网络恐怖活动犯罪及其整体法律对策*

皮　勇

内容提要:信息时代的到来,也使基于恐怖主义目的而使用互联网的网络恐怖主义得以产生,它具有网络化、国际化、信息化等新特征,是具有更大影响力和破坏力的综合形式的恐怖活动类型,给国际社会和各国带来新的严峻挑战。目前打击网络恐怖活动的对策包括技术、法律、思想宣传、公共政策等多个方面。其中的法律对策至少应有打击网络恐怖活动的预防与控制法、刑事程序法和犯罪法三个部分,预防与控制网络恐怖活动的立法是关于甄别、发现、介入干预和紧急情况下控制网络恐怖活动的相关措施立法,相关犯罪法和程序法由网络犯罪和恐怖活动犯罪的刑事立法组成。近年来国际社会和各国对打击网络恐怖犯罪的立法都在不断完善发展中,本文通过比较研究国际国内打击网络恐怖活动犯罪的刑事立法,进而分析了反网络恐怖活动犯罪的立法现状和未来发展。

关键词:网络恐怖　预防与控制法　刑事立法　公共政策　网络犯罪

皮勇,新疆大学法学院教授。

21 世纪人类文明进入信息社会,网络化成为社会生活的重要特征,一种新的恐怖主义——网络恐怖主义在网络社会环境中产生,它借助互联网将国际性、区域性和国家范围的恐怖活动融为一种超越疆域限制的新型恐怖活动形式,借助于被广泛应用和依赖的信息基础设施和机电一体化设备设施将恐怖活动和思想渗透融为一体,是全球化、信息化的社会背景下具有更大影响力和破坏力的综合形式的恐怖活动类型,给各国和国际社会带来新的严峻挑战。[1] 为了有效应对网络恐怖活动的挑战,有必要研究这一新型恐怖活动现象并探索有效的对策。

一　网络恐怖活动的界定

根据研究的科学性要求,研究网络恐怖活动,首先应确定其上位概念"恐怖主义"的内涵。从文义上看,恐怖主义是一种意识形态或者思想理论,但是目前国际社会相关立法采用"恐怖主义"这一术语表达的却是"恐怖活动"的概念。目前国际社会未能就"恐怖主义"的

* 本文得到教育部"新世纪优秀人才支持计划"、中南财经政法大学法治发展与司法改革研究中心重点项目"网络恐怖活动犯罪的整体法律对策"资助。

〔1〕 See Ulrich Sieber, "The Threat of Cybercrime", in Council of Europe (ed.), *Organized Crime in Europe*, Strasbourg 2005, pp. 212 – 218.

定义采取一致的立场。虽然欧洲理事会2002/2008年《打击恐怖主义框架决议》规定了恐怖主义和恐怖活动犯罪的范围,但在联合国成员国范围内还没有形成一致的观点。从1934年开始国际联盟已经在讨论防止和惩罚恐怖活动的公约草案,该公约虽然在1937年获得通过,但未正式生效。自1963年起,联合国共通过了13个制止恐怖行为的国际公约,比如《制止恐怖主义爆炸事件的国际公约》、《制止向恐怖主义提供资助的国际公约》、《制止核恐怖主义行为国际公约》等。2006年、2008年、2010年联合国大会先后通过了三份《联合国全球反恐战略》决议,目前联合国成员国也正在就关于制定反对国际恐怖主义的全面公约草案进行协商。虽然反恐国际立法稳步发展,但作为立法基础的恐怖主义定义问题仍然未能解决。因此,国际社会仅能在前述13个公约的范围内就恐怖主义的定义形成基本一致,不同地区、国家对本地区和本国范围内的恐怖活动制定不同的法律,如欧盟、美国、俄罗斯和我国对恐怖活动的范围都采取了有同有别的立场。

其实,还可以通过对比恐怖活动与一般的有组织暴力活动的特征,来理解恐怖主义的涵义。一般的有组织犯罪谋求的是经济利益或者其他非政治上的目的,只是希望在现行社会组织体中实现其活动目的。而恐怖活动虽然近年来有谋取经济利益的趋势,但它的政治或社会目的的特征从未消除,反而主动追求恐怖后果的进一步扩大化、极端化,以有利其最终政治或社会目的的实现,[2]恐怖暴力活动及关联活动只是其犯罪手段和方法。因此,恐怖活动的政治或社会目的则成为恐怖活动区别于一般的有组织暴力犯罪的构成特征。

网络恐怖活动是指与网络和恐怖活动相关的一系列活动,关于其具体内涵与外延,国际社会也未达成一致的看法,不仅是因为国际社会对恐怖主义的定义存在分歧,还因为不同国家和国际组织对网络恐怖活动的性质的认识也存在分歧。

美国联邦调查局官员认为,网络恐怖活动是非政府团体或者秘密组织实施的有预谋的、有政治动机的针对信息、计算机系统、计算机程序和数据的袭击,引起对非战斗目标的暴力活动。[3] 这种观点将网络恐怖活动限定在网络恐怖袭击的范围内,并将其与暴力型恐怖活动直接联系。

德国刑法学教授乌·西伯尔(Ulrich Sieber)认为,对"网络恐怖主义"的界定可以采取两种方法,一种是恐怖活动分子利用互联网实现了什么?另一种是互联网给恐怖活动分子什么特别的能力?[4] 他采取前者,将网络恐怖活动界定为出于恐怖主义目的使用互联网的三类行为,包括利用互联网对计算机系统实施破坏性攻击、通过互联网向公众传播非法内容,以及以计算机为基础进行策划与支援恐怖活动的其他行为。[5]

联合国反恐任务实施力量工作组(CTITF,下文简称"联合国工作组")将网络恐怖主义界定为四类行为,即:(1)利用互联网通过远程改变计算机系统上的信息或者干扰计算机系统之间的数据通信以实施恐怖袭击;(2)为了恐怖活动的目的将互联网作为其信息资源进行使用;(3)将使用互联网作为散布与恐怖活动目的有关信息的手段;(4)为了支持用于追求或支持恐怖活动目的的联络和组织网络而使用互联网。[6]该界定中增加了"为了恐怖活

---

〔2〕 参见刘玉燕:《中国政府恐怖主义危机管理问题研究》,北京师范大学出版社2011年版,第1页。

〔3〕 See Mark M. Pollitt, "Cyberterrorism: Fact or Fancy?" *Proceedings of the 20th National Information Systems Security Conference*, October 1997, pp. 285 – 289.

〔4〕 See Ulrich Sieber, *Cyber-terrorism-The Use of the Internet for Terrorist Purposes*, 2008, Council of Europe.

〔5〕 See Ulrich Sieber, International Cooperation against Terrorist Use of Internet, in Revue Internationale de Droit Penal, 3e/4e trimesters (2006), S. 399.

〔6〕 See United Nations Counter-Terrorism Implementation Task Force Working Group, *Report* on *Countering the Use of the Internet for Terrorist Purposes*, 2009, p. 5.

