质量与复杂程度。随着各国反恐力度的不断加大，恐怖活动组织与人员已开始借助“暗网”（主要指一些存储在网络数据库中、不能通过超链接方式访问，需要运用动态网页技术访问的信息资源集合。亦即不属于那些可以被常规搜索引擎检索的表面网络，意图构建一张广义上的“暗网”）进行犯罪活动的趋势愈发明显。

大数据应用、移动互联网、云计算物联网三大技术的广泛应用，使过去传统信息化应用模式悄然发生变化。由于网络信息的全球性、开放性、共享性、快捷性、即时性、传播方式多样等固有特征，网络恐怖主义成为了新时代的安全治理难题。随着互联网的普及，网络安全问题正在变得越来越突出。例如，近年来，“伊斯兰国”等恐怖组织，通过非法手段掌控网络社群媒体，运用网络社交平台在虚拟空间“线上”从事恐怖主义活动，宣扬暴力恐怖主义、宗教极端思想、传授制枪制爆以及恐怖袭击等犯罪方法，煽动实施爆炸、暗杀、投毒和自杀式袭击等恐怖活动音视频。“9·11”事件发生后，美国联邦调查局查出恐怖分子除以网络邮件进行联络，更运用网络途径宣扬恐怖主义、募集资金、协调行动等，凸显利用网络协助恐袭。再如，2013年9月，肯尼亚首都内罗毕西门购物中心暴恐事件的制造者，对袭击事件整个过程进行了“推特直播”，以此宣扬其暴力恐怖行为和极端主义思想。同时，还向全世界招募圣战士参与恐怖袭击活动，进行激进暴力恐怖攻击行动，危害目标国家和地区的和平与安全，导致区域和国际安全环境的持续动荡。通过网络发布血腥视频，不仅能达到制造民众的心理恐慌、炫耀实力、吸引世界关注，给国际社会的反恐行动施加压力的目的，甚至还起到妖言惑众、挑起事端、激化矛盾的作用[5]。

（三）网络恐怖主义犯罪的表现形态

许多西方国家对网络恐怖主义的意涵，大多采用“国际安全与合作中心”在一份名为《网络安全及恐怖主义国际会议提案》（Proposal for an International Convention on Cyber Crime and Terrorism）文件上所使用的定义：“未经合法权力授权之下，故意使用或威胁使用暴力破坏扰乱互联网系统，此种行为将可能造成一人或多人死亡或受伤；使有形财产的实质毁损、社会失序或严重的经济损失”。学者托马斯（Timothy L.Thomas）指出，近年来的国际反恐行动已查获诸多恐怖分子所使用的电子计算机，通过分析电脑设备，可发现恐怖分子开始利用网络进行搜集资料、理念宣传、筹措资金、交换情报、远程指挥、组织动员、招募新人及隐匿行踪等证据活动，托马斯将此类活动统称为“网络恐怖主义策划行为”。同时，还有学者则将恐怖分子在网络空间的所有活动，一概视为网络恐怖主义犯罪行为。学者古德曼（Marc D. Goodman）将网络恐怖主义表现形态分为两大类。一类为“激进恐怖分子在网络空间实施的各种活动”，包括通过网络进行宣传、鼓动和募款等“支援性活动”，如人员培训、交换情报和筹划攻击，与威胁恐吓等“操作性活动”。另一类为“利用计算机网络攻击国家的重要基础设施”，即通过电子计算机、网络攻击与一般民众日常生产生活息息相关的各项基础设施，主要包括大众运输系统、政府官方网站、银行及金融机构等。美国国防部认为网络恐怖主义是非国家行为者利用计算机及电信能力，针对信息资讯、电脑系统、电脑程序实施的犯罪行为，以制造暴力并破坏公共设施，或制造社会恐慌，最终达到迫使政府或国际组织实现其特定的政治主张或意识形态等目的[6]。

网络恐怖主义呈现两种表现形态，一种是将网络作为辅助工具的工具型网络恐怖主义，另一种是将网络作为攻击目标的目标型网络恐怖主义[7]。工具型网络恐怖主义是指为了实现恐怖主义的政治主张和行为等意识形态目的，通过计算机网络进行的违法犯罪活动。例如，反侦查、筹资、通联和宣传等行为活动。目标型网络恐怖主义是指意图实现其政治、意识形态等目的的主张和行为，针对网络信息系统、网络空间实施的恐怖袭击，意图制造社会恐慌、危害公共安全、侵犯人身财产等违法犯罪活动。当前，工具型网络恐怖主义活动异常活跃，从未来发展来看，目标型网络恐怖主义威胁可能更加突出，袭击重点将是金融行业、商业系统，以及高度网络化、智能化管理的水、电、气等供应控制系统，油气管道、客运中心、航空机场枢纽和车站码头管理系统等。

