武漢大學學報(哲学社会科学版)
WUHAN UNIVERSITY JOURNAL (Social Science)
第70卷 第2期 2017年3月
Vol. 70. No. 2 Mar. 2017. 073～084
DOI:10.14086/j.cnki.wujss.2017.02.007

网络时代微恐怖主义及其立法治理

皮 勇 杨森鑫

摘 要：在信息化网络化时代背景下，微恐怖活动滋生蔓延，网络应用改变了微恐怖主义的活动形态，使微恐怖主义具有跨国延展性和灵活的组织性，成为当前恐怖活动的最新组织形态。在微恐怖活动形成的作用因素中，网络环境是其形成发展的主要温床，潜在恐怖活动人员中的重点人物是微恐怖活动的“大脑”。法律手段是应对网络时代微恐怖活动最重要力量，虽然现有立法已经对微恐怖活动形成的要素作出规制，但仍存在立法缺憾。要有效遏制网络时代的微恐怖活动，应当在协调反恐行政法与反恐刑法的基础上，对微恐怖活动的网络生存空间进行立法严控，从立法上防范重点人员并巩固反恐斗争的社会基础，织密防控的法网。

关键词：微恐怖主义；网络时代；作用因素；立法治理；反恐
中图分类号：D922.1;D924.3 **文献标识码**：A **文章编号**：1672-7320(2017)02-0073-12

网络时代恐怖主义由有组织犯罪形态向新的阶段发展，呈现出不同的发展样态。第一种是在国家政权瓦解或控制能力严重削弱的地区，形成以“伊斯兰国”为代表的“建国”模式和以利比亚等国出现的大规模恐怖袭击甚至“军事割据”的模式(Brian Michael Jenkins，2013)；第二种是在国家控制力弱的地区，形成不定期发动有一定规模的有组织恐怖活动的模式，如在相同时间针对一国多个目标发起的大型联动恐怖袭击；第三种是在国家控制力较强的地区，形成地域上分散的、个体或松散团伙式的微恐怖袭击模式，如“独狼”恐怖袭击曾在欧美国家引起极大恐慌。信息化时代背景下，网络行为模式与微恐怖活动相结合是当前恐怖活动的最新组织形态，能制造大量恐怖活动人员及活动，并能有效躲避反恐部门的侦测和打击，对社会持久破坏，一旦当地反恐控制能力削弱，微恐怖活动就会转向前两种形态的恐怖活动。当前我国面临的主要是后两种恐怖活动的威胁，由于反恐部门的严密防控，第二种恐怖活动发生数量较少，而第三种微恐怖活动在部分地区“遍地开花”，使当地社会陷入失控的危险境地。作为第三种恐怖活动的高级形态，网络时代的微恐怖活动危害更大，需要深入研究其特性、形成机理与规制困境，从立法角度寻求微恐怖主义的治理之道。

一、网络时代微恐怖主义的特性

微恐怖主义，又称小规模恐怖主义，其执行者选择的不是最大或最引人注目的行动，而是那些有望成功的行动(法里德·扎卡里亚，2010)。微恐怖活动不仅规模微小，而且组织程度松散、地域分散、活动时间无规律。由于其作案成本低、难以被及时察觉端倪，以致屡屡得手，长此以往形成巨大的规模效应。经过多年的全球反恐斗争，以“基地”为代表的高度组织化的恐怖活动组织被打散，恐怖活动组织开始热衷于不求恐怖活动规模与杀伤效果，只求恐怖活动一次成功率的“简单恐怖活动模式”，微恐怖主义随之兴起。后拉登时

代,“伊斯兰国”异军突起、攻城略地,但近年来在国际社会的联合打击下,其实力大为削弱,逐步采取“化整为零”的活动策略,号召恐怖活动人员在本土实施“圣战”,通过多点爆发的“分包式”恐怖袭击扩张其国际影响力。恐怖活动和恐怖组织的碎片化趋势,使微恐怖主义成为国际社会关注的焦点问题。概言之,微恐怖主义既是一种恐怖活动战略,也是一种恐怖活动的组织形态,其活动轨迹为:第一步利用思想渗透大量培植恐怖活动人员,将大规模恐怖活动转化为个体式、小团伙式的恐怖活动;第二步煽动暴力恐怖活动,在反恐控制力强的地方“遍地开花”,破坏社会稳定;第三步在弱控制地区,组织大规模恐怖袭击,从割据地方最终走向“建国”的模式。在我国,大规模、有组织的暴力恐怖活动较少,而个体式、松散团伙型暴力恐怖活动较多。微恐怖主义的出现,不等于反恐斗争取得胜利或控制住局势,这种无处无时不在、难以根除的微恐怖主义发展态势会造成更广泛的社会恐慌,影响社会稳定的基础。一旦地方反恐控制力削弱,微恐怖活动就会发展成大规模的暴力恐怖袭击。如果不能逆转其组织化趋势,当反恐控制力量进一步削弱时,局势有可能向前述第一种恐怖主义模式发展。

在信息时代背景下,网络化极大延展了微恐怖主义的生命力。恐怖活动重在恐怖主义思想和恐怖情绪的“传递”,在网络应用高度发达之前,微恐怖活动相互间的“联通”以及对社会的“传递”能力有限。而在网络时代,借助于高度发达的互联网、多媒体技术,微恐怖主义的联络、组织能力激增,以网络化的形式在思想和行动上勾连呼应,演化为越来越高的组织化程度。网络时代的微恐怖主义以极快的速度招募大量恐怖活动人员,并借助多方位的宣传手段增强行动的影响力,以排山倒海之势对各国安全造成威胁。网络时代的微恐怖主义已经由一种边缘性或是低层次的反抗,成为主导社会安定的不容小觑的力量(李湛军,2006:2)。与传统恐怖活动相比,网络时代的微恐怖主义具有跨国延展性和灵活的组织性。

(一)网络时代微恐怖主义的跨国延展性

在全球化信息化浪潮的推动下,以互联网为依托,微恐怖活动“外溢效应”明显,跨国性特征突出(梅传强、张永强,2015)。当前网络应用的高度发展,不仅使恐怖主义的宣扬方式日趋多媒体化,而且导致恐怖主义内容信息快速广泛的传播,这些促成了微恐怖主义的跨国延展性。恐怖主义动态画面式的传播比传统平面铅字形态的传播更具视觉冲击力,能够产生更强的恐怖效果(李景治等,2009:43)。不同于传统口口相传式讲述极端思想,网络时代的微恐怖活动大多通过图片、音视频甚至网络游戏等方式宣扬宗教极端思想(Marcus Schulzke,2014),这些音视频渲染效果极强,极大推动了恐怖主义在全球的泛滥。网络媒体特别是网络论坛、即时网络通信的出现丰富了恐怖活动人员之间信息传递、联络交流的方式,也为恐怖主义的国际化发展提供生存空间。互联网开放性、共享性与隐蔽性并存的特性,使其成为恐怖活动组织及人员宣扬恐怖主义思想的理想平台(崔莉,2015),“网上”、“网下”结合的传输渠道使得恐怖主义信息的传播范围极为广泛。利用互联网与现代移动通信技术,恐怖活动组织及其人员可以更快捷、低成本地传递恐怖活动信息,促成了恐怖主义的跨国化发展。可以说,宣扬方式的多媒体性、信息传播的无地域限制性和信息交流活动的即时性,促使微恐怖主义在全球蔓延。