动的目的将互联网作为其信息资源进行使用”的一类行为,其理由是,他们采纳的定义与网络资源的关系更密切,更符合打击网络恐怖活动的需要。

对网络恐怖活动范围的界定,应反映恐怖活动的实质,符合现有法律规定,并适合研究目的的需要。前述美国对网络恐怖活动的定义,是将网络犯罪和暴力恐怖活动犯罪进行组合,袭击信息、计算机系统、计算机程序和数据是暴力恐怖活动犯罪的犯罪方法或手段。这一定义不符合当前国际社会的反恐立法,也有违国际社会对恐怖主义的基本立场。虽然目前国际社会没有对恐怖主义的定义形成统一的认识,但获得国际社会广泛认同的是,恐怖主义不是一种意识观念,而是以暴力活动为主要行为方式来实现特定的政治或社会目的的行为,恐怖活动组织和人员的终极目的不是暴力行为本身造成的结果而是通过暴力活动向广大公众传递恐吓信息来实现。[7] 把恐怖活动狭隘地理解为暴力活动本身,有违国际社会对恐怖主义实质的共识和立法,前述国际公约规定的恐怖活动犯罪没有止于暴力恐怖活动的范围。造成物理损害的暴力恐怖活动只是恐怖活动中的一种而不是全部,在恐怖分子的暴力活动之前,都会有一系列的社会性的而不只是物理意义上的事件或者活动,[8]“网络恐怖主义”不应局限在网络恐怖袭击的范围内。

西伯尔的观点和联合国工作组的观点分别是从网络恐怖活动犯罪立法和网络恐怖活动的对策两个角度作出的界定。本文的研究不仅要讨论网络恐怖活动犯罪立法,更要将网络恐怖活动作为一种犯罪学意义上的犯罪现象进行对策学的研究,且重点是相关整体法律对策,因此,本文采纳联合国工作组对网络恐怖活动的界定,即,网络恐怖活动是基于恐怖活动目的使用互联网的活动,它包括网络恐怖袭击、利用互联网传播恐怖活动相关非法信息、利用互联网进行恐怖活动联络和资助恐怖活动和利用互联网收集信息和获取技术支持四类活动。

二 信息社会环境下网络恐怖活动及其应对

现代意义上的恐怖活动不仅转向“既让更多的人死,也让更多的人看”式的扩大化、极端化的行事方式,而且,全球化、信息化的发展也为其扩张创造了条件,“传统意义上的恐怖主义如今借助于现代化环境的孕育,已经由一种边缘性或是低层次的社会反抗,一下子成为了具有能主导社会安全与稳定的一种不可小视的能量。”[9] 网络恐怖活动具有网络化、国际化、信息化等新特征,给国际社会和各国反恐斗争提出了新的挑战。

(一) 网络恐怖袭击

网络恐怖袭击是指利用多种计算机、网络技术通过互联网对计算机系统、数据进行破坏性攻击而实施的恐怖袭击。[10] 那些造成互联网大范围中断、关键计算机系统受到攻击,有造成极严重破坏后果和危险的,可以认为是网络恐怖袭击。

目前网络恐怖袭击有两类。第一类是针对关涉到国计民生的控制关键设施的袭击,诸

---

〔7〕 See United Nations Counter-Terrorism Implementation Task Force Working Group, *Report on Countering the Use of the Internet for Terrorist Purposes*, p. 2.

〔8〕 See Max Taylor and John Horgan, “A Conceptual Framework for Addressing Psychological Process in the Development of the Terrorist”, *Terrorism and Political Violence*, 18 (2006).

〔9〕 参见李湛军:《恐怖主义与国际治理》,中国经济出版社 2006 年版,第 2 页。

〔10〕 参见 U. Sieber and P. Brunst, eds., *Cyberterrorism and Other Use of the Internet for Terrorist Purposes*, Council of Europe, 2007, pp. 12 – 21; C. Foltz, “Cyberterrorism, Computer Crime, and Reality”, *Information Management & Computer Security*, 15. 3. 2004, Vol. 12, pp. 154 – 166; U. Sieber, The Threat of Cybercrime, pp. 173 – 175。

如高速铁路、金融中心、核电站核设施、水坝等的计算机控制系统，一旦出事会直接给国家安全、社会公众安全造成严重危害。在这类案件中，最典型的是2007年爱沙尼亚事件，该次网络袭击影响了爱沙尼亚的新闻网站和银行的金融服务，造成广泛的恐慌。[11] 另一类是以整个互联网为目标进行的网络袭击，它可以通过袭击互联网域名管理系统来进行。一般来说，运行在13个相互独立的根服务器上的域名管理系统本身是极为抗破坏的，近期有安全专家发现，这类服务器仍然隐藏着脆弱性，如对请求IP地址的路由服务器系统的攻击可使其难以迅速恢复。此外，使用破坏力巨大的计算机病毒也能对互联网上的计算机系统进行攻击。[12]

在网络恐怖袭击中，黑客技术和计算机病毒技术起着关键作用。有些恐怖分子使用其他黑客同样的非法侵入工具包，例如计算机病毒程序、特洛伊木马程序、网络蠕虫程序、网络侦测软件、间谍软件、键盘记录程序、网络安全分析器等，非法侵入目标计算机系统并实施后续的攻击。还有一些恐怖活动分子不是采用高技术手段，而仅是利用内部工作人员的身份来完成恐怖袭击。抵御黑客非法侵入，需要不断完善计算机系统的安全防护、提升安全管理，但进攻与防御始终处于主动与被动状态，尤其是对于内部人员作案，就更加难以杜绝。网络恐怖袭击的另一种常用但又难以控制的方法，是使用僵尸病毒发动网络攻击：恐怖活动分子利用僵尸病毒程序感染并控制数量巨大的计算机系统，利用这些受控制的计算机系统发动拒绝服务攻击。由于发起攻击的是无辜的受控制的计算机系统，且难以追踪背后的控制者，使得控制此类网络恐怖袭击活动和处罚犯罪都很困难。更为糟糕的是，互联网上出现了僵尸网络租赁者，恐怖活动分子不需要自己建立或者拥有发动袭击的僵尸网络，可以很容易地以每小时200－300美元的价格向网络犯罪分子非法租赁，他们要做的只是设定攻击目标，就可以完成恐怖袭击，这样一来，即使是很穷的恐怖组织也能使用这种攻击方法。[13]

值得注意的是，网络恐怖袭击和网络犯罪的界线似乎越来越模糊了，二者使用犯罪方法和造成恐慌后果的细微差别仅在于网络恐怖袭击的目标范围有别于普通网络犯罪，后者偏向于谋求经济利益。虽然在一国法域内将网络恐怖袭击按照网络犯罪进行惩处没有法律障碍，但在处理跨国网络恐怖袭击案件时，就会遇到引渡条件的限制问题。

（二）利用互联网传播恐怖活动信息

前文谈到，恐怖活动本质上是信息的传递、沟通，相比借助于传统的有形媒体传递信息的方式，利用互联网传递信息具有广泛性和快速性、直接影响受众、交互性等优势，因此，在互联网产生后不久，就被恐怖活动分子用于传播非法信息，并形成了恐怖活动组织的新公众媒体策略。目前利用互联网传播恐怖活动相关非法信息发展出六类行为：（1）威胁实施恐怖活动犯罪；（2）煽动、宣传、美化以及合法化恐怖主义；（3）训练恐怖分子；（4）招募恐怖分子；（5）恐怖主义募资与融资；（6）散布种族主义和仇外主义材料，否认、支持或者为种族灭绝寻找正当借口。[14] 以上行为虽然都只是散布信息，但其危害不亚于暴力形式的恐怖行为，它们有的是暴力恐怖行为的准备、动员和组织，甚至本身（如威胁行为）就是恐怖活动，

---

〔11〕 Tikk, Kaska and Vihul, "International Cyber Incidents: Legal Considerations", *NATO CCD COE*, 2010, p. 18 et. seq; Ashmore, "Impact of Alleged Russia Cyber Attacks", *Baltic Security & Defence Review*, Vol. 11, 2009, p. 8 et seq.

