中国对网络恐怖主义的法律规制研究
(중국의 사이버테러 법적규제에 대한 연구)

마광(马光**)*** · **백아혜(**白雅慧**)****

논문요지

9.11사건으로 인해 전 세계적으로 테러에 대한 주의가 고조되었고 테러는 점차 중요한 국제안전문제로 부상하였으며 테러는 사회의 안정을 해치고 국민의 생명과 재산안전에 막대한 위협을 야기하였다. 최근 들어 인터넷의 빠른 발전과 더불어 테러와 인터넷의 융합도 새로운 발전을 가져왔는데 사이버테러는 새로운 테러의 형태로 급속히 자리매김하였다. 현재 중국의 사이버테러는 아직 도구형 사이버테러의 형태가 주를 이루는데 즉 인터넷을 통한 온라인 및 오프라인 결부의 테러가 그 중심에 있다. “형법”, “테러방지법”, “사이버안전법” 등 법률은 중국의 테러방지 및 타격에 있어 중요한 역할을 하였으나 국제적인 입법에 비하면 아직도 일부 문제점이 발견된다. 본 논문에서는 우선, 중국의 종교 및 지역적 특성과 결부하여 현존의 사이버테러에 대해 정의를 내리고 사례를 들어 중국에서 사이버테러의 특성과 형태에 대해 설명하고 특히 인터넷이 중국의 테러활동에 대해 어떠한 도구역할을 하는지 설명하고자 한다. 다음으로, 기존의 중요한 입법에 기초하여 중국의 사이버테러 억제 관련 입법의 단점을 분석한다. 마지막으로, 상술한 문제를 분석한 기초 위에 해당하는 법 개정 건의를 하고자 한다. 특히 글로벌 배경 하에서 중국은 국제적인 선진 경험을 충분히 흡수하여 자체의 사이버 테러관련 법체계를 합리적으로 수립해 나아가야 한다.

검색용 주제어: 인터넷, 테러, 입법, 규제, 사이버안전

· 논문접수: 2020.12.08. **· 심사개시**: 2020.12.23. **· 게재확정**: 2021.01.11.

* 중국 절강대학교 광화법학원 부교수, 중국 변호사

** 중국 절강대학교 광화법학원 대학원생, 교신저자

一、引言

随着互联网和大数据的快速发展，网络信息日益渗透到生活的每个角落，信息科技和媒介的更新日益加快，导致恐怖主义逐渐与网络相结合。与传统物理空间内制造恐怖袭击不同，网络恐怖主义基于互联网的全球流动性和共通性的特点，在网络空间中传播恐怖信息、招募人员甚至通过网络开展恐怖袭击等活动。根据中国国家信息安全测评中心发布的关于"2018年上半年国际恐怖主义态势报告"显示，2018年1月至6月，在全球40多个国家发生了600多起恐怖袭击案件，比前一年同期略有增长，反恐刻不容缓。[1)]

不同于传统恐怖活动模式，网络恐怖主义传播的时效性较强，且以网络和媒体为导向，网络攻击和诱导相结合，客观上使得影响的维度和范围更为分散和广泛，使得恐怖主义向新的冲突方式转型。

二、中国网络恐怖主义的特点

（一）网络恐怖主义的定义

网络恐怖主义问题首当其冲即为定义，但是目前国内外尚未有明确界定。关于网络恐怖主义的定义最早是由美国加州情报与安全研究所资深研究员巴里科林于1986年提出，认为它是"网络与恐怖主义相结合的产物[2)]，使用网络的组织形式和信息时代的特点不同于传统冲突模式，在这种模式中，参与者更喜欢独立的、分散的、分级的组织和策略"。[3)]2000年，德国乌西伯尔教授提出，网络恐怖主义包括两层含义：一是恐怖分子利用网络实现了什么；二是互联网给了恐怖分子什么样的特别能力。[4)]在英国政府《反恐怖主义法案(2000)》中，将与政府利益或社会利益的黑客行为定性为恐怖主义行为。[5)]2003年，美国联邦调查局对"网络恐怖主义"做出定义："通过利用电脑或者电信设备，导致暴力、破坏、扰乱服务，通过在特定人群中制造混乱和打消确定性来制造恐惧，旨在影响政府或人群，以符合特定政治、宗教、社会或者意识形态议程。""911"事件后，2001年美国颁布《爱国主义法案》（USA PATRIOT Act），网络恐怖主义第一次作为法律术语出现。联合国反恐任务实施力量工作组(CTITF)将网络恐怖主义基于恐怖主义的目的使用互联网界定为四类行为，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为目的，发展相关信息的手段；(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)]联合国毒品和犯罪问题办公室（UNODC）将网络恐怖主义定义为"蓄意利用计算机网络作为发动攻击的手段……目的是破坏计算机系统、服务器或基础设施等目标的正常运作"。[7)]以色列著名网络恐怖主义研究学者Weimann Gabriel教授认为恐怖主义和极端主义已经逐渐将网络作为实现恐怖主义的重要工具。[8)]搜索中国学术期刊网络出版总库（CNKI）发现国内较早提及恐怖主义