网络技术衍生出更多的恐怖活动人员,在网络环境下,宗教极端思想控制下的分散的个体恐怖活动以整体形象出现,加剧了恐怖主义的国际化进程。微恐怖活动没有所谓的领导层或核心层,其发动由下层兴起,互联网环境为这种自下而上的微恐怖主义创造了便利条件,数量极大的不隶属于任何恐怖组织的潜在极端分子仅仅借助于网络就可以创建各自的“恐怖帝国”,通过发动个体或小规模的恐怖袭击并借助网络进行信息扩散,就能引起全国乃至世界的关注,引发的广泛社会讨论和社会政策的回应反作用于恐怖活动发生地区,形成“越恐越反,越反越恐”的死循环。在封闭的网络空间中,“志趣相投”的极端分子结成小群体,在网络上发泄情绪并相互刺激,促成了极端心理的蔓延和强化(凯斯·R·桑斯坦,2010:65),还能对其他易感人群进行滴灌式的熏陶、渗透,使其在不知不觉中完成恐怖主义思想的洗脑过程,从而使恐怖活动人员遍及全球。由于恐怖主义意识形态上的共通性,“区域割据式”特别是“建国式”恐怖主义会对全球恐怖活动人员产生强大的号召力,如当前 ISIS 吸引了全球 100 多个国家和地区数以万计的宗教极端恐怖活动人员加入(马晓霖,2016),成为吸引全球恐怖势力的“磁场”和恐怖主义放射蔓延

的中心。各国恐怖活动人员在完成所谓“迁徙圣战”以及暴恐训练后，再回流母国实施恐怖活动，加速了微恐怖主义的国际化步伐。

（二）网络时代微恐怖主义的灵活组织性

网络联络和信息沟通的交互性，使得微恐怖活动具有灵活的组织性。网络不仅为微恐怖活动提供高效、低成本的信息传输渠道，也为其进行即时性的组织联络创造了极大便利，是微恐怖活动完成有组织化发展的重要环境条件。不同于传统恐怖活动组织从上而下的思想灌输和命令下达方式，网络恐怖联络活动可以进行即时的、交互式信息沟通，既可以是特定人员之间公开或隐蔽的联络交流、组织策划恐怖活动，也可以是不特定群体内的即时信息互动，能以非典型的组织、策划者的新形式完成恐怖活动的组织。分散的微恐怖活动人员或团伙借助网络可以集腋成裘，逐步发展为成员数量众多、规模巨大、具有较高组织性的恐怖活动组织，为实施恐怖活动创造条件。

网络时代的微恐怖主义组织形式更灵活，很可能造成更严重的危害后果。在后拉登时代，恐怖活动的组织形式从金字塔式转向分散式、多中心的网络形式（周效坤、杨世松，2005：446），“化整为零”实施分散的、小型的恐怖活动成为当今世界恐怖主义的重要特征（张家栋，2011）。松散的组织结构和活动模式使得这类恐怖活动生存能力更强，更容易成功实施突然袭击，并且可以随时调整攻击时间和目标，加大了反恐机构及时应对的难度。网络时代的微恐怖主义具有“聚零为整”、“零整互化”的能力，能使全球分散的微恐怖活动相互协调，形成整体合力。在“圣战”运动碎片化过程中，恐怖活动组织及人员利用互联网传播极端思想，结成跨国、跨地区组织，催生了大量狂热的恐怖活动人员，使得微恐怖活动无时无处不在，并且“来无影、去无踪”。在完成规模化发展的初级形态之后，网络时代的微恐怖主义还有聚合发展的高级形态，即，通过互联网的信息联通和对微恐怖活动的有效组织，将分散的微恐怖活动组织成大规模的恐怖行动。高级形态的微恐怖活动对一些个人或恐怖团伙具有极强的感召作用，能够由中心向外围不断扩散，力量不容小视。

总之，网络时代的微恐怖主义是一种新型的恐怖活动战略，能繁衍滋生大量的恐怖活动人员及活动，组织化程度高，并有跨国化发展的趋向，应引起我国的高度重视。

二、网络时代微恐怖活动形成的作用因素与立法规制现状

在全球法治化的大背景下，微恐怖主义的防治应纳入法治化轨道。法律是国家反恐斗争的基础，治理网络时代的微恐怖主义必须要符合法治化的要求，而法治化的治理也具有极强的宣示作用，能够保证处理过程的合法正义，避免恐怖活动人员反向施暴的可能。法律手段是治理微恐怖活动最重要、最有效的力量，只有建立完善的法律防控机制，才能为打击微恐怖活动提供强有力的保障根基，本文即是在立法治理的视角下探讨微恐怖主义的防控之道。网络时代微恐怖主义的产生是多种因素共同作用的结果，微恐怖活动形成的作用因素是该类活动产生的重要基础，根据其形成机制进行阻断式治理应为立法回应的重点。其中犯罪场理论、情境预防理论、犯罪空间理论等犯罪形成的基础理论均注重犯罪环境、犯罪人、反制力量的作用，这些因素是我们治理的重点。在网络时代微恐怖活动的形成机理中，网络环境、微恐怖活动人员、反恐力量发挥重要作用，虽然我国已有相关立法对上述作用因素进行规制，但仍存在不足。

（一）网络环境的基础支持作用与相关立法

犯罪的发生离不开一定的社会环境，网络环境是微恐怖主义滋生的“温床”。作为传统空间的延伸，网络空间已经成为微恐怖主义喧嚣的场所和传播极端意识形态的平台。网络环境对微恐怖活动的形成起到支持作用，网络应用改变传统恐怖活动层级式的组织结构，使微恐怖活动实现去层级化和交互式信息流通（皮勇，2015），从而为转化易感人群、为分散的微恐怖活动团伙和个人实现有组织化发展提供基础条件。在网络时代微恐怖活动的形成发展链条中，起关键作用的有以下几个因素，且与之相关的立法均存在不足：

第一,“毒源”、“毒路”。所谓“毒源”,是指恐怖活动组织网站或其他传播恐怖主义内容信息的网站,该类网站是恐怖主义信息的制作和传播之源,大多设置在我国境外国家或地区,但能够通过互联网向我国境内传播恐怖主义内容信息。所谓“毒路”,是指访问以上网站的网络通道。为避过我国防火长城系统的拦截,这些网站还开发和提供避绕拦截的“翻墙”软件和计算机程序,使境内人员可以获取这些网站的非法信息。