基于已有研究成果并借鉴国外关于网络恐怖主

义的界定，笔者认为，网络恐怖主义是恐怖主义与互联网相结合的产物，是恐怖主义在网络上的延伸，具体是指恐怖活动组织与人员基于政治目的或意识形态等其他特定目的，通过利用网络作为犯罪辅助载体，或把网络作为实施恐怖攻击的目标对象，从而达到制造社会恐慌、人员伤亡或经济财产损失等严重社会后果的恐怖主义行为，其最终目的是利用网络为实施恐怖主义犯罪提供服务。维护网络安全是促进国家发展的前提和条件，应当客观把握当前网络恐怖主义犯罪的新动向、特征及打击难点，坚决防范和打击网络恐怖主义及其他违法犯罪活动。

三、风险挑战：网络恐怖主义犯罪的新动向、特征及打击难点

（一）网络恐怖主义犯罪的新动向

互联网改变了人类社会生产生活和思维方式，对人类社会的发展进步起到了重大影响和推动作用，并形成了网络这一社会活动的新空间。网络是一把双刃剑，在为人类提供各种便利的同时，也为恐怖主义提供了滋生发展的温床。

1.网络恐怖主义成为威胁世界安全与稳定的新方式

网络恐怖主义作为“互联网+”版本的代表，是现代科技革命背景下恐怖主义活动的新型表现形式。一方面，网络恐怖主义作为新兴的恐怖主义表现形式是传统违法犯罪的延伸和扩充。由于网络恐怖主义所牵涉的范围十分广泛，包括网络科技本身存在的局限，黑客病毒、程序安全漏洞、恶意系统程序、电脑蠕虫等恐怖袭击手段不断变化翻新，正当某些系统及程序漏洞获得修补的同时，尚有更多新安全软件问世，也随之出现更多新的漏洞，各种变化皆使得网络恐怖主义比传统恐怖主义更加难以被发现。另一方面，与传统恐怖主义相比，网络恐怖主义具有“非现实破坏性”、随意性、突发性和低成本性，恐怖活动组织的隐蔽性、制造恐怖结果的超时空性，以及与传统恐怖主义的关联性等。恐怖活动组织与人员利用网络信息技术，以进一步扩散极端主义主张。例如，在网络空间开展宣传暴恐极端主义思想、制传暴恐音视频、招募补充人员、募集筹集经费、传授恐怖活动技能、远程数据破坏或实施网络恐怖袭击等犯罪行为[8]。

2.科学技术成为助推网络恐怖主义滋生发展的新动力

网络恐怖主义通过各种科学技术手段，用最小的代价在网络虚拟空间制造恐怖氛围，甚至能够制造比传统恐怖活动影响更大的网络空间和现实空间的双重灾难[9]。一方面，全球信息化背景下，恐怖活动组织与人员的制爆规模、技术水平及爆炸装置种类威力不断升级。恐怖组织利用网络技术手段，通过特定网络渠道获取信息，或在恐袭后宣布负责，或为恐怖组织成员提供培训资料和犯罪方案，从而构建了方便组织内外信息传递的线上、线下的运作模式[10]。随着网络恐怖主义肆虐及现代信息技术的快速发展，境内外涉恐违法犯罪人员利用各种非法渠道，传递被封堵的境外网站链接，利用“网盘”等存储空间中的极端信息，进行宣传煽动、秘密勾连和策划指挥，网络恐怖主义新动向已成“白热化”发展态势。另一方面，在科学技术发展影响之下，暴恐音视频成为暴恐分子从事民族分裂、宗教极端和暴恐活动的最主要诱因。从国内看，据统计，在暴恐音视频的传播影响之下，“三股势力”案件中涉案人员基本都曾下载观看传播恐怖音视频，暴恐团伙受暴恐音视频影响作案的占到70%以上，北京“10·28”、昆明“3·01”等案件作案暴徒均是直接受暴恐音视频的毒害[11]。近年来，制作发布暴恐音视频数量虽持续减少，但拉拢大学生参加“圣战”、煽动对我国海外利益目标实施袭击内容增多。从国际上看，“伊斯兰国”等暴恐极端组织持续煽动全球穆斯林袭击“异教徒”，不断在网络社交平台发布暴恐音视频和电子书，散播宗教极端思想，煽动全球穆斯林群众用石头、刀、卡车等一切可能的方式袭击“异教徒”，声称将持续在人口密集场所发动袭击。“伊斯兰国”等暴恐极端组织还加大网络传授制枪制爆、毒气等使用方法，并企图将电子设备改造成爆炸装置实施暴恐行动。

3.“暗网”恐怖活动成为网络恐怖主义更加隐蔽的新表现

利用“暗网”加密渠道，降低制造恐怖事件的成本和技术门槛，大大提高了行动能力，缩短了恐怖活动行为周期。“暗网”背景下的恐怖主义存在狭义说和广义说之分。广义的“暗网”也被扩大解释为所有使用了特殊软件或特殊配置的加密传输信息，从而导致政府监管部门无法有效管控的网络通信和联络方式。除“Tor”网络（The Onion Router，俗称“洋葱路由器”）等隐蔽网络外，还包括非标准协议加密网络通信（如翻墙工具）、虚拟专用网络（如VPN在线代理