---

1) 宋汀、曹伟：《2018年上半年国际恐怖主义态势报告》,《中国信息安全》2018年第9期，第86页。
2) 康均心、虞文梁：《大数据时代网络恐怖主义的法律应对》,《中州学刊》2015年第10期，第60页。
3) John Arquilla, David F. Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica California, 2001, p.31.
4) 刘仁文：《刑事法治视野下的社会稳定与反恐》，社会科学文献出版社2013年版，第224-225页。
5) 陈钟：《论网络恐怖主义对国家安全的危害及其对策》,《江南社会学院学报》2004年第3期，第18页。
6) 王娜：《网络恐怖主义犯罪的刑事立法应对》,《犯罪学论坛（第二卷上）》，第405页。
7) Nicholas Tsagourias, Russell Buchan, Research Handbook On Internet Law and Cyberspace, Eward Elgar Publishing, p.147.
8) Weimann, Gabriel, Terrorism in cyberspace: the next generation, Woodrow Wilson Center Press, 2015, p.57.

和网络的文章为1996年10月15日在广东金融电脑杂志上发表的《恐怖主义入侵电脑》。首次将“网络恐怖主义”写入文章标题的是简观于2000年3月23日在国际展望期刊上发表的《各国纷纷制定措施打击网络恐怖主义》。国内一些学者也对网络恐怖主义进行了定义，如朱永彪和杨恕认为网络恐怖主义的概念可以概括为:“恐怖主义与网络的结合及其在网络上的延伸,以及针对网络实施的恐怖主义。”[9]盘冠员、章德彪认为网络恐怖主义是指为了实现政治、意识形态等目的，利用或者针对网络制造社会恐慌、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。[10]王秀梅,魏星星认为网络恐怖主义犯罪的定义是指个人或组织、团体基于政治目的或其他社会目的，以网络为辅助工具或者以网络为攻击目标而实施的，从而导致严重的公众恐慌或经济损失等后果的恐怖犯罪行为。量刑时也要针对其所造成的社会后果严重程度进行区分对待。[11]

（二）中国网络恐怖主义的特点

1、宗教极端主义和区域性

近年来，网络恐怖主义的宗教极端主义和地域性的特点显著。宗教极端主义是将宗教和极端化相结合，与其他世俗的利益表达方式相比,宗教具有神圣性和不可置疑性,从而可以使有关组织和个人可以掩藏自己的利己动机。[12]自19末20世纪初一些宗教分裂势力歪曲伊斯兰教的教义，极力鼓吹“泛突厥主义”或“泛伊斯兰主义”，鼓吹圣战,篡改历史，鼓吹“圣战”就是要杀人，殉教即为自我毁灭等邪说。该教义事实上是披着宗教极端主义的外衣，实则行恐怖主义之实。此外一些境外“东伊运”恐怖组织通过网络社交平台,向中国实施的传播极端思想、培训暴恐袭击方法、煽动实施恐袭的行径也加剧了中国的网络恐怖主义问题。

通过以“恐怖”和“恐怖组织”为搜索词在裁判文书网进行搜索得到86个搜索结果，除去重复性案件和无关案件筛选出54例案件，54例案件全部包含通过网络观看恐怖活动或宣传恐怖活动的内容，发生在新疆或犯罪分子为新疆籍（目的为参加圣战）的共计10例，北京共计10例、云南共计8例，以上三地已占到总数的半数以上。[13]54例案件中真正由于相关网络视频着手实施恐怖主义活动如制造炸药、向境外恐怖分子转账、意图加入恐怖组织以及实施暴恐行动的案件有13例，发生在新疆或犯罪分子为新疆籍的共计10例，发生在云南的共计3例。因此中国网络恐怖主义在地域性特征上仍是有迹可循，以少数民族地区尤其有伊斯兰教信仰地区为重点如新疆、云南等，其次为中国的首都北京市。一方面在有宗教信仰的少数民族地区易于通过利用歪曲的教义进行洗脑，降低宣传成本和人员招募成本，恐怖主义的发展能够在短时间内取得成效。另一方面北京作为中国的首都，在国际社会中承担着重要角色，在北京发动恐怖袭击既能够引起国内外的广泛关注，又能使得恐怖组织和恐怖分子获得极大成就感。