在铲除“毒源”、“毒路”的立法方面,当前我国《刑法修正案(九)》规定的帮助信息网络犯罪活动罪,有效遏制了为传播恐怖主义内容信息提供技术帮助和支持的行为,但存在条款内容含糊和范围不清的问题。如,该罪规制的是境外犯罪人利用信息网络向境内传播恐怖主义信息还是境内犯罪人向境外获取恐怖主义信息,并不明确,其中获取恐怖主义、极端主义信息的行为是否属于犯罪行为,也缺乏法律依据,在非法持有行为构罪的情况下,主动获取行为反而无法定罪不具合理性。为阻断恐怖主义信息的跨境传输,《反恐怖主义法》第 19 条规定“对互联网上跨境传输的含有恐怖主义、极端主义内容的信息,电信主管部门应当采取技术措施,阻断传播”,但对电信主管部门的责任设置并不符合实际。电信、网信等主管部门属于行政机关,根本不具有采取技术措施以阻断传播的能力,需要依靠网络服务提供者的技术平台才有可能实现阻断传播的目的,该条的规定与现实不符,缺乏可操作性。《网络安全法》也增加了“国家采取措施,监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁”的总括性规定,“对来源于中华人民共和国境外的上述信息,应当通知有关机构采取技术措施和其他必要措施阻断传播”,为防止微恐怖主义的跨境传播提供依据,但却忽略了境内网络用户的主动获取行为,也没有注意到恐怖活动信息传入过程中相关技术工具的支持作用。

第二,“毒网”。所谓“毒网”,是指进行恐怖活动联络、交流的网络平台或网络空间。在我国境内的网络交流平台或即时通信空间中,存在对公众或特定人群散布恐怖主义思想、煽动恐怖活动的网络交流空间,还有封闭性的对潜在恐怖活动人员进行培训、发展组织的网络论坛与网络聊天室等,这些网络平台对发展恐怖活动组织及其成员产生了重要影响。

在治理“毒网”的立法方面,当前缺乏对各种网络交流平台和封闭性交流空间中恐怖活动信息的立法控制,不利于防止利用网络空间宣扬恐怖主义思想、煽动恐怖活动的行为。《刑法修正案(九)》增设非法利用信息网络罪,如果利用信息网络设立用于传授恐怖活动犯罪方法、制作或销售涉恐物品的网站、通讯群组的,可以直接以该罪处理。但该罪的适用范围有限,对于在不以上述目的成立的通讯群组内传播涉恐信息、煽动实施恐怖活动的,能否追究组建网络社区群主的法律责任,相关立法严重滞后。当前恐怖活动组织和人员利用网络社交平台进行大范围、点对点地宣传,公共网络空间受众的不确定性和信息复制传播的快速性使得危害后果更加严重,而《反恐怖主义法》和《网络安全法》均未对利用网络平台实施的宣传、传播、交流恐怖活动信息的行为作出特别规定,立法存在缺陷。

第三,“毒材料”。所谓“毒材料”,是指重要的恐怖主义内容信息材料。近年来暴恐音视频和其他民族分裂主义、宗教极端主义内容材料是我国微恐怖活动及人员暴增的直接诱因,是潜在恐怖活动人员完成自我转化的关键条件,也是恐怖活动组织及人员极力扩散的物品。

在惩治“毒材料”的立法方面,《刑法修正案(九)》规定的非法持有宣扬恐怖主义、极端主义物品罪对恐怖主义信息在境内的传播起到遏制作用,但却无力应对当前涉恐物品大量从境外流入的现实问题。而且,缺乏对走私、贩卖、运输宣扬恐怖主义、极端主义物品等上游行为的法律规制,无法切断整个恐怖活动的供应链,不利于全面全程防控微恐怖活动。虽然《反恐怖主义法》对网络服务提供者规定了提供技术支持和协助等义务,但是当前网络服务提供者主要是通过效率低下的字符匹配和人员识别进行技术协助,对于采用密语、加密技术传递的恐怖主义信息材料,这些措施几乎完全失效。此外,《反恐怖主义法》也没有突出防止传播恐怖主义内容信息的关键性,在当前网络时代背景下,境外恐怖活动组织及人员利用境外网络服务器向我国境内传输恐怖主义内容信息和进行恐怖活动勾连,《反恐怖主义法(草案)》曾设立条款要求将提供互联网服务的设备和客户数据留存在我国境内,对提供技术接口和解密服

务也做出强制性要求，但这些主要的安全防范举措都没有在《反恐怖主义法》中保留。《网络安全法》关于关键信息基础设施的运营者在境内运营中收集的重要数据在境内存储的规定，一定程度上承接了《反恐怖主义法（草案）》的内容，但涵盖的对象范围十分有限，存在立法真空地带。

只有在法律上实现“堵源”、“断路”、“破网”和“除毒”，才有可能消除微恐怖活动滋生的环境，有效遏制网络时代微恐怖活动的发展。

（二）重点潜在微恐怖活动人员的“首脑”作用与相关立法

作为犯罪主体的潜在犯罪人，是犯罪发生作用的基点。目前我国反恐热点地区“精英民族分离化，草根宗教极端化”问题突出，实施分裂破坏活动的主要是小部分立场不坚定的公职人员和知识分子，而实施暴力恐怖活动的主要是小部分宗教极端人员。这部分知识精英利用其较高的社会地位蛊惑煽动民众，不仅不为反恐怖斗争“发声亮剑”，反而为恐怖活动及人员放声辩护；而部分立场不坚定的公职人员表面积极工作，底下搞工作虚化，滋长了恐怖活动人员的嚣张气焰。在我国，宗教极端主义是暴力极端主义的主要根源（Scott Gibbs，2005），极端化的宗教情感是支持恐怖活动的特殊精神力量（钱学文，2013：47），我国反恐焦点地区极端思想的传播全部藉由宗教途径（张弛，2015），地下非法讲经点成为传授极端主义思想的策源地和培植新一代恐怖活动人员的孵化器（何秉松，2013：767）。部分受境外分离主义思潮影响的野阿訇和伊玛目等宗教人员成为草根群众接受恐怖主义思想的主要传送者，而大量底层边缘化的易感人群受恐怖主义内容信息洗脑控制，成为实施恐怖活动的主体力量。我国新疆，特别是南疆地区“学经为荣、上学为耻”的观念泛滥，为极端宗教提供了生存空间。

潜在恐怖活动人员中的重点人物是微恐怖活动的“头脑”和“指挥棒”。境外恐怖活动组织及其头脑人物是微恐怖活动形成的主要诱因，但其对我国境内微恐怖活动的影响是通过恐怖主义信息材料间接进行的，而我国境内的重点潜在恐怖活动人员则能以直接和间接两种形式递进影响其他潜在恐怖活动人员。前述部分立场不坚定的公职人员和知识精英不仅与易感群体具有相同的民族和宗教认同，而且具有较高的社会地位和知识水平，他们善于利用民族、宗教知识和情感，其言论行为更容易被易感人群接受，从而成为底层极端人员的“头脑”，能对微恐怖活动的发动和组织发挥重要的领导作用。如果不控制这些重点潜在恐怖活动人员，就无法摧毁微恐怖活动背后的“智库”，无法从思想理论体系层面掌控反恐斗争的主动权。作为微恐怖活动的“智囊团”，微恐怖活动人员中的重点人物是微恐怖活动形成的主要诱因，微恐怖活动防控的关键节点也应是这些重点人物，而在对微恐怖活动重点人员的规制方面，当前我国的相关立法存在不足。