网络）、加密即时通信软件。特别是翻墙工具和VPN代理网络主要被用于穿透国家网络关防，访问被封锁的境外网站和网络服务，加密即时通信软件也经常被违法犯罪人员用作秘密通联的特殊渠道。狭义的“暗网”特指通过专门的隐蔽通信工具在互联网上搭建隐蔽网络，其中使用最广泛的就是“Tor”网络，其他典型的网络包括I2P（Invisible Internet Project，即“隐形网计划”）等，不同的网络空间彼此互不相通。架设在“暗网”上的网站采取特殊措施对真实位置进行深度隐藏，只允许本网络用户访问，普通互联网上的用户和搜索引擎则无法访问和查询该网站信息。此外“伊斯兰国”等恐怖极端组织与人员将一些网络在线活动转向“暗网”，利用其进行恐怖主义犯罪活动，进一步增大了“暗网”的社会危害性。

（二）网络恐怖主义犯罪的主要特征

1.犯罪手段的多元化

网络恐怖主义导致暴恐极端主义思想比以往任何时间节点都更容易传播扩散，甚至比生化袭击武器的破坏力还强大。第一，利用即时通信工具向他人传播、教授“圣战”及制作爆炸装置技术音视频信息，有的在用户群内发布相关网络链接地址。“三股势力”人员利用网络即时通信工具勾连、传播宗教极端思想、煽动策划暴恐活动动向十分突出[12]。第二，恐怖分子利用网络进行宣传动员、网络攻击、资金转移、内部联系、人员招募、危险品购置、“独狼”行动、情报获取与知识传递等活动。第三，暴恐分子频繁变更网络发布平台。例如，“东伊运”将恐怖音视频作为主要煽动极端主义手段，频繁变更发布网络平台域名网站。新域名服务器一般设立在境外部分反华欧美国家和地区，恐怖组织利用境外互联网购买或出售物品是其网络恐怖活动的重要表现。第四，“翻墙”登陆敌对网站，转发境外谣言信息。重点地区人员使用“翻墙”软件登陆境外敌对网站，也有人将境外“东突”反宣视频上传至国内网站[13]。第五，暴恐视频发布数量也不断增多、内容多样。暴恐音视频和电子书发布屡见不鲜，策划煽动恐怖袭击的气焰十分嚣张。如新疆拜城县“2·17”暴恐案中，团伙成员多次聚集在主犯出租屋内聚众观看恐怖音视频，逐渐形成极端主义思想，随即进行制爆试爆活动，预谋实施“圣战”直至案发。

2.行为方式的隐蔽性

与传统恐怖活动相比，网络恐怖活动更加“无形”。第一，从利用境内网站、网盘等公开传播，转向利用境外即时通信工具传播链接地址，利用私密网盘、通信群组、关系圈子和加密传输等方式传播，并不断更新和升级版本，依靠网络虚拟和隐蔽特性恐怖组织更易隐藏其中使其难被察觉，以加大侦查部门的监测难度。第二，暴恐分子媒体制作与传播技术日益娴熟，并转向更隐蔽的方式传播网络暴恐音视频。据统计，大量已发暴恐案件都与恐怖音视频有关，90%的涉案人员都交代曾经观看过恐怖音视频，可见暴恐分子受恐怖音视频“洗脑”十分严重[14]。“基地”、“伊斯兰国”组建了专门的媒体部门或宣传团队，这些音视频主要通过加密传输、多渠道存储分享等方式传入中国境内，与以往在境内网上公开传播不同，暴恐分子开始利用通信群组、圈子等非公开隐蔽渠道传播相关链接地址，并且不断更新版本以增加监测难度。第三，恐怖音视频大肆宣扬“圣战”等极端主义思想，暗中传授暴恐犯罪技能，已成为催生境内暴恐活动的重要“思想根源”，网上暴恐音视频成为暴恐活动的“训练教材”，成为危害国家安全和公共安全的心腹大患。加之，网络空间无远弗届，恐怖组织可在世界任何角落从事不法活动。据相关报道，每年恐怖组织利用网上赌球、网上博彩业等洗钱、筹集资金达数亿美元。大量暴恐音视频流传到社会，通过手机储存卡、U盘、二手手机等在人际间相互传播，并积极拓展新的传播渠道，继续谋求网络生存空间，更加难以发现和及时阻断。

3.意识形态的煽动性

恐怖组织不仅运用网络进行宣传、攻击关键基础设施或从事其他犯罪行为，更可通过“启发”与“激进化”手段促成“孤狼式”恐怖攻击。网络恐怖主义的现实威胁，最大特点是通过“激进化”的方式“启发”潜在支持者。“启发”意指具有宗教、种族或社会背景的人士，原已具有某种程度的攻击倾向或反社会性格，在接受媒体宣传、暗示或煽动后，获得执行恐怖主义的指导。网络科技与社群媒体的兴起即成为“启发”的绝佳平台，因为不需要人际间的实体互动，更不必加入恐怖组织，只要网络社群灌输观念，即可产生“激进化”的效果。而“激进化”通常是指采取一种被主流社会拒绝的宗教观，并以此将暴力合理化，以便促使社会与政治现状的改变。由于网络恐怖活动无须耗费大量时间和金钱招募人员，其训练门槛低亦属间接操作，恐怖组织更易招揽及保留