2、零散式攻击

目前中国的网络恐怖主义还未能形成大规模的攻击，零散式攻击和个体化攻击最为普遍。

零散式的攻击也表现为无差别化的攻击，人人皆为目标人人皆为猎物。根据新闻报道中国近十年的恐怖袭击中包括有平民、宗教协会工作人员、武警等人员，几乎都为无辜人员。如2014年4月30日，新疆乌鲁木齐市火车南站发生暴力恐怖袭击案件，2名暴徒在

9) 朱永彪、杨恕：《网络恐怖主义问题初探》,《中州学刊》2006年第9期，第14页。
10) 盘冠员、章德彪：《网络反恐大策略－如何应对网络恐怖主义》,时事出版社2016年版，第14页。
11) 王秀梅、魏星星：《打击网络恐怖主义犯罪的法律应对》,《刑法论丛》2018年第3期，第49页。
12) 张家栋：《当代恐怖主义的宗教根源》,《国际观察》2006年第2期，第49页。
13) 截至2019年12月15日通过裁判文书网http://www.court.gov.cn/wenshu.html搜索判例所得数据。

火车站出站口携带凶器砍杀无辜群众，同时引爆爆炸装置，该恐怖袭击案导致死伤共计82人。后证实两名暴徒长期受宗教极端主义思想影响。[14)]

随着互联网的发展加之中国反恐力度不断加大，不同于早先组织化的攻击方式，目前恐怖主义组织愈发倾向于隐藏在互联网之中伺机而动，通过网络不断渗透获取信息，进而通过“散”发动“暴”。网络恐怖主义的零散式攻击模式在于线上联络和线下攻击相结合，线上通过网络达成合意，获取技术指导，完成恐怖活动所需要的资金、武器以及必备品的筹备，进而在线下完成“独狼式”袭击。近几年中国境内的“独狼式”分散袭击多呈现受境外势力影响和指导的趋势，此种分散式个体化的攻击由于更为隐蔽，加大了国家的预防难度，其危险性高于组织化的攻击，因而危害更为严重。

3、“智库”成员和“大众”成员双向递进

近几年恐怖组织的内部结构逐渐成熟，组织形式相对稳定，核心“智库”型成员和普通“大众”型成员并存，分工明确，组织内部纪律较为严密，吸收发展成员有一定程序，发动恐怖袭击有周密的计划。潜在恐怖活动人员中的“智库”成员是网络恐怖活动的核心和领导者，善于利用民族感情以及歪曲的宗教理论，诱导易感人群成为组织成员，其言论行为更容易被易感人群接受。[15)]有一部分的“智库”成员还会成为境外信息的收集者，分布在世界不同地区，及时更新内部信息。如中国公安部公布的第三批认定的恐怖活动人员名单中有6名恐怖活动人员均系“东伊运”恐怖活动组织的骨干成员，均作为组织领导者策划实施对中国境内的多个恐怖活动。

而“大众”成员则是充当一般打手的角色，“大众”包括一般的恐怖分子也包括被洗脑的平民，目前呈现年轻化的趋势，且女性成员逐渐增加。他们通过网络平台接触到宗教极端主义的视频和信息，对信仰极度狂热，尤其是在激烈冲突的环境下成长的“大众”成员，受暴力影响更为明显。[16)]

4、受到境外势力干预和支持

中国的网络恐怖主义受到较多境外“三股势力”的干预和支持，境外势力发展相对成熟，并且时刻着眼于中国境内潜在的漏洞，利用一切机会不断输入恐怖信息以及发展和转化中国境内潜在的极端分子，呈现“境外有种子，境内有土壤的、网上有市场”的局面。境外的“三股势力”互通有无、相互配合，境外势力和境内势力形成联络体系，境外恐怖组织主要负责提供资金和线上的远程指导操控，教授制造武器的方法，提供培训基地，将训练有素的恐怖分子派往境内带领境内恐怖分子发动恐怖活动，在必要的情况下帮助境内恐怖分子逃脱追捕。