《刑法修正案（九）》规定了宣扬恐怖主义、极端主义、煽动实施恐怖活动罪，将宣扬煽动者作为刑法处罚的对象，对于部分“两面派”宗教人士、高层知识精英和公职人员的宣扬、煽动行为，符合构罪条件的，可以直接适用该罪处罚。对于尚不构成犯罪的上述潜在重点微恐怖活动人员，《反恐怖主义法》和《网络安全法》却没有因他们的特殊地位而重点提防，虽然《反恐怖主义法》第 33 条规定：“重点目标的管理单位应当对重要岗位人员进行安全背景审查。”但安全背景审查的内容和法律依据并不明确，重点目标的管理单位的范围也不明晰，其能否涵盖行政机关、宗教场所、教育部门等均有待明确。宗教是穆斯林的“精神食粮”，部分“两面派”宗教人士对草根社会具有重大影响，而《反恐怖主义法》仅界定了“恐怖主义”、“恐怖活动人员”，却没有规定“极端主义”、“宗教极端人员”等相关概念，法律制度的不健全促使宗教中部分“极端化”要素的生长，并使被普遍压抑的草根社会，特别是青年群体对这些“极端化”要素产生一种“选择性亲和”，从而强化了恐怖主义进一步蔓延的可能性。对宣传恐怖主义、极端主义的重点人员采取法律措施，从对策学层面上讲是最有效的，不控制这些重点人员，就有可能使其反过来控制普通易感群众。《反恐怖主义法》对参与恐怖活动、极端主义活动情节轻微，尚不构成犯罪的人员规定了帮教措施，对刑满释放但仍具有社会危险性的人可作出安置教育的决定，这些规定均具有保安处分的性质，但对于具有明显的恐怖主义、极端主义倾向、影响力和人身危险性更大的需重点关注的人员，《反恐怖主义法》却缺乏相关的预防性规定。如果不从立法上控制这些重点潜在微恐怖活动人员，限制其通过网络

传播极端主义意识形态的能力,则有可能使其继续向下涓滴渗透,释放"磁吸效应",影响更广泛的社会群体。

(三)反恐力量的制约作用与相关立法

专群结合的反恐力量是控制网络时代微恐怖活动的主要力量。微恐怖活动散落于各地,不会大量聚集,常随意选择攻击的时机和地点以保持进攻的主动性,出其不意的突然性是其关键优势。由于网络时代微恐怖活动的跨国延展性和灵活组织性,以应对恐怖活动组织见长的专业反恐力量受到客观条件的限制,往往不能即时发现和阻止微恐怖活动,特别是隐蔽即时通信、信息加密等技术手段的运用,使得监控网络恐怖活动愈发困难,正是由于微恐怖主义的上述特性,社会公众的支持和配合至关重要。当前我国专门反恐部门的建设进展迅速,《反恐怖主义法》也将专门工作与群众路线相结合作为基本原则,专群结合的反恐怖工作体系日益完善。但是,由于网络时代微恐怖活动灵活的组织性,以上反恐力量仍然不足以对其进行有效防控。《反恐怖主义法》第 7、8、9 条建立了立体条块式的反恐怖主义组织架构,为反恐提供体制和职能方面的保障,但却没有充分调动社会力量参与反恐,特别是在应对网络时代的微恐怖活动以及防止恐怖主义思想的形成和传播上没有调动公众参与,不具有高效性和针对性。我国的反恐怖社会参与力量不足,在揭批恐怖主义思想方面,社会力量的参与有限。《反恐怖主义法》第 17 条中反恐的宣传教育也只到村(居)民委员会层面,缺乏对公众个体参与反恐的规定,这不利于教育引导社会公众正确认识恐怖主义,给恐怖主义在意识形态领域留下宽松的活动空间。

在网络时代背景下,网络服务商、电信运营商等公共信息业务服务单位控制大部分互联网基础设施,既是网络安全的重要一环(Lech J. Janczewski & Andrew M. Colarik,2013:615),又是网络空间的主要共治主体(李源粒,2014)。在防控网络时代微恐怖活动的工作中,如果没有以上单位的协助,反恐部门很难发现和遏制该类微恐怖活动,因此,应当对以上单位规定必要的协助管理的反恐法律责任。网络服务提供者提供服务的行为对网络犯罪的实施起着重要作用(陆旭,2015),《刑法修正案(九)》规定拒不履行信息网络安全管理义务罪、帮助信息网络犯罪活动罪,赋予网络服务提供者相应的刑事责任。网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务,经监管部门责令采取改正措施而拒不改正,致使恐怖主义信息、极端主义信息大量传播的,依照拒不履行信息网络安全管理义务罪追责。明知他人利用信息网络实施恐怖活动犯罪,为其犯罪提供互联网接入等技术支持,或提供支付结算等帮助,情节严重的,依照帮助信息网络犯罪活动罪定罪处罚。网络服务提供者是防控微恐怖活动的重要力量,可以说《刑法修正案(九)》有关网络服务提供者责任的规定,对打破微恐怖活动形成的中间层具有重要意义,但拒不履行信息网络安全管理义务罪的罪状设计并不能提高网络服务提供者维护网络安全的积极性,对网络服务提供者明知是恐怖活动信息而放任传播,但监管部门未发现时如何处理,存在较大争议。《网络安全法》也对网络服务提供者的义务作出规定,网络运营者要履行网络安全保护义务,接受政府和社会公众的监督,承担社会责任。该法第 24 条还规定网络运营者在提供特定服务时,应当要求用户提供真实身份信息,这有利于防止滥用网络实施违法犯罪行为。第 28 条规定了网络运营者支持和协助侦查办案的法律义务,但对支持和协助的内容没有作出具体规定,不利于侦查和追究危害网络安全的微恐怖活动行为。在网络时代微恐怖主义的防控过程中,直接与之发生关系的是网络服务提供者和广大网络用户,特别是网络服务提供者直接管理与微恐怖活动相关的网络空间。由于现有立法没有全面规定网络服务提供者等社会组织和社会公众在反恐工作体系中的作用,对网络时代微恐怖活动的直接管控相对缺失。

网络中的恐怖主义思想是孕育微恐怖主义的不竭动力,遏制恐怖主义思想在互联网环境中的传播是防控微恐怖主义的重要立足点。其中,恐怖活动组织网站及其他传播恐怖活动信息的网站、恐怖活动网络交流空间、恐怖活动信息材料和重点微恐怖活动人员是微恐怖活动形成发展的关键因素,应予以有效控制。反恐力量等制约网络时代微恐怖活动的力量不足,没能形成遏制微恐怖活动发展的格局,需要适应这类新型恐怖活动的特性有针对性地增强反恐能力。只有在识别微恐怖主义形成因素的基础上,