追随者。另外，从网络暴恐音视频内容看，当前的“启发”与“激进化”不再通过组织“面对面”聚会的形式，转为多由“线下”论坛、影音网站及网络社群所组成，成为恐怖主义的最新形态。此类音视频呈现出系列化、多语种的发展趋势，内容涉及煽动“圣战”、教授制枪制爆、炫耀鼓吹实力、招募人员等，且往往在境内发生恐怖案事件后第一时间发布、进行声援、吹捧“战果”。通过借助信息传播的影响力，任何恐怖袭击事件抑或网络恐怖活动本身，均能通过网络宣传推波助澜而引起更大关注，更助其宣扬理念。

（三）网络恐怖主义犯罪的打击难点

1.切断渠道难

恐怖活动组织与人员滥用世界经济全球化、科技信息化的发展优势，不断传播暴恐极端主义思想，变本加厉危害国际社会和人类安全，成为国际安全领域中最为棘手的现实难题之一。网络技术侦查手段跟不上，反制能力弱，难以做到有效侦控。新型网络传播工具层出不穷，现有传统侦查措施已跟不上科技发展步伐。目前，中国国家互联网中心相关部门还难以完全阻截“加密代理”、“虚拟专网”和“穿透工具”。暴恐分子很容易通过“加密代理”、“翻墙”软件等从境外网站获取恐怖音视频和下载链接地址。暴恐分子通过境内网站、社交应用等传播渗透行为还难以被有效防范和控制，境内网上勾连传播的渠道难以被切断。

2.铲除源头难

网络恐怖主义犯罪无国界化引发的犯罪扩张存在反恐困境。实践中，暴恐音视频主要依托Google、YouTube等基于“大数据”、“云计算”的境外大型网站发布传播，拍摄团队位于巴基斯坦、伊拉克、叙利亚、阿富汗等涉恐重点国家的边境地区，拍摄完毕后传至土耳其等国进行后期加工编辑，之后上传境外大型互联网站，利用境外大型网站网盘、即时通信工具进行存储传播。其维护人员主要分散在土耳其、荷兰等多个欧洲国家，服务器主要位于北美、欧洲等地区，对这类网站进行封堵和技术反制难度较大且成本较高，交涉和举报时间较长。网络恐怖主义犯罪可能间接性地引起遍布于多个地区的恐怖活动，造成更多的经济损失和人员伤亡，对其打击和预防难度也随之增加。

3.管控制裁难

恐怖音视频网流传时间长、存量多，大量恐怖音视频流传在社会上，并通过手机存储卡、优盘、二手手机等在人际间传播，发现和清理难度较大。特别是以关键词过滤为主的监控方式难以有效监测恐怖音视频，尤其是对二手手机、电脑音像市场的管控难度较大，难以有效阻断恐怖音视频的传播扩散。暴恐分子普遍使用境外加密即时通信工具、手机“黑卡”隐蔽传播暴恐音视频，采取“机卡”分离携带暴恐音视频，增加了发现、侦查和打击难度。目前，我国法律法规针对恐怖主义犯罪的网络空间化引发刑法评价体系还十分滞后，特别对观看、持有、上传、存储、下载暴恐音视频等行为的法律认定，以及打击为网络犯罪提供“穿透工具”等行为，尚缺乏明确的法律依据和制裁手段。而网络监管和网络反恐法律的滞后以及现有法律体系中存在的漏洞使得网络空间成为恐怖分子实施犯罪的平台。

4.封控“暗网”难

“暗网”因其特殊的加密服务特性成为恐怖活动组织与人员的“避风港”。相较于常见的恐怖活动行为，“暗网”恐怖主义行为手段更具有隐蔽性，实现途径更具技术性，拓展功能具辅助性。“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。通常难以被常规搜索引擎发现，用户需通过程序性注册，以动态请求方式借助“Tor”等特定工具登录浏览[15]。“Tor”网络等“暗网”也可以被用作穿透网络关防的工具，用户通过“暗网”连接到一个境外代理节点，再进入普通互联网，访问已被封堵的境外涉及极端内容的网站。由于“暗网”具有良好的匿名性和抗追踪性等特征，大量非法网站依附其上。

四、治理路径：网络恐怖主义犯罪的政策治理

（一）以总体国家安全观为指导，充分发挥刑事法律在网络反恐中的重要作用

网络空间不是法外之地，维护网络安全是总体国家安全观的重要组成部分。网络恐怖主义及其犯罪的治理，需要通过国际法治和国内法治两个层面来开展，其中，国际法制度的实施最终还是要通过转化或吸收的方式依靠国内法来实现。当前，无论是从法律、政策还是从安全角度出发，网络空间都还是一个没有形成全球共同规范的未知领域，无论是权威、透明度还是责任都不是很清晰[16]。预防和打