5、与黑客结合更为密切

网络的快速发展也带了许多的安全威胁。网络大数据的进步给予了黑客可趁之机，恐怖组织也着眼于一切能够发动网络袭击的手段和方式，对黑客技术虎视眈眈。黑客组织愈发和政治运动以及恐怖主义相结合，过去类似案件中国曾经多有发生，黑客组织“匿名者”曾参与“阿拉伯之春”、“占领华尔街”等多个运动，2012年攻击了数百个中国政府、企业以及组织的网站。[17)]根据2019年第44次《中国互联网络发展状况统计报告》，2019上半年CNCERT约1.4万个IP地址对中国约2.6万个网站植入后门，同比增长约1.2倍。同期国

14) 贾宇：《中国反恐怖主义法律问题研究》，中国政法大学出版社2018年版，第43页。

15) 皮勇、杨淼鑫：《互联时代的微恐怖主义及其治理——兼评<刑法修正案(九)>和<反恐怖主义法>相关条款》，《刑法论丛》2016年第3期，第495页。

16) 周展：《文明冲突、恐怖主义与宗教关系》，东方出版社2009年版，第22页。

17) 朱永彪、任彦：《国际网络恐怖主义研究》，中国社会科学出版社2014年版，第60页。

家计算机网络应急技术处理协调中心监测发现并协调处置中国境内被篡改的网站近4万个，其中被篡改的政府网站有222个，相较于2018年上半年数据有5个月呈现增长态势。[18]通过数据可推测持续增长的网络漏洞问题将会给予境外恐怖势力可趁之机，在结合黑客技术的基础上，通过代码渗透到网站服务器，获得服务器控制权，对中国境内的网站植入恐怖视频和恐怖信息。中国的网络安全问题面临严重的紧迫性，恐怖主义和黑客相结合能够通过前述的漏洞和数据问题侵入中国的网络系统，在线上发布恐怖信息攻击预定目标，或勒索钱财为恐怖组织筹集资金。中国网络产业的发展已然成为经济政治文化发展的重要部分，一旦发动网络攻击必然会造成巨大损失，因此要要严密防范网络黑客攻击。

三、中国网络恐怖主义的立法现状和呈现的问题

（一）中国网络恐怖主义立法现状

1、网络主权的合法性

中国网络立法重点强调网络主权。网络主权实质上是国家主权在互联网领域的延伸概念。但网络主权目前仍然是一个尚未明确的概念，虚拟的互联网领域是否存在国家主权在国际范围内仍有分歧。

中国坚定了国家享有网络主权的立场，确定国家对于网络空间的有效管辖。2015年12月16日在习近平主席在第二届世界互联网大会开幕式上发表主旨演讲强调，在互联网治理中须尊重网络主权。应该尊重各国自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利。[19]确立网络主权的合法性在中国防恐立法和网络安全立法中均有体现，共同明确了网络反恐中国家的治理责任。2015年12月27日通过的《反恐怖主义法》是中国第一部应对恐怖主义的专门法典，《反恐怖主义法》第二条、第四条等条文均强调国家在反恐中的责任。2015年7月1日公布的《国家安全法》第二十五条明确提出了要打击网络犯罪，维护国家网络主权，惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为。2017年6月1日正式实施的《网络安全法》第一条、第五条、第七条以及第十二条等条文的内容不断在强化立法中网络主权的重要性。国家对于网络主权的确认意味着中国对于发生在中国境内的网络恐怖主义犯罪拥有规制权利，权利对外表现为国家在网络空间的平等权、自主权和自卫权，不受他国干涉，对内表现为国家对网络空间的最高管辖权。[20]

2、刑法加大对恐怖主义的打击力度

中国刑法并没有对网络恐怖主义做出明确的定义，也没有专门罪名对网络恐怖主义进行规制。但网络恐怖主义作为恐怖主义的重要表现形式，仍然能够被涵盖在恐怖主义犯罪中。梳理中国刑法发展历史，中国逐步加大了对于恐怖主义犯罪的打击力度。