制定针对性的法律对策，建立法律上的“隔离体系”和“免疫系统”，才能有效迎战网络时代微恐怖主义的威胁。

三、网络时代微恐怖活动的立法治理路径

前文分析了网络时代微恐怖活动形成的作用机制，要有效遏制网络时代的微恐怖活动，应当在协调反恐行政法与反恐刑法的基础上，对其关键环节和重点对象采取有力措施，通过完善相关立法干预、阻碍微恐怖活动的形成进程，以全面防控微恐怖活动。

（一）协调好反恐行政法与反恐刑法

法治是反恐的重要指导原则，反恐怖主义必须要根植于法治，从法律角度寻求打击微恐怖主义的新思路和新方法。我国现有治理网络时代微恐怖活动的法律规定主要集中在《反恐怖主义法》、《网络安全法》等反恐行政法和《刑法》中，协调好反恐行政法与反恐刑法的关系是立法应对的前提条件。当前我国已基本形成了以《反恐怖主义法》为主导，以惩治恐怖活动犯罪的刑事立法为保障，以其他相关领域的反恐立法为补充的全方位反恐立法体系，通过前文分析可知，目前我国的立法规定尚不足以应对网络时代微恐怖主义的威胁，需要用一张不断扩大的立法网络来支撑对微恐怖活动的防控，防止出现“法外反恐”以及微恐怖主义的应对措施脱离法治轨道的问题。

《反恐怖主义法》是防范和惩治恐怖活动的基本法律和综合性立法，为治理微恐怖活动提供法律依据。《反恐怖主义法》涵盖事前预防、事中应对处置和事后恢复以及其他必要的组织法和保障法内容，将反恐工作的各个环节予以规范化，是防范和惩治恐怖活动的专门法。该法除一般性的规定外，还设有安全防范、情报信息、应对处置等专章，为防控恐怖活动提供全面的法律指导。在治理网络时代微恐怖活动的过程中，要充分发挥《反恐怖主义法》的核心和基础作用，填补其法制漏洞，为防控微恐怖活动提供坚实的法律支撑。作为维护网络安全的专门法律，《网络安全法》在网络时代微恐怖活动的治理中同样发挥重要作用。《网络安全法》是网络安全领域的特别法，是保障网络安全的管理法和防控网络危害行为的预防法，该法从基本性制度、网络运行安全保障制度、监测预警与应急处置制度等方面构建了较为完整、科学的网络安全保障体系，为应对网络时代的微恐怖主义提供法律支持。由于网络时代的微恐怖主义是在网络环境下滋生的，也正因为网络化的组织结构，微恐怖主义具备跨国延展性和灵活组织性，成为国家安全的重大威胁，所以对其的治理可以适用《网络安全法》的相关规定。

作为惩治恐怖活动的保障法，《刑法》只有在反恐行政法不足以治理恐怖活动时才发挥作用。《刑法修正案（九）》大幅度改革了以往粗线条的反恐罪名体系，增加和修正了涉恐的罪名条款。虽然《刑法》是惩治恐怖活动犯罪的有效手段，通过剥夺恐怖活动人员再犯的能力或直接消灭恐怖活动人员等，能够起到较好的反恐效果，但是刑事打击只是暂时性地缓解了“病痛”，并不能彻底根除“病灶”。由于恐怖活动人员思想的极端性，其可以牺牲自己及亲人的生命进行自杀式的恐怖袭击（杨森鑫，2016），不可能因为受到刑法惩罚而放弃实施恐怖活动犯罪。所以刑事立法只能作为保障法，而无法在整个恐怖活动的治理链条中起主导作用，确立恐怖活动犯罪刑事立法的保障地位，对织密反恐的法网具有重要意义。

协调好反恐刑法与反恐行政法的关系，是应对网络时代微恐怖主义的重中之重。刑法是防控恐怖主义犯罪的最后一道防线（师维，2012），刑事、军事手段作为打击严重犯罪的最后手段，作用十分有限，对恐怖活动的治理还需依赖政治和行政的手段。与国外相比，我国网络法治化进程缓慢，目前网络的治理主要依赖于国务院颁布的管理条例，这些互联网管理的法规条例层级低，内容方面多为原则性规定，并非针对恐怖活动行为而设置，其法律应对措施和责任条款的作用有限。《反恐怖主义法》的出台一定程度上弥补了反恐行政立法效力不足的问题，其“法律责任”一章的规定也为恐怖活动行为人行刑责任的对接提供依据，《网络安全法》中也有与《反恐怖主义法》、《刑法》相对接的内容，如该法中网络运营者安全保护义务、技术支持协助义务的规定就与《反恐怖主义法》、《刑法修正案（九）》对网络服务提供者责任条款的规定有机衔接。当然，当前行刑立法之间仍存在不协调之处，如，《反恐怖主义法》对“恐怖活动”

行为类型的界定就没有与《刑法》的规定相对应,这使得追究恐怖活动行为的行政责任无法与刑事责任协调统一,对此需要进行立法修正。在网络时代微恐怖活动的防控中,实现反恐行政法与刑法的衔接与有序过渡,是全面防控和惩治微恐怖活动的重要一环。

(二)对微恐怖活动网络生存空间进行立法严控

网络环境既可以被微恐怖活动行为人所利用,也可以作为遏制微恐怖主义的重要节点,而网络环境的治理必须有相关的法律支撑。前文分析了网络时代微恐怖活动形成的关键环节,"堵源"、"断路"、"破网"和"除毒"是防控微恐怖主义的有效对策,应在这些方面采取强有力的法律措施。

第一,"堵源"、"断路"。我国应采取有效的法律措施阻断恐怖活动组织网站和传播恐怖主义内容信息的网站向我国境内传播非法信息。目前我国对境内网络信息的管控力度大,利用境内网络传播涉恐信息困难,使用境外服务终端传递恐怖主义信息成为新趋势。由于境外网络服务终端不受我国境内网络主管部门的管控,加上相关人员通常运用加密手段传递恐怖主义信息,防控境外恐怖主义信息的流入难度极大。在现有立法规制物态信息传递的同时,对于动态层面的信息流动也应纳入规制范围。上文分析到《刑法修正案(九)》帮助信息网络犯罪活动罪对境内网络用户主动获取境外涉恐信息的行为规定模糊,应在帮助信息网络犯罪活动罪的相关司法解释中明确,无论是明知境外犯罪人利用信息网络向境内传播恐怖主义信息还是境内犯罪人向境外获取恐怖主义信息,为其提供技术支持和帮助的,均应构成该罪。