〔12〕 Tikk, Kaska and Vihul, "International Cyber Incidents: Legal Considerations", p. 18 et. seq; Ashmore, "Impact of Alleged Russia Cyber Attacks", p. 8 et seq.

〔13〕 See "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", *A Report of the U. S. Congressional Research Service*, January 2008, http://www.fas.org/sgp/crs/terror/RL32114.pdf.

〔14〕 See Ulrich Sieber, International Cooperation against Terrorist Use of Internet, S. 413.

它们与暴力恐怖袭击一样能造成公众的恐慌心理。

从利用互联网传播非法信息的发展规模和组织方式看,自 20 世纪 90 年代末期“基地”组织建立第一个网站向公众宣传其观念起,随后 10 年里恐怖组织的网站数量超过 5000 个,所有大的恐怖组织都建立了网站。同时,这些网站上所发布信息的质量和复杂程度也在提升,2002 年“基地”组织的媒体发布网站上还只有 6 个音视频文件,到 2007 年就增加到近百个。在信息交流方式上,也由单一的信息推送转变为信息交流互动。随着各国强化对互联网网站的管理,许多恐怖组织通过精心设计的逐级强化控制的金字塔公告栏论坛系统动态发布信息,恐怖组织对网上交流者进行审查筛选,被选中的人转入更高层次的、更具保密性的交流空间。虽然各国都在强化互联网管理,但互联网上的恐怖活动相关非法信息并没有得到有效的控制,其原因是互联网的特性有利于隐藏信息发布者的身份,在追踪信息来源时,最多只能查出信息发出的 IP 地址,进而查到某地的某台计算机系统,而要查到具体发布人,还要知道什么人什么时候登陆电脑,可是,这个登陆信息因为备份空间的限制不会保留太长时间,如果没有建立用户实名上网制度,侦查人员往往查到发信息的网络设备后就难以再继续下去了。利用互联网的这一特性,恐怖分子可以利用匿名的网络咖啡店、不安全的无线接入点、通过被侵入的计算机系统来隐藏起真实地址信息,以及利用代理服务器、移动网络服务、云计算服务等来隐匿发布者的真实身份,使得追查他们的踪迹几乎是不可能的。

在应对互联网上的恐怖活动相关非法信息问题上,移除非法信息或者拦截访问是包括我国在内的一些国家的作法,在一国法域范围内这种方法是可行的和合法的,但这种方法难以解决跨国性非法信息流动问题,且容易引起国际法律争端。我国采取了“防火长城”系统建立对包括恐怖活动相关非法信息进行拦截的防火墙系统,同时要求互联网服务商协助管理经由其处理的互联网信息。虽然这些措施能阻止访问较广范围的不法信息,但互联网天生具有抵御控制的技术特性,效果并不好。另外,快速变动主机技术的广泛使用使得国家机关拦截访问恐怖活动相关信息或者其他恶意内容变得几乎不可能。这些方法的采用代价是巨大的,不仅国家在拦截和过滤内容信息上投入巨大,而且使网络服务商负担沉重,严重限制了公众对互联网的正常使用,还带来一系列隐私和人权问题。衡量打击恐怖活动犯罪措施的效果和付出的代价,以上措施实在不是恰当的对策。因此,许多国家更愿意采用监视恐怖分子在线活动的方法,并将其用于情报和司法活动。

(三)利用互联网进行恐怖活动联络和资助恐怖活动

1. 利用互联网进行恐怖活动联络

互联网在本质上是信息交互的平台,交互式信息沟通方法更多地被用于进行暴力恐怖活动的联络活动。为了进行恐怖活动而组建的网络社区,包括论坛、网站、社交网络系统中的特定群等等,实际上是恐怖组织的组织平台,而互联网的特性使这一平台的运作实现了低成本、高便利、多功能,对暴力恐怖活动的进行有明显的支持帮助作用。

暴力恐怖活动一旦实施,无论其是否造成人员伤亡或伤亡数量的多少,都会给社会造成恐慌,摧毁社会安宁心理,影响社会稳定,因此,各国对利用互联网联络恐怖活动都在进行侦查和遏制。不过,现代信息安全技术的发展和民用化,使得恐怖活动分子也能使用诸如密码技术等来掩饰、隐蔽其网络联络活动,并且使用的密码技术越来越复杂和先进,密码长度增加到 256 位,使用了这种高级加密技术的信息凭现有计算机技术进行强行破解几乎没有成功的可能。同时,恐怖分子也在使用诸如多重加密技术的其他数据加密技术进行通信。恐怖分子一般不相信商业加密软件,而使用可以检查其中是否存在“后门”的开放数据源的加

密程序,[15]有些恐怖组织也自己制作使用加密软件。

除了密码技术外,信息隐藏技术也被恐怖分子用于互联网通信联络,它可以将袭击计划隐藏在各种计算机文件中,而使侦查者不知道哪些是藏密文件而不会去检测。信息隐藏技术与加密技术不同,加密技术可以通过解密技术解决,但目前还没有破解信息隐藏技术的方法。还有,由于互联网上存在海量的信息和通信联络,在互联网上恐怖分子有足够多的地方来隐匿,而司法机关对这些隐藏信息的搜索随着信息量的迅速增加变得越来越失去实际效用。从整体上看,司法机关采取的技术措施在效果上是非常有限的。

2. 利用互联网资助恐怖活动

利用互联网支持恐怖活动的另外一种重要活动,是为恐怖活动募集活动资金和转移资金。互联网的应用为恐怖分子筹集、使用和藏匿钱财提供了新的方法,恐怖分子不仅从电子商务中赚取钱财,也在其商业网站上设立接受捐赠的链接,许多恐怖组织还以所谓慈善组织的名义募捐资金,但实际用于暴力恐怖活动。目前智能移动电话中的软件服务也成为恐怖组织募集资金的新方法,利用广泛的移动电话客户群和手机金融服务等优势,恐怖组织隐秘地获取大量资金。此外,恐怖分子还利用网络信用卡诈骗、身份诈骗和通信诈骗获取资金来支持其活动。网络金融系统更是为恐怖分子洗钱和转移资金提供了极大的便利,其方式方法有多种,例如利用网络赌博洗钱、使用不记名的全球范围内可用的储值卡、使用手机支付系统等。

这些新的资金筹集和流转方法,对侦查机关而言既是挑战也是机遇,一方面侦查机关可从互联网中获取更多的恐怖活动组织资金活动的线索,但另一方面有些新的支付和流转方式不在正常的金融网络系统内,也给金融网络管理体系提出了新的要求。

(四)利用互联网收集信息和获取技术支持

互联网上大量的公共信息和私人信息给恐怖分子收集信息提供了很大的便利,阿富汗的"基地"组织训练手册中曾建议恐怖分子利用公共资源而不是采取非法手段收集信息,它至少可以获得所需信息的80%,[16]恐怖分子从互联网上能收集到诸如大使及其家属的私人背景资料、居住地址、家庭关系和社交关系等,为其制定恐怖袭击计划提供关键信息。互联网还是恐怖活动分子收集犯罪方法、掌握犯罪工具的资料库,通过互联网能收集到各种有关制造毒物毒气、爆炸物、使用枪械、地雷进行暗杀等信息,有些恐怖组织网站还为恐怖袭击者提供训练,教授如何制定实施破坏活动、绑架人质和杀人的计划,堪称"虚拟的恐怖活动分子训练营"或"恐怖活动分子大学"。