中国1997年制订的刑法典中只有一百二十条明确提出恐怖主义类型犯罪，但是仅对于组织、领导和积极参加恐怖活动组织的犯罪的行为以及其他参加进行规制。法定刑最高仅为十年，相对其危害性，打击力度相对较小。

2001年12月29日公布并实施的《刑法修正案（三）》所修订之处整体均加大了针对恐怖活动犯罪的打击力度。首先在刑法典原有的一百二十条的基础上进一步规制，对于组织

---

18) 中国信息网：《第44次中国互联网络发展状况统计报告》，
http://www.cac.gov.cn/2019-08/30/c_1124938750.htm。
19) 新华网：《习近平在第二届世界互联网大会开幕式上的讲话》，
http://www.xinhuanet.com/politics/2015-12/16/c_1117481089.htm。
20) 朱雁新：《国际法视野下的网络主权问题》，《西安政治学院学报》2017年第1期，第109页。

和领导恐怖组织的犯罪分子判处十年以上有期徒刑或者无期徒刑，加大了对于组织和领导恐怖组织的刑罚力度。另外在此条文后增加第一百二十一条认定资助恐怖活动的行为属于犯罪行为，从资金角度扩大对于恐怖主义活动的范围。单位实施资助行为的，采取"双罚制"，单位和直接负责的主管人员和其他直接责任人员均须承担责任。其次，为呼应联合国安理会2001年第1373号决议即各国应将为恐怖活动提供或筹集资金的行为规定为犯罪的内容，在原一百九十一条洗钱罪的规定的毒品犯罪、黑社会性质的组织犯罪、走私犯罪的基础上加入为恐怖活动犯罪洗钱的规定，扩大洗钱罪的上游犯罪的范围，并对主管人员和其他直接责任人员的刑罚进行了明确规制，从而于资金方面进一步达到事前预防和事后打击的双重效果。最后，在原刑法第二百九十一条后增加一条，作为第二百九十一条之一，将明知是编造的恐怖信息而故意传播，严重扰乱社会秩序的情形认定为犯罪。此条文旨在打击部分人云亦云故意传播虚假恐怖信息的行为，以维护社会秩序和公共安全。

2011年5月1日施行的《刑法修正案（八）》扩充了第六十六条中关于累犯的规定，在原有的危害国家安全犯罪的基础上增加认定恐怖活动犯罪和黑社会性质的组织犯罪为累犯，并在其他条款中补充了关于累犯的处罚规定。加大对于重复实施恐怖活动犯罪的处罚力度，以期防微杜渐，防止恐怖分子重复犯罪，教育惩戒不思悔改的犯罪分子，充分发挥刑法的双重作用。

2015年11月1日正式施行的《刑法修正案（九）》在2014年和2015年中国部分地区恐怖活动频发的社会现实基础上，立足实践，总结犯罪斗争经验，对于恐怖主义做出更为细致的规定。其中对于第一百二十条的修改和扩充力度最大，增加了对于一百二十条中罚金的规定，增加对恐怖主义的财产刑，优化刑罚结构，从资金源头打击恐怖分子遏制恐怖主义。在一百二十条之一第一款和第二款增加了为资助恐怖活动培训的处罚情形。规定资助恐怖活动组织、实施恐怖活动的个人的，或者资助恐怖活动培训的，处有期徒刑、拘役、管制或者剥夺政治权利，并处罚金。在刑法第一百二十条之一后继续增加五条，将准备实施恐怖活动行为；宣扬恐怖主义、极端主义、煽动实施恐怖活动行为；利用极端主义破坏法律实施行为；强制穿戴宣扬恐怖主义、极端主义服饰、标志行为；非法持有宣扬恐怖主义、极端主义物品行为均纳入恐怖活动犯罪中。增加的内容旨在扩大针对恐怖主义犯罪的刑法适用范围，严密反恐刑事立法体系。同时也体现了预防优先的利益保护立场，从事后惩治恐怖犯罪前移为事前预防，惩治资助、培训、传播恐怖组织或恐怖信息的行为，充分发挥刑法的震慑作用。第三百一十三条中针对司法机关调查取证问题中在原有的明知他人是间谍犯罪的基础上增加了明知他人是恐怖主义和极端主义犯罪拒绝配合的处罚情形，加强恐怖主义犯罪在刑事取证方面的打击力度。第三百二十二条在原有违反国（边）境管理法规，偷越国（边）境的规定中特别增加了为实施恐怖活动而偷越国边境的规定。以完善恐怖分子事前在境外培训集资事后逃跑的行为，不断织密反恐行动网络，加大刑法规制。此外《刑法修正案（九）》中增加的部分和信息网络相关的罪名也引起广泛注意，新增规制包括出售个人信息、通过网络传授犯罪方法等犯罪情形。此类犯罪均立足于互联网发展下出现的新型犯罪方式，明显加大对信息的保护力度，打击包括网络恐怖主义包含在内的网络犯罪。