前文分析到,境外涉恐网站是我国境内恐怖主义内容信息的重要来源,而我国《反恐怖主义法》"安全防范"章却没有禁止访问境外涉恐网站的规定,而且还删除了草案中网络服务提供者预设技术接口、将密码方案报送审查、用户数据留存境内的条款,这不仅与我国恐怖活动发展的国际化趋势不符,而且也无法有效回应网络时代的微恐怖活动。应在《反恐怖主义法》第 19 条第 2 款中补充规定,境内网络用户禁止访问境外宣扬恐怖主义、极端主义的网站,禁止制作、传播、使用避绕、破坏电信、互联网主管部门阻断境外恐怖主义、极端主义内容信息的技术措施和工具或者提供技术帮助。根据上文提到的《网络安全法》的问题,并使之与《反恐怖主义法》的内容相衔接,应在第 50 条增设一款规定,境内网络用户不得访问境外宣扬恐怖主义的网站、下载宣扬恐怖主义的信息,不得传播、持有宣扬恐怖主义的材料。只有从源头入手,才能更好地防控网络时代的微恐怖活动。

第二,"破网"。要加强对各种网络交流平台和封闭性交流空间中恐怖活动信息的立法控制,防止利用网络空间宣扬恐怖主义思想、煽动恐怖活动。目前我国在"破网"方面主要依靠网络服务提供者的字符识别和物态空间的人员协助,但存在字符经技术处理或暗语替代后无法识别及效率不高的问题。当前恐怖活动组织成员使用"暗网"进行勾连①,加密信息和网络聊天室的私密性增加了安全机关侦破的难度。网络服务提供者是网络平台的实际控制者和监管者,必须在《网络安全法》和《反恐怖主义法》中增强网络服务提供者对网络平台的监管责任,控制网络社交平台和封闭性网络空间中恐怖活动信息的流通,使网络平台和网络空间成为信息时代的"稳定器"。

《反恐怖主义法》中还应明确规定社交平台群主的行政责任,实现网络平台发起人刑事责任与行政责任的有效衔接。即使群主没有在该特定网络社区中发出倡议或鼓动实施恐怖活动,也应追究其不报告恐怖活动的法律责任,若其明知他人在利用其组织的网络社区进行恐怖活动而没有进行拦阻、剔除或者解散该网络社区的,应追究其疏于管理的法律责任。网络时代微恐怖活动在发展到大规模事件前,会有明显的临事表象,如果能果断采取干预措施,是可能将恐怖事件遏制在萌芽阶段的。我国《反恐怖主义法》"应对处置"一章应规定恐怖事件风险评估和预警机制,一旦恐怖事件发生的危险处于较高级别时,立即启动临事应对处置预案。

---

①"暗网"特指互联网上数量庞大的"隐身"网站,网站内容被网络工具隐藏,用户可在网站上匿名交流。参见环球网:"联合国:警惕极端组织使用'暗网'进行联络",http://world.huanqiu.com/hot/2016-08/9330611.html,2016 年 12 月 20 日最后访问。

第三，“除毒”。恐怖主义的实质是思想意识的传递，网络环境为恐怖活动组织及人员传播恐怖主义内容信息提供便利，清除互联网环境中的恐怖主义内容信息是防止恐怖主义思想向易感人群渗透的重要举措。要重点清除暴恐音视频及其他具有强烈煽动作用的宣传材料，当前大量“自杀式”恐怖袭击人员就是受这些材料的影响完成“自我转化”和“洗脑”的（皮勇、杨淼鑫，2015）。虽然近年来我国加大了对“三非”活动的管控力度，但利用手机、暴恐音视频进行“自教育”、分散传播的现象仍十分严重，这些宣传材料大多来自境外涉恐网站，清除从境外流入的宣扬恐怖主义、极端主义的物品尤为必要。

目前我国的涉恐物品大多是隐藏在移动硬盘等不易被海关查处的电子设备中走私入境，由于这些涉恐物品并非普通的货物物品，按照走私普通货物、物品罪定罪并不合适，而且相关贩卖、运输行为并无适当的罪名可以适用。在非法持有行为入罪的情形下，缺乏对走私、贩卖、运输等上游行为的规制，将无法切断整个恐怖活动的供应链。应在《刑法修正案（九）》非法持有宣扬恐怖主义、极端主义物品罪之前增设走私、贩卖、运输宣扬恐怖主义、极端主义物品罪，以切断整个“毒材料”的产业链。《反恐怖主义法》第 19 条赋予网络服务提供者发现含有恐怖主义内容信息，停止传输、删除信息等作为义务，违反义务的可根据该法第 84 条的规定处罚，实现了《反恐怖主义法》与《刑法》的有机衔接。此外，为阻断恐怖活动信息材料的传播，还应在《反恐怖主义法》中规定，在我国境内提供电信业务、互联网服务的，应将相关设备、境内用户数据留存在我国境内。拒不留存的，不得在我国境内提供服务。

（三）从立法上防范重点潜在微恐怖活动人员

重点人员对网络时代微恐怖活动的形成起关键作用，控制此类重点人员是防控微恐怖活动的关键。这些重点人员主要是前文分析过的对煽动恐怖活动作用大的人员，包括部分野阿訇、“骑墙派”宗教人士、立场不坚定的公职人员和知识精英，他们以直接或间接、公开或隐秘的方式宣扬分裂主义、极端主义和恐怖主义思想，煽动实施恐怖活动。由于立法欠缺等原因，我国对上述人员的处置往往大事化小、小事化了，但这类人员越来越嚣张，甚至敢在宗教活动场所、课堂以及其他开放场所公开宣扬极端主义、恐怖主义思想。由于这类人员的长期宣扬煽动，我国部分地区特定民族的民众对国家、民族的认同感显著下降，这样的“土壤”中孕育出数量庞大的“独狼式”恐怖活动人员，其走向团伙化、组织化是必然。要改变这种结果，关键要控制该类重点人员，尤其是能直接向公众散布恐怖活动信息的人员，如网络焦点人员、具有较高社会地位的高校教师和公职人员等，加强对这些重要岗位人员的背景审查，防止其凭借有利地位成为宣扬恐怖主义的精神领袖。对于重点的潜在微恐怖活动行为人，特别是具有较强影响力的“网络大 V”，应设立类似国外危险人员的保安处分措施，对符合一定条件的重点危险人员实施网络通信管制，限制其上网的权利，并将适用于该类危险人员的管制措施正当化、法治化。

前文指出，由于互联网上存在恐怖主义相关信息，易感群体受非法信息的影响后可能转化为“独狼式”暴恐人员，由于初犯者存在心理障碍，其更多的是通过组成恐怖活动团伙来实施恐怖活动。通常这种恐怖活动团伙或组织在熟人中形成，网络社区的兴起，为素未谋面的陌生人组成恐怖活动团伙或组织创造条件，且该种组织更难被侦测。利用互联网发展微恐怖活动团伙或组织有两种方式：第一种是利用互联网组织他人实施恐怖活动或协调多个恐怖组织的活动，组织者或联络人只是将网络作为一种共同联络的技术手段；第二种是具有相似心态的潜在恐怖活动人员在网络空间的交流中，以忽发且未经沟通却被认可的意图或称“闪客意志”的形式，组成恐怖活动团伙并以各自分散的行动在同一时间和地点共同实施恐怖活动。由于互联网联络的广泛性，第二种形式可能汇聚较大数量的恐怖活动人员，如聚集多人对关键信息系统发动网络攻击等。对于第一种情形，应重点控制在网络空间中发挥组织和协调作用的关键人员，通过对其严厉惩治以警诫潜在的恐怖活动人员，同时搜索该关键人员联络群体的恐怖活动发展情况。对于第二种情形，由于没有传统有组织犯罪意义上的组织、领导者，即使能查明“倡议”的提出者，也难以按照传统共同犯罪的规定将其认定为组织犯或主犯。