击网络恐怖主义犯罪行为的国内法制度应尽快完善。[17]党的十八届四中全会提出，要加强互联网领域立法，完善网络信息服务、网络安全保护、网络社会管理等方面的法律法规，依法规范网络行为，强化针对破坏网络安全等重点问题的治理[18]。

充分发挥刑事法律在网络反恐中的重要作用，坚持以总体国家安全观为指导，采取有效措施，全面推进网络空间法治化。第一，在刑事立法层面，为有效应对恐怖主义，实现预防和惩治恐怖活动的法律化、制度化、常态化，并与国际接轨，全国人大常委会于2015年12月27日颁布了《反恐怖主义法》。执法部门在应对网络恐怖主义犯罪等新型犯罪时，应以《反恐怖主义法》、《网络安全法》和《刑法修正案（九）》为根本指导。《刑法修正案（九）》仍然以保护计算机系统和数据为主，并重点打击利用计算机和网络实施的相关犯罪。增设了违反网络服务商义务的犯罪，第286条之1规定了“拒不履行信息网络安全管理义务罪”；增设利用信息网络实施其他犯罪和帮助他人利用信息网络实施犯罪的规定，第287条之1规定了“非法利用信息网络罪”；第287条之2规定了“帮助信息网络犯罪活动罪”等。《刑法》出现了扩张的内在动因与现实需求，并以“风险社会”和预防犯罪作为刑事立法政策调整的背景，表现为帮助行为的正犯化、预备行为的实行行为化、过失危险行为的犯罪化以及行政犯和义务犯的出现等，彰显中国依法打击一切形式的恐怖主义行为的信心和决心。笔者认为，可增设包括利用网络进行犯罪或以袭击网络为目标的高科技恐怖主义犯罪罪名，即有关网络恐怖主义罪名，并配置适当的法定刑[19]。第二，在刑事打击层面，依法打击网络恐怖主义、涉恐音视频等违法犯罪活动。集中打击网络恐怖主义特别是传播暴恐音视频等违法犯罪行为。开展集中打击，集中梳理一批涉恐怖音视频案件线索，查明情况、固定证据，及时依法打击处理，以免造成现实危害。打击网络恐怖主义还应当严格贯彻落实《国家安全法》、《反间谍法》、《国家情报法》等法律法规，将打击违法犯罪与执行法律政策有机统一。第三，在刑事执法层面，执法部门应当用好用足现有的法律规定和“两高一部”出台的《关于办理暴力恐怖和宗教极端刑事案件适用法律若干问题的意见》，重点打击首要分子、骨干成员，对情节较轻、危害不大、未造成严重后果，且悔过的初犯、偶犯及其他情节显著轻微的，采取治安处罚、社区矫正、教育转化、重点人管控等措施，积极争取教育挽救大多数。在深入开展严厉打击暴力恐怖活动专项行动的同时，讲究法律政策和工作方式方法。区分宗教极端违法犯罪与正常宗教活动的本质区别，既要精准打击网络恐怖活动组织与人员的违法犯罪行为，又要依法保护少数民族群众的合法权益。综合运用多种手段，坚决铲除网络暴恐活动滋生蔓延的土壤，坚决把暴恐违法犯罪分子的嚣张气焰打压下去，全力确保取得良好的政治效果、法律效果和社会效果。

（二）以加强网络社会管理为抓手，依法开展网络恐怖主义犯罪侦查

针对网络恐怖主义活动整体态势开展形势研判，通过对网络恐怖主义犯罪案件的类型、发案量、作案对象、重点人群、作案手段等方面的数据进行科学统计分析，准确把握当前网络恐怖主义的整体态势、发展规律和发展特点[20]。

1.跟踪发现预谋的网络恐怖主义犯罪行为

研究发现，“独狼式”恐怖分子在袭击之前都热衷于搜索、观看网络暴恐音视频。以网络社会管理为抓手，加强定期巡查，彻底封堵查删危害信息。通过对网络情报信息的深挖和经营，及时发现前瞻性、预警性情报信息，从而提前预防和制止犯罪，最大限度地减少现实危害。一方面，运用大数据手段可以分析监测网络恐怖主义网站的IP地址等数据信息，结合该IP所登录的社交账号发布的言论信息，通过浏览次数与发布言论程度划分其危险等级，并通过IP判断其所在区域位置，在恐怖活动发生之前，将预谋实施恐怖活动的人员抓获。另一方面，完善特殊领域的阵地控制建设。加强网络刑事特情与治安耳目的力量建设，为反恐怖长期斗争提供智力支撑。加强情报技术研发储备，建立网上网下发现通报、情报交流和会商研判机制，建立健全公安机关与国家安全、武警部队等部门的协同联动机制。