3、重点地区立法加强

基于中国网络恐怖主义地域性较强的特点，部分地区率先加强区域性的反恐立法。新疆地区是中国反恐问题中典型重点地区，在新疆恐怖分子从未停止实施恐怖活动的步伐，制造了多起暴恐案件。根据中国环球电视网CGTN在2019年12月6日发布的两部关于新疆反恐的纪录片中提供的数据，据不完全统计1990年至2016年年底新疆共计发生近千起暴力恐怖事（案）件，造成大量无辜群众被害，造成的经济损失无法估量，数百名公安民警因此殉职。[21]

21) CGTN:《Extremism strikes Xinjiang》, https://www.cgtn.com/search?keyword=xinjiang。

2014年制定的《关于进一步维护新疆社会稳定和实现长治久安的意见》明确要强化新疆地区的网络安全监管，严厉打击暴力恐怖活动。[22]同年第二次中央新疆工作座谈会中在总结新疆5年经验的基础上，强调打击犯罪加强互联网建设和管理的重要性。[23]2017年4月1日起施行的《新疆维吾尔自治区去极端化条例》（以下简称《条例》）旨在遏制和消除极端化，防范极端化侵害，实现社会稳定和长治久安。条例也对网络恐怖主义做出了相应的规定，第十九条、第二十五条、第二十六条的规定明确要打击由互联网产生的恐怖主义，治理网络恐怖主义传播；针对主流的社交平台，强化网络监管部门相关工作，通过技术手段阻断境内外信息的传播和联络。2018年12月26日新修订的《新疆维吾尔自治区实施〈中华人民共和国反恐怖主义法〉办法》（以下简称《办法》）第六条将利用互联网等方式宣扬传播恐怖主义、极端主义或者传授恐怖犯罪方法的认定为恐怖活动。进而惩治通过网络发动的恐怖活动。此外第十七条第二款、第二十条第一款又从安全防范的角度对预防网络恐怖主义的方法进行了规制，进而做到惩防结合，先发制敌。

（二）中国网络恐怖主义立法存在的问题

1、立法过于单薄，缺乏体系规制

目前缺少专门针对网络恐怖主义的立法规制，对于网络恐怖主义的重视尚待加强。《刑法》和《反恐怖主义法》为中国打击网络恐怖主义提供了重要规制依据，关于网络恐怖主义的内容在《刑法》中被包含在了恐怖主义、侵害计算机信息系统、计算机信息系统数据等犯罪之下。分析实践案例可得行为人对于计算机安全的损害仅为手段行为，而最终的目的是实现恐怖主义目的，是计算机犯罪和恐怖主义两者的结合。[24]此外目前相关法律条文中，关于网络恐怖主义的内容呈现出零散碎片化的分布特点。条文大部分是将互联网作为媒介或工具，并非专门立足网络恐怖主义进行规制，因此仅靠两部法律对于网络恐怖主义进行打击太过单薄，难以全面有效的打击网络恐怖主义犯罪，中国当前网络犯恐怖主义犯罪的立法结构与罪名已经开始大大的滞后于网络恐怖主义整体发展态势。[25]

针对《反恐怖主义法》，网络恐怖主义使得恐怖分子更为分散而不会集结成群，而《反恐怖主义法》规制对象针对的是群体性的线下集结恐怖分子，因此针对网络中分散的恐怖分子不足以进行全面防控。对于恐怖人员的认定仅仅在《反恐怖主义法》第二章恐怖活动组织和人员的认定中提及，在网络恐怖主义领域缺少统一的认定标准。通过网络实施恐怖主义活动的类型、受众范围、造成损失范围等等因素均未作规定。目前中国可查询到的案例中大多数为借助网络平台进行的宣扬恐怖主义犯罪，但此类犯罪分子是否为网络恐怖分子也尚未形成定论。