互联网上的信息和技术应用还为实施恐怖活动提供了技术和物力支持。谷歌地图就在多起恐怖袭击中被恐怖活动分子使用。互联网上的地下信用卡信息交易市场也成为恐怖活动分子青睐的场所,恐怖活动分子从此类网上黑市购买信用卡信息,然后用于为恐怖组织活动购买装备。

互联网上的信息、技术等可以为所有人得到,包括恐怖分子,在这些信息和技术中,有些是合法的使用,如谷歌地图应用、手持GPS定位仪、网上合法公开的公共单位和私人的信息等,对于恐怖分子使用这些信息和应用技术的,没有也不可能采取限制性措施。不仅是因为缺乏合理、合法的依据,而且是因为以上技术应用很容易被其他互联网应用所替代,从而对其使用进行限制难以取得实际的控制效果。反恐部门唯有适应互联网应用的发展,提升自

---

〔15〕 这些"后门"设置可以帮助侦查机关迅速识别恐怖活动分子和解密信息。

〔16〕 See"Dot-Com Terrorism",*The New Atlantis*,Spring 2004,pp. 91 – 93,http://www. thenewatlantis. com/publications/dot-com-terrorism,访问时间:2012年12月24日。

身技术对抗能力,以更大更强的侦查能力来对恐怖活动的新发展进行反平衡。至于诸如网络信用卡信息黑市、病毒等破坏性信息工具市场等有害信息和技术应用,由于其存在本身就是违法的,执法机关应对这些非法信息和技术应用的"地下市场"进行取缔。当然,这一举措并非是针对网络恐怖活动犯罪的专门对策,而是对控制包括网络恐怖活动在内的各类网络犯罪都有积极作用的一般性的犯罪控制对策。

(五)打击网络恐怖活动犯罪的其他挑战

网络恐怖活动与网络犯罪具有诸多共同的客观特征,因此,恐怖活动分子能利用网络犯罪实施网络恐怖活动。另外,目前各国都存在大量的网络犯罪组织,犯罪人乐意将其技术能力和服务卖给出价最高者,这样一来恐怖组织不需要有自己的技术人员和设备就能获得网络恐怖活动所需的高级技术能力,突破网络安全防范,避开追踪和侦查。由于网络恐怖活动与网络犯罪之间的共生关系,打击网络恐怖活动的对策中应当包含遏制网络犯罪人非法提供技术信息的内容。因此,遏制网络犯罪遇到的各种挑战,也成为打击网络恐怖活动的挑战。

目前新兴技术以指数性速度发展,且有发展不平衡及运用广泛的趋势。如机器人技术,可以预见在不远的未来,与网络技术结合的机器人技术几乎肯定会成为恐怖分子的攻击工具,其造成的破坏力更大而控制的难度更高。打击网络恐怖活动必将遇到这些技术应用所带来的挑战,反恐部门应当未雨绸缪、尽早防范。

三 打击网络恐怖活动的整体法律对策

在恐怖主义产生的根源短时间内无法消除,而正确有效的反恐战略、社会政策尚未发挥出作用前,打击网络恐怖活动的对策只可能是治标的,针对恐怖活动和恐怖分子的对抗性的策略,[17]是对网络恐怖活动的滋生发展进行介入式的遏制对策。这些遏制对策的目标是将网络恐怖活动造成的危害控制在一定限度之内,为反恐斗争背景环境的改变和反恐基本对策发挥作用争取时间。基于此,所采取的控制对策应当是包含技术、法律、思想宣传、公共政策等多方面的综合性对策。

其原因首先在于,法律对策和技术对策都发挥着重要作用。技术对抗措施是遏制网络恐怖活动的基础和保障,没有强有力的技术措施,就不可能有效预防、发现和阻止网络恐怖活动。但是,技术不是打击恐怖主义的万灵药,技术反制措施应当体现在适当的法律框架内。技术对抗措施如果脱离法律的框架,则不仅难以取得遏制网络恐怖活动的正面效果,反而会出现负面结果。其次,舆论宣传对策也对反恐发挥着积极作用。网络恐怖活动在信息传播和联络方面的能量极大,揭露、批驳恐怖组织宣传的思想意识,进行反制性的思想和舆论宣传,对削弱网络恐怖活动的消极影响具有重要作用。最后,与互联网管理相关的公共政策。目前组成互联网的信息基础设施大部分掌握在提供各类互联网服务的网络服务商手中,它们实际管理着互联网,对互联网运行和社会安全具有实际的影响力,需要他们在维护互联网安全与秩序中担当起社会责任。国家机关有必要与网络服务商合作,共同管理互联网,以实现对网络恐怖活动的有效控制。另外,在互联网社会中广大网络用户不仅是信息的

〔17〕 参见王逸舟等:《恐怖主义溯源》,社会科学文献出版社 2010 年版,第 15 - 16 页。

接收者,也是各种网络社交社区的参与者,应动员社会力量来发现、监控网络恐怖活动。[18]

根据前述打击网络恐怖活动的基本对策制定的法律对策,至少应包括打击网络恐怖活动的预防与控制法、刑事程序法和犯罪法三个部分。这里要强调打击网络恐怖活动的预防与控制法,原因是:(1)暴力恐怖活动犯罪一旦发生就难以控制,后果极为严重。而且,恐怖活动犯罪不同于普通刑事犯罪,事后刑事处罚产生的预防效果不佳,反而有利于恐怖分子进一步扩散有害信息。因此,从对策学的角度看,应在恐怖活动初露端倪时及时发现、尽早介入。(2)网络恐怖活动利用互联网等信息技术,具有更强的隐蔽性、反侦查性和更大的社会危害性,采取有效的预防与控制措施比事后采取措施效果更好。(3)网络恐怖活动兼有暴力、宣传煽动、组织联络、帮助支持等活动内容,需要对这些行为采取提前识别、介入干预和截断清除等预防控制措施,并以立法的形式确定下来,作为打击网络恐怖活动法律体系的重要组成部分。另外,恐怖活动犯罪是具有跨国性特征的国际犯罪,研究网络恐怖活动的法律对策,不能局限于一国立法的视野范围内,而应与国际反对网络恐怖主义立法相一致;还要考虑与网络犯罪立法等现有立法之间的关系,构建起协调、有效的打击网络恐怖活动犯罪的法律体系。

(一)网络恐怖活动犯罪的预防与控制法

预防和控制网络恐怖活动犯罪的国际公约目前仅有欧洲理事会的《防止恐怖主义公约》,它规定了13个与反恐有关的国际公约规定的恐怖主义范围的四类犯罪,即公然煽动实施恐怖主义罪、招募恐怖活动分子罪、训练恐怖活动分子罪和附属犯罪。由于前述13个公约规定的主要是暴力恐怖活动犯罪,欧洲理事会《防止恐怖主义公约》规定以上四罪的确可以起到预防和制止后续暴力恐怖活动犯罪的作用,同时,也要看到,该公约设立以上四罪后,实际上也扩大了恐怖活动犯罪的范围,使这四罪成为恐怖活动犯罪立法中的一部分,欧洲理事会2008年《打击恐怖主义框架决议》也将以上四罪吸纳为恐怖活动犯罪。