2.掌握网络恐怖活动组织与人员的动态规律

一方面，通过将不同恐怖活动组织与人员实施网络恐怖违法犯罪行为后遗留下的数据进行对比碰撞，发现不同恐怖活动组织实施网络恐怖主义行为的技术特点，并通过与金融社交网、房产等数据串联，掌握不同恐怖活动组织与人员的活动规律，有针对性地采取预防和打击措施，减少恐怖活动带来的损失。通过某个地方对网络犯罪情报信息开展深挖

扩线，梳理出大批量、大范围的涉恐情报信息。另一方面，掌握网络恐怖活动组织与人员的动态规律需强化三项措施：一是强化基础工作。完善恐怖音视频样本数据库，及时向互联网企业提供恐怖音视频关键词、样本、特征值和技术识别特征。加强对互联网企业安全审核人员的业务培训，提高其对网络恐怖活动组织与人员、恐怖音视频的识别判断和处理能力。二是加强监督检查。依托派驻互联网企业网安警务室力量，加强网上重点阵地管控，督促互联网企业加强内容审核，落实屏蔽过滤、删除关闭和注册审核、内容审查等安全防范措施。三是落实责任追究。对未按要求采取有效安全防控措施的互联网企业追究法律责任，依法予以打击处理。

3.强化对境外源头的网上侦控与技术反制

其一，根据《反恐怖主义法》等相关法律法规，电信业务经营者、互联网服务提供者，应当为公安、安全等机关依法进行防范、侦查、调查恐怖活动提供技术接口和解密等技术支持和协助，积极开展涉恐信息源头的网上侦控。依法加强对大数据的监督和管理，特别是加强对互联网企业掌握的涉及国家利益、国家安全以及个人隐私的数据信息的保护。其二，组织专门力量加大境外网上刑事侦查和内线侦控力度。加强对加密信息的技术管控，深挖境外制作发布恐怖音视频的组织与人员，查清其组织体系、人员身份、现实背景，掌握其活动情况，收集固定证据。网安、技侦、国际合作等专业部门加强协作配合和情报指挥一体化合作渠道，建立健全网上打防管控综合体系，提高网上涉恐活动的预警监测、网络管控等能力。其三，加强对敌技术渗透和技术反制。控制境外网上煽动宣传阵地，掌握制作、传播、访问暴恐音视频的境内人员线索，对境外“东伊运”自建网站和举报、交涉无效的境外发布传播平台、宣传账号实施技术反制，摧毁恐怖极端网站服务器硬件设施。组织专门力量持续开展常态化、密集式、不间断的技术反制措施，促使境外网站主动删除暴恐音视频及其网页链接，关停相关账号。

（三）以维护网络空间安全为依托，全面强化网络恐怖主义打击防范

全面贯彻落实《反恐怖主义法》第三章安全防范内容，依法全面开展互联网监管措施。提升互联网企业的责任感和使命感，将互联网反恐措施内化为互联网行业的自律准则，主动配合政府甄别、清除互联网涉恐相关信息，实现政府与企业在互联网反恐、网络安全等问题的良性互动。

1.开展打击网上暴恐音视频的专项行动

一方面，加大对境外网站信息的封堵力度，封住网络恐怖主义境外来源渠道。搜集掌握境外恐怖音视频发布传播平台和账号，及时发现发布恐怖音视频的动向，判明上传渠道，在固定证据的同时，第一时间予以封堵。对境外发布传播恐怖音视频的平台、链接地址及张贴、传播恐怖音视频的网站，一经发现立即封堵。坚决打击暴恐音视频制作、发布、传播源头，开展清理网上暴恐音视频专项行动，全面清理境内主要商业网站、微博、移动即时通信工具等网络应用软件中的涉暴恐信息，严厉打击和封堵网上宗教极端主义思想与暴恐音视频等内容的传播，整治打击暴恐音视频网下传播渠道，依法查处违法犯罪分子，坚决切断利用网络煽动策划暴力恐怖活动的渠道和通道。另一方面，深化打击暴恐音视频的制作与传播，深挖细查境内暴恐信息传播源头，明确刑事打击重点，严厉打击网络恐怖主义犯罪活动。重点打击参与制作发布、从境外网站下载并在境内网上传播、提供网址煽动观看下载、下载后利用移动存储介质进行传播、组织聚众观看暴恐音视频、受恐怖音视频煽动刺激开展暴恐活动等犯罪活动[21]。

2.强化对网上传播渗透渠道的管控力度

一是持续开展对“翻墙”在线代理网站网页、虚拟专网（VPN）、手机“翻墙”APP软件的专项整治工作。配合网信办等部门加强对外交涉力度，与境外互联网企业建立快速举报的处置渠道。二是强化网络监管力量建设，建立健全部门联络沟通会商和指挥协调机制，调动各方资源、力量和手段，全面落实网上监控处置、防范控制、侦查打击措施，及时发现、封堵和处置涉恐有害信息。三是开展对网上“穿透”工具的集中清理整治，全面清理境内网上“翻墙”软件、VPN等程序的下载链接，强制关闭境内外网络恐怖主义相关代理网站、网页虚拟专网和相关下载链接，依法处理境内网上传播、制售“翻墙”软件工具的网站和人员。加强对提供恐怖音视频客户端软件下载的手机应用网站的打击整治专项行动，及时清理、下架有关软件。四是加强封控处置和管理控制，坚决切断恐怖音视频利用互联网和二手手机市场传播的渠道。建立打击整治长效工作机制，实现“打掉发布源头，切断传播渠道，铲除扩散土壤，消除现实危