笔者认为，对于已经实施恐怖活动的个体，不论人数多寡，都应以恐怖活动犯罪认定，若存在共同犯罪故意的，按照共同犯罪论处，若不能证明存在共同犯罪故意的，应按照同时犯各自定罪处罚。同时，为

防止发生这种“闪客”形式的恐怖活动,应将法律介入的时间提前,将发起讨论恐怖主义内容的网络社区、组织他人参加该社区讨论的人员作为关键人员,采取必要的法律措施。此外,还应顺应网络时代微恐怖活动的发展,完善我国刑法中有组织犯罪的规定。网络时代的微恐怖主义是一种网络“聚众性”犯罪,恐怖团伙或个人在网络上传播极端思想、提出犯罪计划,其他人自愿加入进行集体形式的犯罪(皮勇,2004)。该种情况下犯罪人之间不存在传统有组织犯罪的组织结构和意思联络,但鉴于该行为严重的社会危害性,应考虑发展共同犯罪理论,扩展有组织犯罪的立法规定,或将其作为一种新的共同犯罪形态单独规定处罚条款。

(四)从立法上巩固反恐斗争的社会基础

一方面,要通过立法保障社会公众成为反恐的中坚力量。社会公众是应对微恐怖活动的主力军,除持续以跨部门力量遏阻恐怖主义的威胁外,亦要充分发挥社会公众在反恐中的重要作用(Seth G. Jones, 2012)。美国在反恐中常面临这样的疑问“我们每天捉拿、杀死或劝止的恐怖分子比部分宗教学校和激进神职人员招募、培训和部署对付我们的恐怖分子多吗?”(埃里克·施密特、汤姆·尚卡尔,2015:41)恐怖组织通过网络输出极端主义意识形态,这些极端意识形态像癌细胞一样在世界各地扩散。“野火烧不尽,春风吹又生”,消灭恐怖分子并不能最终解决问题,只要有极端主义意识形态的存在,毙命的恐怖分子就会被新的恐怖分子取而代之。极端主义思想是恐怖分子的精神鸦片,麻痹着恐怖分子的神经,从意识形态领域封堵极端主义思想的产生之源是应对微恐怖活动的核心环节,而社会公众是意识形态领域反恐的中流砥柱。

只有确立社会公众在意识形态领域反恐中的法律地位,使其积极主动地参与到反恐的宣传教育、情报收集以及协助配合中,团结和扶持爱国的少数民族力量,分化和打击具有分裂倾向的人员和顽固分子,才能筑牢防控微恐怖活动的铜墙铁壁。有关部门应当主导并发动社会力量在互联网等媒介上正面宣传国家的反恐政策,使易感人群在网络上能够获得足够的正面信息,抵御“三股势力”的思想渗透和控制。如前文所述,《反恐怖主义法》规定了政府部门、企事业单位、村(居)民委员会在反恐工作中的作用,但却缺乏社会公众参与反恐的规定,这对社会公众主动参与应对微恐怖活动极为不利。应在《反恐怖主义法》第 8 条中规定,社会组织特别是网络服务提供者、社会公众是反恐工作的主体,只有肯定公众和社会单位的反恐主体身份,才能真正从制度上保障全民反恐、全面反恐战略的落实。

另一方面,要明确网络服务提供者的法律责任,使之成为反恐的基础力量。网络服务提供者是网络社会的控制者和管理者,需要对其设定全面的协助管理义务,否则国家将失去治理网络社会的必要基础。通过前文我国立法现状的分析可知,当前我国对网络服务提供者法律责任的设置不全面,需要进一步增强网络服务提供者对严重恐怖活动的防控责任,对于有涉恐可能性的通讯大群组、可能会诱发大规模恐怖袭击的信息,网络服务提供者应主动搜索或配合相关部门进行技术搜查。除《反恐怖主义法》规定的网络服务提供者的责任外,结合网络时代微恐怖活动的特点,网络服务提供者至少还应承担以下反恐责任:一是,对涉嫌从事与恐怖活动相关的网络空间进行监控,主动发现、报告、拦阻可能会诱发严重恐怖活动的相关信息;二是,支持社会公众利用其系统发布揭批恐怖主义的正面信息;三是,不发布传输与反恐工作相背离的不利信息,如渲染暴力恐怖场面、宣扬恐怖主义思想的信息等。

不可否认的是,法律手段仅是治理网络时代微恐怖活动的一个维度,防控恐怖主义是一场综合性的较量(王逸舟,2010:15),需要运用多种手段进行全方位治理。只有利用刑事司法体系,辅以情报机构,必要时加上军队,才能在反恐和尽可能少地危害相关权利间达成恰当的平衡(奥德丽·库尔思·克罗宁、詹姆斯·M·卢德斯,2015:132)。但反恐的基石是法治,有效的反恐对策必须得到法律支撑,并通过法治的手段落实。当前我国立法不健全是应对网络时代微恐怖主义的短板,在微恐怖主义的防控中,应建立完善的法律壁垒,对微恐怖主义威胁作出有针对性的立法应对,以力争从社会肌理中清除微恐怖主义这一痼疾。

参考文献：

[1] 崔　莉(2015). 打击本土恐怖主义任重道远. 解放军报,2015-01-16.

[2] 何秉松(2013). 后拉登时代国际反恐斗争的基本态势和战略(上). 北京：中国民主法制出版社.

[3] [美]奥德丽·库尔思·克罗宁、詹姆斯·M·卢德斯(2015). 反恐大战略：美国如何打击恐怖主义. 胡溦等译. 北京：新华出版社.

[4] 李景治、宫玉涛、刘元玲(2009). 反恐战争与世界格局的发展变化. 北京：当代世界出版社.

[5] 李源粒(2014). 网络安全与平台服务商的刑事责任. 法学论坛,6.

[6] 李湛军(2006). 恐怖主义与国际治理. 北京：中国经济出版社.

[7] 陆　旭(2015). 网络服务提供者的刑事责任及展开——兼评《刑法修正案(九)》的相关规定. 法治研究,6.

[8] 马晓霖(2016). 斋月攻势多点爆发 伊斯兰国全球"分包"恐袭. 华夏时报,2016-07-11.

[9] 梅传强、张永强(2015). 我国恐怖活动犯罪的现状、特征及防控对策. 北京师范大学学报(社会科学版),6.

[10] 皮　勇(2004). 论网络"聚众"性犯罪及其刑事立法. 人民检察,2.