这里研究的网络恐怖活动犯罪的预防与控制立法,主要是与甄别、发现、介入干预和截断、阻止网络恐怖活动措施相关的立法。关于这方面的内容,还没有形成国际法律文件,但已经有国家提议,在国际层面上采纳一项措施,通过制定国际法为互联网提供商设定识别其托管的网站所有者的义务,并要求网络服务商不向被认定为参与了恐怖活动的个人和组织提供网络服务。[19] 有一些国家已经制定了这方面的规定,如根据英国2006年《恐怖主义法》的规定,英国警察可以向那些为恐怖活动相关非法信息提供主机服务的人提出披露通知,要求其在两周内移除或者改变内容。其他一些国家也在采取类似的做法,但没有要求网络服务商主动过滤恐怖活动相关非法信息,是因为存在法律的障碍以及使网络服务者负担过重的商业成本,这也是欧洲理事会相关决议的基本立场。[20] 相关的甄别、发现等措施都限于国家有权机关依职权行使。此外,国外还有保留数据的规定。

我国较早就开始制定互联网管理法规,国务院颁布的《互联网信息服务管理办法》及《计算机信息网络国际联网管理暂行规定实施办法》、信息产业部、公安部、文化部、国家工商行政管理局联合颁布的《互联网上网服务营业场所管理办法》、信息产业部颁布的《互联

---

〔18〕 See United Nations Counter-Terrorism Implementation Task Force Working Group, *Report on Countering the Use of the Internet for Terrorist Purposes*, pp. 21 – 22.

〔19〕 See United Nations Counter-Terrorism Implementation Task Force Working Group, *Report on Countering the Use of the Internet for Terrorist Purposes*, p. 12.

〔20〕 See the "Commission Staff Working Document: Accompanying Document to the Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on Combating Terrorism".

网电子公告服务管理规定》等行政规章都规定了提供网络服务者不得传播有害信息,还规定了网络服务提供者有记录和保留通信往来数据和内容信息的义务。

我国有关网络服务提供者不传播有害信息的规定,与英国的《反恐怖主义法》的相关规定相似,都是阻止恐怖活动相关非法信息在网络上散布的制度,它使得相关的网络服务提供者有义务参与预防和控制网络恐怖活动。如果没有这一法律义务,国家机关将在控制网络恐怖活动中疲于奔命,且难以取得有效的控制效果。不过,目前我国的相关规定还比较原则,没有针对不同种类的网络信息服务提供者制定不同的管理规定,对不执行或者不严格执行拦阻非法信息义务的,没有规定具体的处罚措施,这使得预防控制网络恐怖活动的整体效果打了折扣。另外,对于网络接入服务和平台服务的网络服务提供者的法律义务不够明确,主要原因在于网络通信数据量达到海量程度,网络接入服务和平台服务提供者实际上根本无法履行其相关义务,这样做有可能会影响公众正常使用互联网,不利于国家信息化发展,但是,如果不对他们规定特定情况下过滤、拦阻、截断义务,则可能使恐怖分子轻易地利用网络服务进行网络恐怖活动。目前我国还没有规定紧急情况下网络服务提供者的特殊协助义务,这明显不利于预防和控制网络恐怖活动犯罪,因此,有必要对不同种类的网络服务提供者设定相应的社会责任立法,尤其对新型网络服务如移动互联网服务提供者等规定特别的法律义务,并对紧急情况下规定非常态的网络控制法。

我国有关网络服务提供者记录和保存与其服务相关的通信往来数据或内容信息的规定,不是用于预防或控制网络恐怖活动等犯罪,但却对案发后调查和发现恐怖犯罪至关重要。该法规对不同种类的网络服务者规定不同的协助义务。网络信息服务提供者被要求记录保存已提供或系统发布的信息内容及其发布时间、互联网地址或者域名等内容数据和往来信息,而网络连接服务提供者只被要求记录和保存上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等往来信息。网络服务提供者的法定义务为记录信息、保存信息并备份一定时间,并在国家有关机关依法查询时予以提供。虽然记录和保留信息制度给网络服务提供者增加了一定的经营成本,但它却是控制和处罚网络恐怖活动犯罪所必要的。与欧盟的相关规定相比,我国的规定使网络服务提供者的负担更重,同时,大量公众的信息被记录和保留,却没有配套的保护公众个人数据的法律出台,存在国家全面监控网络社会活动、侵犯公众通信自由和通信秘密权的隐忧。

因此,打击网络恐怖活动的预防和控制法引起了对人权保障的担忧,美国《爱国者法》、英国《反恐怖主义法》和欧洲反恐怖主义立法实施以来,人权倡议者一直在反对其中有关监控、扣押方面的特别规定,如何处理好打击网络恐怖活动和保障人权的关系,是我国制定反网络恐怖活动预防与控制立法必须考虑的问题。在风险社会和信息社会环境下,人们在享有前所未有的自由和便利的同时,也面临包括恐怖活动犯罪在内的更严重的安全威胁,它不同于应对传统社会环境中普通犯罪,肩负维护社会安全和保障公民权利双重任务的法律必然要适应现代社会环境下的新挑战,以实现维护安全和权利保障的平衡发展。在恐怖活动犯罪的严重威胁下,相关立法应贯彻优先保护社会公共安全兼顾保障公民人权和自由的原则。因此,原则上前述反恐立法中的特别措施是正当和必要的,应对网络恐怖活动犯罪的预防和控制法也是如此。但是,在公共安全优先兼顾保障人权的原则下,反恐措施的选择和使用上也应体现平衡保护公共安全和保障人权两方面的需要,并非凡是对反恐有积极作用的措施都可以不加选择、不分情况地使用。由于现代信息技术支撑的侦查措施等特别侦查手段对广大公众的权利可能造成严重侵犯,其使用必须考虑公众权益受损的代价与反恐效率和效果的平衡,要遵循反恐措施选择上的效率优先原则和紧急情况下特别对待原则,具体而

言:应区别常态和紧急情况下的预防与控制恐怖活动措施的选择和使用,在非紧急情况下,如果有多种反恐措施可以选择,不得选择效率低下或侵犯公民权利严重的措施;在紧急情况下,允许使用包括强制性反恐措施在内的各类措施。对于网络恐怖活动犯罪而言,不仅其预防和控制法,而且在后面要谈到的犯罪法和刑事程序法中,都应体现常态立法和紧急情况立法的不同,平衡反恐需要与保障人权的关系。

(二)网络恐怖活动犯罪相关刑事程序立法

网络恐怖活动犯罪不仅给犯罪的预防和控制、刑事实体法立法带来新问题,也给该类犯罪的侦查、追诉、引渡等提出了新的挑战。应对这一新挑战的国际法律规范分为二类。第一类是打击网络犯罪的国际法律文件中的刑事程序立法;第二类是打击恐怖活动犯罪的国际法律文件中的刑事程序立法。

第一类规制网络犯罪的刑事程序立法,联合国层面上还没有相关国际法律文件,不过,欧洲理事会2001年就通过了《网络犯罪公约》,明确规定适用于网络犯罪的调查电子数据证据的特别程序,包括快速保护静态的计算机数据、提供令、搜查和扣押静态计算机数据和实时收集计算机数据4种刑事调查措施。[21] 2006年欧洲议会和欧盟理事会还通过了《关于与可公共获取的电子通信服务或者公共通信网络的连接中产生或者处理的数据的保留并修改Directive 2002/58欧盟指令》的2006/24欧盟指令,规定有关欧盟范围内公共电子通信服务中数据的保留措施。我国刑事诉讼法对网络犯罪的特殊规定较少,直到2012年3月14日通过的新《刑事诉讼法》才开始以法律形式明确电子数据的证据地位,并规定调查网络犯罪的特别侦查措施,但仍然没有规定网络犯罪相关的电子数据证据的认证规则。不过,"两高"和公安部在此前已陆续颁布了收集、认定电子数据证据的司法解释和规定。