害，全力维护网络秩序、净化网络环境，全力维护社会稳定民族团结”的总目标。

3.全面加强情报信息的搜集甄别能力

第一，强化情报信息引领，公安、安全、军事机关在其职责范围内，加强反恐怖主义情报信息搜集工作，对搜集的有关线索、人员、行动类情报信息，因工作需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦查措施。第二，加强对境外即时通信工具的侦控、对暴恐案件涉案电子设备的勘验、对抓获的暴恐极端分子的审查，及时发现获取恐怖音视频情报信息线索，重视对境外涉暴恐网站与应用的技术渗透，及时发现访问、下载恐怖音视频的境内人员等情报信息线索。第三，从网吧、二手手机市场、宗教等重点场所阵地以及涉恐关注群体人员中，发现获取网络恐怖主义音视频情报信息线索。科学针对境外即时通信工具的技术封控，组织技术力量开展情报信息线索的侦控攻关，及时发现并有效切断境外恐怖音视频向境内传播渗透渠道。第四，网络恐怖音视频的传播具有顽固性和再生性，情报信息搜集主要关注五类平台：(1)各种境内网盘、文档分享、视频分享、音乐下载、语音聊天室、即时通信工具、手机音视频APP应用工具、音视频发布网站；(2)微信、QQ等各种即时通信工具及其群组；(3)各种语音聊天平台、搜索引擎和电子邮箱；(4)各种手机音视频工具、手机APP软件和下载链接；(5)境内网站、微博、论坛、贴吧等。

（四）以搭建“网络空间命运共同体”为桥梁，深化推进网络反恐怖主义国际合作

1.把反恐工作深深扎根于人民群众之中，坚决打赢网络反恐人民战争

未来反恐工作不仅要强化打击恐怖主义犯罪，更要防范其宗教极端主义等意识形态领域在网络上对人民群众的无形侵蚀，持续加强技术反制和国际执法合作，坚决打掉境外制作发布恐怖音视频的源头和平台，依法打击网络恐怖主义犯罪活动，以便有效应对全球互联网发展新挑战。建立“专群结合、全民参与”的全社会反恐、防恐常态化工作机制。群众的力量至关重要，只有紧紧依靠群众、发动群众，人民群众广泛参与，才能真正对恐怖活动形成围剿之势，最大限度地将暴恐犯罪摧毁在萌芽状态[22]。第一，宣传典型案例。党政机关及反恐怖职能部门应挑选典型案件，与新闻媒体等部门协作配合开展反恐法治宣传教育。揭批恐怖主义、极端主义的邪恶本质，使人们切实意识到传播、持有暴恐音视频等网络恐怖主义也是严重犯罪行为。第二，宣传方式多样。利用互联网、广播、报纸、电视等媒体渠道和微信、微博、短信等渠道，揭批网络恐怖主义的现实危害性和应承担的法律后果，加强舆论宣传和警示教育，切实增强群众对网络恐怖主义的免疫力。开展法制宣传，通过以案说法、现场讲座、采访法律专家等形式，宣传相关法律责任。第三，完善举报奖励机制。畅通多形式的举报渠道，鼓励群众向网络违法犯罪举报网站、110报警电话、短信报警平台等举报涉恐怖音视频情报信息线索，对举报线索有功人员及时予以奖励。通过宣传发动，提高全民反恐意识，使恐怖分子和恐怖信息在网上无处可藏，形成全社会严打、严治、严防的全民反恐良好氛围。

2.加强国际合作是防范和打击网络恐怖主义的必然要求

目前，国际恐怖主义已进入新一轮活跃期，国内外反恐战场已勾连为一体，极端分子还以“人权”、“宗教”为重心，通过网络媒体大肆攻击我国政府治疆政策。“一带一路”倡议下的反恐国际合作，同样面临着网络恐怖主义的严重威胁与挑战[23]。网络已成为世界各国打击恐怖主义的主战场之一[24]。网络的开放性、跨国性、便捷性决定了网络安全是全球面临的挑战，维护网络安全是国际社会的共同责任。鉴于严峻的网络反恐斗争形势，第51届联合国大会第210号决议提及“各国必须高度重视恐怖分子利用电子产品、有线通信系统与网络工具进行的犯罪行为”。2014年第68届联合国大会通过《联合国反恐战略》，首次将打击网络恐怖主义犯罪写入全球反恐战略框架内容之中。2016年12月，中国国家网信办发布《国家网络空间安全战略》，将维护网络空间安全上升到国家安全的战略高度。特别是大数据背景下网络空间已成为国际反恐战略要地，维护网络安全成为21世纪各国政府维护国家安全的优先目标。联合国安理会2129号决议对成员国打击网络恐怖主义作出了明确规定。通过加强同各国的双边、多边网络安全对话交流和信息沟通，积极参与全球和区域组织网络安全合作，营造良好的网络安全外部环境；深入参与、积极引导网络空间国际规则制定进程。深化在政策法律、技术创新、标准规范、应急响应、关键信息基础设施保护、打击网络犯罪、网