[11] 皮　勇(2015). 全球化信息化背景下我国网络恐怖活动及其犯罪立法研究——兼评我国《刑法修正案(九)(草案)》和《反恐怖主义法(草案)》相关反恐条款. 政法论丛,1.

[12] 皮　勇、杨淼鑫(2015). 论煽动恐怖活动的犯罪化——兼评《刑法修正案(九)(草案)》相关条款. 法律科学,3.

[13] 钱学文(2013). 中东恐怖主义研究. 北京：时事出版社.

[14] [美]凯斯·R·桑斯坦(2010). 极端的人群：群体行为的心理学. 尹宏毅、郭彬彬译. 北京：新华出版社.

[15] [美]埃里克·施密特、汤姆·尚卡尔(2015). 反恐秘密战：美国如何打击"基地"组织. 洪漫译. 北京：新华出版社.

[16] 师　维(2012). 反恐刑法的基本理念及立法完善研究. 河北法学,7.

[17] 王逸舟(2010). 恐怖主义溯源. 北京：社会科学文献出版社.

[18] 杨淼鑫(2016). 论恐怖活动特殊关系人"连带责任"的追究——俄罗斯经验与中国路径. 青海社会科学,3.

[19] 法里德·扎卡里亚(2010). 微恐怖主义的一年. 时代周刊,2010-12-27.

[20] 张　弛(2015). 解密暴恐分子生成路径. 凤凰周刊,4.

[21] 张家栋(2011). 从英国骚乱看恐怖主义的发展趋势. 学习月刊,19.

[22] 周效坤、杨世松(2005). 信息反恐论. 北京：军事科学出版社.

[23] Scott Gibbs(2005). Islam and Islamic Extremism: An Existential Analysis. *Journal of Humanistic Psychology*,45(2).

[24] Lech J. Janczewski & Andrew M. Colarik(2013). 赛博战与赛博恐怖主义. 陈泽茂、刘吉强等译. 北京：电子工业出版社.

[25] Brian Michael Jenkins(2013). The Role of Terrorism and Terror in Syria's Civil War. *RAND Testimony*,2013-11-20.

[26] Seth G. Jones(2012). The Future of Irregular Warfare. *RAND Testimony*,2012-03-27.

[27] Marcus Schulzke(2014). Simulating Terrorism and Insurgency: Video Games in the War of Ideas. *Cambridge Review of International Affairs*,27(4).

Research on Micro-Terrorism and Its Legislative Measures in the Age of Network

Pi Yong & Yang Miaoxin (Wuhan University)

Abstract: At present, large-scale and organized terrorist activities are difficult to implement due to the tight control against terrorist organizations by the anti-terrorism departments of various countries. Individual or loosely organized micro-terrorist activities become the latest strategy and latest form of terrorist activities. Under the background of globalization and network era, the combination with network makes micro-terrorism transnationally extended and flexibly organized. Micro-terrorism becomes a threat to national security that should not be underestimated. The main topics to be discussed in this paper are: What is Micro-Terrorism? What are the characteristics of micro-terrorism in the Internet age? How is micro-terrorism formed in the age of network, and how to regulate it through legislation?

This paper analyzes and defines micro-terrorism and its characteristics in the Internet age. Micro-terrorism, also

known as small-scale terrorism, with loose organization, geographical dispersion and irregular hour. It is the latest form of terrorist activities. Compared with the traditional terrorist activities, micro-terrorist activities in the Internet age, with the help of highly developed Internet and multimedia technologies, shows a trend of strict organizations and transnational extension. Our country should take measures against micro-terrorism, among which the legal means is the most important and effective one. Only by establishing perfect legal prevention and controlling mechanism can we provide strong foundation for combating micro-terrorism. This article is to discuss the prevention and control of micro-terrorism from the perspective of legislative governance.

A lot of factors result in the generation of micro-terrorism in the Internet age. However, blocking the resources according to its forming mechanism should be the key. The basic theories of the crime formation are focusing on the physical settings, offenders and the role of counter-force in a crime, and these factors are the key points of our governance. In the formation mechanism of micro-terrorist activities, the network environment, micro-terrorist activities personnel and anti-terrorism forces play important roles. Although relevant regulations are already in existence, more efforts are needed to tackle the following specific problems: First of all, the network environment plays a supporting role in the formation of micro-terrorism. However, the legislative provisions against "toxic sources", "toxic materials" and crime-related processes are incomprehensive or inadequate. What's more, some potential terrorists who play a leading role in terrorist crime are out of touch by the existing provisions. Last but not least, counter-terrorism forces are major constraints toward such crime, provisions of anti-terrorism liability of the public and Internet service providers are inadequate.

The main conclusion of this paper is that, effective measures to the key links and key objects should be taken in order to curb the micro-terrorist activities effectively in the Internet age. In addition, relevant provisions should be perfected to hinder the formation of micro-terrorist activities process, basis on the coordination of administrative law and criminal law against terrorism. Firstly, it is important to balance between the application of administrative law and criminal law against terrorism to achieve the convergence and transition of the administrative law (mainly anti-terrorism law) and criminal law; Secondly, provisions as "blocking source", "open circuit", "broken network" and "detoxification" aimed at breaking the network environment of micro-terrorism should be carried out; Thirdly, it is necessary to distinguish potential micro-terrorists personnel from the beginning and especially prevent religious leaders, intellectual elites and public officials becoming spiritual leaders in the promotion of terrorism by virtue of their advantage. Lastly, it is essential to consolidate the social foundation of anti-terrorism by legislation, for example promoting the public the backbone of anti-terrorism and making clear of the legal responsibility of network service provider so as to make them the basis of anti-terrorism forces.

The innovations of this article mainly display in the following aspects: In the first place, the concept of micro-terrorism is introduced and the characteristics of micro-terrorism in the Internet age are systematically expounded. In the second place, a comprehensive analysis of the factors for the formation of micro-terrorist activities in the Internet age is conducted. What's more, current situation and difficulties in legislation are clarified according to the provisions of the 9th Amendment of Criminal Law, the Anti-Terrorism Law and the Network Security Law. In the third place, the target of the paper is to seek for the governance path of micro-terrorism in the Internet age from the perspective of legislation, to be more specific, to make the governance of micro-terrorism into the rule of law track, with the hope of providing legislative guidance for combating micro-terrorism in the network era.

Key words: micro-terrorism; the age of network; affective factors; legislative measures; anti-terrorist

■**收稿日期**:2016-06-01

■**作者地址**:皮 勇,武汉大学法学院;湖北 武汉 430072。Email:fxypy@whu.edu.cn。
杨淼鑫,武汉大学法学院;湖北 武汉 430072。Email:yangmiaoxin90@126.com。

■**基金项目**:国家社会科学基金重点项目(13AFX010);武汉大学马克昌法学基金会重大项目(MJ2012A01);湖北法治发展战略研究院重点项目(FZFZYJ2012012)

■**责任编辑**:李 媛