从规范功能的角度比较,我国法律法规和司法解释与欧洲《网络犯罪公约》和欧盟指令的相关规定具有相似性,尤其是在电子数据证据的提交、实时收集计算机数据证据、扣押电子数据证据等方面基本上达到一致,只在电子数据证据的快速保护方面还有较大的差别。但是,目前我国的规定多为行政法规、规章、司法解释,内容零散,配套措施缺乏,不成体系,法律效力弱,操作性不强,特别是明显存在重打击犯罪而轻公民权利保护的缺陷。[22]

第二类规制恐怖犯罪的刑事程序立法,联合国《制止向恐怖主义提供资助国际公约》第8条规定,缔约国应根据其本国法律原则,采取适当措施,以便识别、侦查、冻结、扣押、没收用于实施或调拨该公约第2条规定罪行的任何资金以及犯罪所得收益。相似的规定还有联合国《打击跨国有组织犯罪公约》。欧洲理事会《清洗、搜查、扣押、没收犯罪收益和为恐怖主义提供资金公约》规定了关于没收、调查、冻结、扣押的具体措施以及预防性措施。在恐怖活动犯罪的引渡方面,联合国和欧洲的反恐公约都有涉及。以上国际公约规定的刑事程序立法没有限制恐怖活动犯罪的犯罪手段,故同样可以适用于网络恐怖活动犯罪。我国新《刑事诉讼法》规定了五个方面10个针对恐怖活动犯罪的法条,这些规定当然可以适用于网络恐怖活动犯罪。这些法条涉及的内容包括:(1)案件管辖。第20条规定,"中级人民法院管辖下列第一审刑事案件:(一)危害国家安全、恐怖活动案件";(2)证据调查。第62条规定了保护证人、鉴定人和被害人作证的规定,要求人民法院、人民检察院和公安机关必须为作证的证人、鉴定人和被害人采取规定的必要保护措施;(3)强制措施。第73条规定对

〔21〕 参见皮勇:《〈网络犯罪公约〉中的证据调查制度与我国相关刑事程序法比较》,《中国法学》2003年第4期。

〔22〕 参见皮勇:《新刑事诉讼法实施后我国网络犯罪相关刑事程序立法的新发展》,《法学评论》2012年第6期。

涉嫌恐怖活动犯罪的犯罪人,即使其有固定住处,也可以在指定的居所执行监视居住;第 83 条关于刑事拘留后的通知制度的规定,对涉嫌恐怖活动犯罪的犯罪嫌疑人采取刑事拘留措施后,可以在有碍侦查的情形消失以后再通知其家属;(4)技术侦查措施。第 148 条 - 第 152 条规定了对恐怖活动犯罪可以依法采取技术侦查措施,取得的材料在刑事诉讼中可以作为证据使用,为打击网络恐怖活动犯罪提供了强有力的法律武器;(5)没收违法所得。第 280 条规定了没收逃匿、死亡的涉嫌恐怖活动犯罪的犯罪嫌疑人的违法所得及其他涉案财产的特别程序。以上规定大多将恐怖活动犯罪与危害国家安全犯罪并列规定,反映我国恐怖活动犯罪具有严重危害性和与国家安全的密切联系的特点,也表明刑事诉讼法在应对此类特别严重的犯罪中,考虑到打击犯罪与保障人权并重的平衡。[23]

虽然已经有了以上打击网络恐怖活动犯罪的国内国际刑事程序立法,但由于网络技术等信息科技不断发展并被用于恐怖活动犯罪,一些国际组织如欧洲理事会已在研究设立新的刑事调查措施如秘密在线搜查措施,国际社会打击网络恐怖活动犯罪的刑事程序立法仍在不断发展中。

(三)网络恐怖活动相关犯罪法

网络恐怖活动犯罪立法主要来源于恐怖活动犯罪立法和网络犯罪立法,以及制定专门的反网络恐怖活动的立法。这三种立法模式和立法文件之间的协调也是一个新的立法问题。下面就一些主要的涉及网络恐怖活动犯罪的立法进行分析。

1. 打击网络恐怖犯罪的刑事实体法

针对网络恐怖犯罪的国际立法分为两类:一类是关于网络犯罪的国际立法,主要是欧洲理事会《网络犯罪公约》;另一类是关于恐怖活动犯罪的国际立法,其中既有欧洲的反恐公约,也有联合国反恐公约。

欧洲理事会《网络犯罪公约》与网络恐怖袭击相关的规定主要包括干扰数据和干扰系统的规定,该公约关于非法侵入和拦截的规定,作为网络恐怖犯罪的手段行为或者中间行为,也属于网络恐怖袭击犯罪的内容。根据这些规定,对于恐怖分子利用互联网实施网络恐怖袭击的行为,可以在其活动早期进行追诉。通过以上规定,《网络犯罪公约》将恐怖分子攻击计算机、网络系统和利用计算机、网络系统实施恐怖袭击都规定为犯罪,不论其行为是否造成了物理损害,也不要求证明恐怖分子的特殊犯罪目的。2005 年欧盟理事会《惩治攻击信息系统行为框架决议》是根据欧洲理事会《网络犯罪公约》制定的,[24] 该框架决议要求缔约国确保非法侵入信息系统、非法干扰信息系统以及非法干扰数据等行为被规定为犯罪行为,该决议也适用于网络恐怖袭击犯罪。

不同于欧洲理事会《网络犯罪公约》,2008 年欧盟理事会的《打击恐怖主义框架决议》采用了专门针对恐怖分子的、传统的有形伤害方式的立法模式,该框架决议在事实陈述部分特别规定了利用互联网实施的大规模恐怖袭击及其引发的危险,明确了该决议既适用传统的暴力袭击,也适用利用互联网实施袭击,根据这些规定对网络恐怖袭击的定罪不存在任何法律障碍。

联合国 13 个反恐公约中的 10 个公约都采取与欧盟理事会的框架决议相同的立法模式,规定了典型的暴力恐怖行为与所造成的严重后果,但与后者不同的是,前者没有把实现恐怖主义的政治目的作为主观要件。联合国的反恐公约能解决惩罚大多数网络恐怖活动犯

〔23〕 参见陈光中:《再谈刑事诉讼法之修改》,《中国检察官》2012 年第 1 期。

〔24〕 See EU Council Framework Decision 2005/222/JHA of 24. 2. 2005 on Attacks Against Information Systems (OJ L 69/67 of 16. 3. 2005).