络反恐等领域的国际合作[25]。各国也应在全球治理格局中放眼全局，立足本国国情，采取更具针对性的措施和办法，强化国际联合的反恐机制建设，携手合作[26]。在未来，继续深化网络反恐国际合作，积极与有关国际互联网企业建立合作渠道，促其支持配合开展境外源头打击工作[27]。依法加强网络空间综合治理，加强关键信息基础设施的网络安全防护，科学建立网络安全情报信息统筹机制和规范技术平台开发运用，制定网络安全标准来不断增强网络安全防御能力，确保大数据等核心数据的绝对安全，强化群众预防宣传教育，及时建立反恐情报预警机制[28]。以期实现全方位感知和有效防护，最终做到维护国家网络空间主权安全，全面构建“网络空间命运共同体”。

参考文献：

[1]李淑华.网络安全治理：防范和打击网络恐怖主义的路径选择[J].情报杂志，2017(8)：12-17.

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

[3]皮勇.网络恐怖活动犯罪及其整体法律对策[J].环球法律评论，2013(1)：6-20.

[4]闫雨.我国网络恐怖主义犯罪的立法规制与治理[J].河南师范大学学报(哲学社会科学版)，2019(3)：65-70.

[5]潘新睿.网络恐怖主义犯罪的制裁思路[M].北京：中国法制出版社，2017：236.

[6]谢晓专.叙事、框架与图景：网络恐怖主义威胁研究[J].公安学研究，2018(1)：78-105.

[7]朱永彪，魏月妍，梁忻.网络恐怖主义的发展趋势与应对现状评析[J].江南社会学院学报，2016(3)：25-30.

[8]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.

[9]余丽.关于互联网国家安全的理论探讨[J].国际观察，2018(3)：16-32.

[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(2)：37-44.

[11]隋云雁.受暴恐音视频影响者：不分民族　哪人多在哪作案[EB/OL].中国警察网.2014-07-11/2020-01-17.http://www.cpd.com.cn/n10216060/n10216144/c23887515/content.html.

[12]钟晨赫.恐怖活动案件侦查权研究[D].中国人民公安大学硕士学位论文，2017.

[13]谭佳宁.打击网络恐怖主义的国际法问题研究[D].西南政法大学硕士学位论文，2017.

[14]法制晚报.国信办：暴恐事件与“东伊运”音视频有关[EB/OL].海外网.2014-06-24/2020-01-19.http://china.haiwainet.cn/n/2014/0624/c345646-20779121.html.

[15]李超，周瑛，魏星.基于暗网的反恐情报分析研究[J].情报杂志，2018(6)：10-19.

[16]马国春，石拓.国际涉恐音视频的网络传播及其治理[J].阿拉伯世界研究，2016(1)：108-117.

[17]徐军华.“一带一路”与国际反恐：以国际法为视角[M].北京：法律出版社，2019：186.

[18]李大光.全球化背景下的总体国家安全研究[J].人民论坛·学术前沿，2018(8)：6-19.

[19]王志祥，刘婷.网络恐怖主义犯罪及其法律规制[J].国家检察官学院学报，2016(5)：6-21.

[20]刘军.网络犯罪治理刑事政策研究[M].北京：知识产权出版社，2017：128.

[21]王秀梅，魏星星.打击网络恐怖主义犯罪的法律应对[J].刑法论丛，2018(3)：24-55.

[22]黄志雄.网络空间规则博弈中的“软实力”：近年来国内外网络空间国际法研究综述[J].人大法律评论，2017(3)：236-262.

[23]贾宇，李恒.恐怖活动对“一带一路”倡议实施的威胁评估与对策研究[J].宁夏社会科学，2017(1)：35-43.

[24]陈健，龚晓莺.“一带一路”沿线国家共同应对网络恐怖主义研究[J].新疆社会科学，2017(5)：79-85.

[25]李彦，马冉.网络恐怖主义犯罪国际法治理研究[J].河南财经政法大学学报，2019(1)：147-157.

[26]张吉军.“后伊斯兰国”时代的国际恐怖主义及其治理分析[J].南亚东南亚研究，2019(6)：25-42.

[27]康均心，虞文梁.大数据时代网络恐怖主义的法律应对[J].中州学刊，2015(10)：60-64.

[28]曾粤兴，周兆进.反恐模式：大众参与模式之建构：基于传统反恐模式的反思[J].宁夏社会科学，2015(5)：44-49.

(责任编辑　张　炜)