罪的法律依据问题，但并不能应对全部新形式的网络恐怖活动犯罪，例如对信息基础设施如高速铁路、大坝的计算机系统和公共信息基础平台实施的恐怖袭击，就不能在联合国公约和议定书中找到惩罚的法律依据。

我国打击网络恐怖活动犯罪的刑法也分为两类，即关于网络犯罪的规定和关于恐怖活动犯罪的刑法规定。前者涉及《刑法》第285条和第286条规定的5种犯罪，这些规定仍存在一些立法和司法上的问题，但足以处罚现有的各种网络犯罪包括网络恐怖活动犯罪，并在立法的完备性程度上超过了国际上广泛认同的网络犯罪实体法立法标准，在多数方面也已经达到了要求更高的欧洲理事会《网络犯罪公约》的立法水平。在暴力犯罪立法方面，我国刑法中并没有专门规定的恐怖活动犯罪或者划入恐怖主义犯罪范围的罪名，刑法理论界通常把暴力恐怖犯罪归入危害公共安全罪的范围，如劫持航空器罪、爆炸罪、放火罪，有少量犯罪被规定在其他章节中，如绑架罪等，其缘由除了国际上尚未形成恐怖活动犯罪的定义，没有可以参照的设定恐怖活动犯罪的国际标准；另一方面原因是我国刑法在规定犯罪的罪状上一般不限定犯罪方法，一般性的罪状描述的刑法条款已经可以涵盖大多数恐怖活动犯罪包括网络恐怖活动犯罪，而新出现的少数几种网络恐怖活动犯罪可以在前述网络犯罪的刑法立法的范围内进行规制。

综上，对照前述相关国际立法，我国刑法中有关网络犯罪的规定和恐怖活动犯罪的规定相互配合，为打击网络恐怖袭击犯罪提供了完备的法律保障。

2. 利用互联网传播恐怖活动信息犯罪的刑事实体立法

目前利用互联网传播恐怖活动相关非法信息主要包括六类犯罪行为：威胁实施恐怖活动犯罪，煽动、宣传、美化以及合法化恐怖主义，训练恐怖分子，招募恐怖分子，恐怖主义募资与融资，散布种族主义和仇外主义材料，否认、支持或者为种族灭绝寻找正当借口。与之相关的国际立法和我国相关立法分析如下：

（1）威胁实施恐怖活动犯罪

对于威胁实施恐怖活动犯罪的行为，如下联合国反恐公约明确将其规定为犯罪：《外交代表公约》、《核材料公约》、《海事公约》、《固定平台议定书》、《制止核恐怖主义行为国际公约》。但《非法劫持公约》、《民航公约》、《劫持人质公约》、《制止恐怖主义爆炸事件国际公约》却没有规定相关威胁行为构成犯罪。联合国反恐公约在罪与非罪的设定上采取区别对待，只能解释为联合国反恐公约在威胁实施恐怖活动犯罪行为的犯罪化问题上缺乏一致的制度设计。与联合国反恐公约之间对待威胁实施恐怖活动犯罪的入罪问题上差别化相对应，欧洲理事会《打击恐怖主义框架决议》第1条就明确规定，“恐怖犯罪的行为方式包括：……威胁实施任何前述（a）至（h）款所列行为”，把出于恐怖活动犯罪目的，威胁进行攻击人身安全、身体完整性、绑架劫持人质、造成某些基础设施的大面积破坏、攻击航空器、船舶或其他公共交通工具和货物运输工具、使用武器、释放危险物质等行为，都规定为犯罪。由于以上公约和议定书并没有限定威胁行为的犯罪方法，故利用互联网威胁实施恐怖活动犯罪的，也构成犯罪。

我国刑法对威胁实施恐怖活动犯罪没有特别的规定，刑法条款中规定有“威胁”或者“胁迫”行为的，往往必须到场实施或者以暴力相威胁，仅有《治安管理处罚法》规定了“写恐吓信或者以其他方法威胁他人人身安全的”，可处拘留或罚款。因此，在我国刑法层面上，利用互联网威胁实施恐怖活动犯罪的，还不能以犯罪论处。对比联合国相关反恐公约的要求，我国对威胁实施恐怖活动行为的刑事立法需要进一步完善，而且，从打击犯罪的实际需要来看，这类犯罪同样具有严重的社会危害性，有必要予以犯罪化。

(2)煽动实施恐怖活动以及招募、训练恐怖分子犯罪

对于煽动实施恐怖活动犯罪,招募、训练恐怖活动分子的行为,《联合国安理会 1624 号决议》第 1 款(a)规定,所有国家有义务"采取必要和适当的措施……在法律上禁止煽动实施一种或多种恐怖行为"。欧洲理事会《防止恐怖主义公约》明确规定了"公然煽动实施恐怖主义罪"、"招募恐怖分子罪"和"训练恐怖分子罪"。欧盟理事会《打击恐怖主义框架决议》基本采纳了该公约的作法。欧洲社会的以上两公约都没有限定以上三种行为的犯罪方式方法,当然可以适用于利用互联网实施的情形。

我国刑法中没有规定煽动实施恐怖活动犯罪,但是,煽动行为具有教唆行为的性质,如果行为人利用互联网对特定的个人或者群体进行煽动,意图使后者实施恐怖活动犯罪的,可以按照相应犯罪的教唆犯处罚。如果行为人对不特定的对象进行煽动的,如在互联网上发布煽动实施恐怖活动犯罪信息的,则不能适用教唆犯的规定,将其入罪必须制定新的犯罪立法。需要注意的是,要将该行为与在公共场所包括在网络论坛中一般性地发表个人看法的行为区分开来,避免不适当地扩大刑法的打击范围。对于招募、训练恐怖分子的行为,我国刑法中没有专门规定,但是,《刑法》第 120 条规定了组织、领导和积极参加恐怖活动组织罪,该罪规定的组织、领导或积极参加行为可以涵盖招募、训练恐怖活动分子的行为,并且,该罪对组织、领导、积极参加行为的犯罪方法不作限制,利用互联网招募、训练恐怖分子的,可按照该罪处罚。

(3)为恐怖活动募资、融资犯罪

对于为恐怖活动募资、融资的行为,联合国《制止向恐怖主义提供资助国际公约》第 2 条明确将其规定为犯罪,"本公约所称的犯罪,是指任何人以任何手段,直接或间接地非法和故意地提供或募集资金,其意图是将全部或部分资金用于,或者明知全部或部分资金将用于实施:(a)属附件所列条约之一的范围并经其定义为犯罪的一项行为;(b)意图致使平民或在武装冲突情势中未积极参与敌对行动的任何其他人死亡或重伤的任何其他行为,如果这些行为因其性质或相关情况旨在恐吓人口,或迫使一国政府或一个国际组织采取或不采取任何行动。"[25] 该条第 2 款 - 第 5 款还将企图实施、组织或指使、协助前者犯罪或者与之构成共犯关系的行为也规定为犯罪。"9·11"之后,联合国通过了《安理会 1373 号决议》,"决定所有国家应:(a)防止和制止资助恐怖主义行为;(b)将下述行为定为犯罪:本国国民或在本国领土内,以任何手段直接间接和故意提供或筹集资金,意图将这些资金用于恐怖主义行为或知晓资金将用于此种行为……"该决议第 2 条(e)还规定"所有国家应……确保把参与资助、计划、筹备或犯下恐怖主义行为或参与支持恐怖主义行为的任何人绳之以法,确保除其他惩治措施以外,在国内法规中确定此种恐怖主义行为是严重刑事罪行,并确保惩罚充分反映此种恐怖主义行为的严重性。"[26] 欧洲理事会《洗钱、搜查、扣押、没收犯罪收益和为恐怖主义提供资金公约》也把为恐怖主义募资、融资的行为规定为犯罪。以上公约和决议对为恐怖主义募资、融资的行为都没有规定其犯罪方法,利用互联网实施以上行为的,应在以上国际法律文件规定的范围内。

我国刑法规定了资助恐怖活动罪、洗钱罪,二罪都是重罪及规定了单位犯罪。另外,《刑法》第 66 条还规定,恐怖活动犯罪是特殊累犯,即为恐怖活动募资、融资构成以上二罪

---

〔25〕 这里的"附件",是指该公约后附的《非法劫持公约》、《民航公约》、《外交代表公约》、《劫持人质公约》、《核材料公约》、《机场议定书》、《海事公约》、《固定平台议定书》、《制止恐怖主义爆炸事件的国际公约》9 个反恐公约。

〔26〕 引自联合国《联合国安理会 1373 号决议》第 1 条、第 2 条,http://www.un.org/chinese/aboutun/prinorgs/sc/sres/01/s1373.htm,访问时间:2012 年 12 月 24 日。

的,要按照特殊累犯处罚。我国刑法对以上两罪的罪状表述均没有限定犯罪方法,故利用互联网为恐怖活动募资、融资的,可以按照以上两罪定罪处罚,因此,我国刑法的相关规定已经满足联合国相关公约的要求。

(4)散布种族主义和仇外主义材料犯罪

对散布种族主义和仇外主义材料的行为,目前联合国还没有相关生效的国际法律文件作出规定。欧洲理事会通过的《〈网络犯罪公约〉关于将通过计算机系统实施种族主义和仇外性质的行为犯罪化附加议定书》第 3 条、第 4 条、第 5 条规定了三种犯罪,即通过计算机系统传播种族主义和仇外材料罪、基于种族主义和仇外动机的威胁罪、基于种族主义和仇外动机的侮辱罪。根据该议定书第 2 条规定,这里的"种族主义和仇外材料"是指,"任何写作的材料、图片或者任何其他思想或理论的表示,这些材料提倡、促进、煽动基于种族、肤色、血统、国家或民族的针对个人或者团体的仇恨、歧视或者暴力,如宗教通常是这种因素的托词。"此类材料中显然包括暴力恐怖内容的非法信息。此外,该《议定书》第 6 条还将通过计算机系统向公众传播或使公众知悉有关否认、过分淡化、批准或者为种族灭绝或反人类罪进行辩护等信息的行为规定为反人类罪。以上犯罪相关的帮助和教唆行为也应规定为犯罪。与联合国和欧洲理事会的其他公约和议定书不同,该附加议定书直接规定了利用计算机系统(包括互联网)实施的散布种族主义和仇外材料的犯罪。欧盟理事会《打击种族主义和仇外框架决议》与该议定书不同,它要求成员国对仅实施了《议定书》第 3 条 – 第 5 条所规定行为的,不处罚,但可以作为量刑加重情节;对公开煽动暴力或仇恨和通过向公众散布或分发包含此类内容的小册子、图片或其他此类的行为,应按犯罪处罚。对比联合国和欧洲社会的相关国际法律文件,可以看出,在利用互联网散布种族主义和仇外主义材料行为上,国际社会还没有形成较为一致的立场。

我国刑法中与前述行为相关的规定是第 249 条规定的煽动民族仇恨、民族歧视罪,以上犯罪在民族聚居区发生时,极可能引发暴力恐怖活动犯罪,它与恐怖活动犯罪有着密切的关系,如果行为人本身就是恐怖活动组织的成员和后续恐怖活动的犯罪人,其行为作为实行行为的一部分或者预备行为按照吸收犯的处理原则处理,反之,可能单独构成煽动民族仇恨、民族歧视罪。

3. 利用互联网进行恐怖活动联络的刑事实体法

由于反恐的国际刑事实体立法和我国刑法在恐怖活动犯罪的罪状描述上都没有限定犯罪方法,因此,在打击利用互联网进行恐怖活动犯罪问题上一般没有法律上的障碍。不过,对于利用互联网为恐怖活动进行"谋议"、商量活动计划或者联络并加入恐怖活动组织的,则需要对处罚的相关法律依据进行分析。

一般来说,为实施恐怖活动进行"谋议"、商量行动计划的行为,除非国际国内立法已经将该种行为规定为独立的犯罪,它应属于恐怖活动的预备行为,可以按照相应恐怖活动犯罪的预备犯处罚。

对于利用互联网联络参加恐怖活动组织的,与之有关系的是联合国《打击跨国有组织犯罪公约》,该公约第 5 条如果要适用于参加恐怖组织行为,该恐怖组织必须满足该公约规定的"有组织犯罪集团"的条件,即,要求恐怖活动组织除了实施破坏活动外,还要出于为政治犯罪筹措资金的目的来实施获取金钱或其他物质利益的犯罪活动。这一限定使得该公约第 5 条的规定仅能适用于较少的恐怖活动组织。直接规定参加恐怖活动犯罪集团的国际公约是《打击恐怖主义框架决议》,其第 2 条将"明知其参与行为将为恐怖主义集团的犯罪活动提供帮助,仍然参加恐怖主义集团实施的活动,包括提供信息或物质,或

者以任何形式为其活动提供资助”的行为规定为犯罪,而不再要求有谋利的目的。同样,由于该协议不限制参与恐怖活动集团的方式方法,利用互联网联络并参加恐怖活动集团并在其中从事一定恐怖活动的,可以适用该协议的规定。我国刑法第 120 条规定了“参加恐怖组织罪”,将“积极参加”、“其他参加”恐怖活动组织的行为规定为犯罪。由于该罪对参加行为不限其行为方式方法,故利用互联网参加恐怖活动组织的,可以构成该罪。

结 语

通过对打击网络恐怖活动犯罪的国际立法和我国相关刑法规定的分析,可以得出如下结论:我国刑法的规定已经能满足打击网络恐怖袭击犯罪、利用互联网为恐怖活动募资融资犯罪、利用互联网为恐怖活动进行联络活动犯罪的需要,并达到联合国相关反恐公约的要求。联合国成员国乃至欧洲社会对利用互联网散布种族主义、仇外主义材料行为上没有形成一致的立场,而我国刑法的相关规定已能够处罚利用互联网散布民族仇恨、民族歧视相关材料的犯罪。在打击利用互联网威胁实施恐怖活动犯罪、煽动实施恐怖活动犯罪方面,我国刑法与联合国相关反恐公约的要求有较大的差距,还需要通过新的刑事立法加以解决。关于网络恐怖活动犯罪的法律对策,还涉及到打击犯罪、保护社会安全与人权保障之间的平衡问题、网络服务商的社会责任问题、社会团体参与问题和国家间合作问题,联合国和欧洲社会的有关法律文件或多或少有所涉及,但尚未发展出较为完整的法律体系。

[**Abstract**] In the information age, Cyber-terrorism with the use of Internet for the purpose of Terrorism comes into being. It has some new characteristics such as internetization, internationalization and informationalization. It is a comprehensive kind of terrorist activities, which has much greater effect and power of destruction to the society than the traditional terrorism, and it is becoming a serious and new challenge to the international and domestic society. The countermeasures against Cyber-terrorism nowadays are stopgaps of antagonism which include technology, law, ideological propaganda and public policy. Legal measures against Cyber-terrorism should at least consist of law of prevention and control, penal code and criminal procedural law. Law of prevention and control of Cyber-terrorist activities shall be legislations concerning examination, discovering, intervention and control of Cyber-terrorist activities in emergency. The related penal code and criminal procedural law consist of criminal legislation of internet crimes and terrorist crimes. And they are being developed and completed by the international and domestic society. This article makes a comparative research on the status and the future development of the international and domestic legislation on Cyber-terrorism.

(责任编辑:王雪梅)