此外一些中国关于规制网络安全的条文大多数以条例的形式呈现，立法层级较低，无法充分完善网络恐怖主义的法律体系。《网络安全法》并没有专门针对网络恐怖主义的责任规制，无法应对目标型的网络恐怖主义。目标型网络恐怖主义在中国虽然不属于主要的方式，但是随着网络犯罪和网络黑客的增加很难预测未来是否会带来威胁，而一旦形成目标型的网络恐怖主义在一个14亿人民的国度危害结果是显而易见的。

因此综合而言，在恐怖主义和网络迅速结合的趋势下，中国目前针对网络恐怖主义的立法较为单薄，以《反恐怖主义法》和《刑法》为核心，以《网络信息法》为补充，且涉及到的条文均是分散化的，甚至一些条款存在优先顺序不明，认定标准不一致的情形。此外，

---

22) 中国政府网：《中央政治局研究进一步推进新疆社会稳定和长治久安工作》，http://www.gov.cn/xinwen/2014-05/26/content_2687490.htm。

23) 新华网：《习近平在第二次中央新疆工作座谈会上发表重要讲话》，http://www.xinhuanet.com/photo/2014-05/29/c_126564529.htm。

24) 王志祥、刘婷：《网络恐怖主义犯罪及其法律规制》，《国家检察官学院学报》2016年第5期，第21页。

25) 于冲：《网络犯罪罪名体系的立法完善与发展思路——从97年刑法到<刑法修正案(九)草案>》，《中国政法大学学报》2015年第4期，第45-46页。

现有可借鉴的法律依据集中在刑事领域，其他手段运用较少。宏观层面尚未形成体系性的规制，对于遏制网络恐怖主义的力量不足，在具体案件中易于发生法律空白的情形。

2、重点地区防控力度缺乏，信息监控立法不完善

目前重点地区反恐立法是以《反恐怖主义法》作为主要参照的，如新疆地区实施的《办法》所采取的模式和《反恐怖主义法》几乎相同。《反恐怖主义法》的出台背景带有应急色彩，集刑法、行政、刑诉于一体，其防控问题集中在第三章安全防范和第四章情报信息中，部分条款实质上是原则性的规定，并未对具体实施情况做出明确规定。

恐怖主义活动在新疆较为复杂，新疆地区制订的相关法律法规应当因地制宜，且须充分结合本地反恐经验。相对应新疆地区实施的《办法》中针对信息监控的规制被融合到第四章情报信息中，除此之外只是零散的在其余条款中被提及。随着互联网的发展，在新疆地区境内恐怖分子之间的信息联络逐步加强，《办法》中对于信息的防控手段过于单薄笼统，没有针对不同部门的分工问题进行规定，也没有结合不同领域的特点区分防治方式，会造成部门分工不明，职权模糊化，易在实务中出现越界监管、越权指挥、处罚标准差异化的情形，从而影响刑事责任的认定，以及产生信息监控无法体系化和常态化管理的问题。[26]此外信息监控较为复杂，涉及公民信息安全以及企业监控责任和范围问题，而新疆地区作为网络反恐的主要阵地，并没有细化信息监控的相关立法内容，对于信息监控立法尚待进一步完善。

3、国际合作不足，国际反恐机制不完备

目前网络恐怖主义的发展已经突破了空间的限制，跨国性特点显著，对其防范已不是个别国家独有的问题，恐怖主义目前已是牵一发而动全身，严重危害世界各国的稳定和安全。网络恐怖主义作为非传统安全，将世界各国紧密的联系在一起，需要世界各国联手共同打击和遏制网络恐怖主义。中国积极参与多边合作，如积极通过参与上海合作组织加强中亚地区反恐合作。但是此类参与活动大多数停留在传统恐怖主义的防范领域，且限于区域性防范，国际化参与程度仍欠缺。

此外，在技术层面中国尚未形成国际化的情报制度和技术研发合作体系，如前文所述，网络反恐需要全球联手全球参与，同样在操作层面上需要突破国界壁垒和意识形态的差异，在全球范围内共享情报信息，共建反恐机制，加强反恐技术的合作和研发，共建国际性的反恐体系。国际交流和合作的步伐应进一步加快。

影响中国网络恐怖主义的主要的领导恐怖势力大部分位于境外，这些势力在事前通过网络形成联络机制支持和指导国内恐怖势力的发展，在事后帮助国内恐怖分子向境外窜逃，使得境外成为了恐怖分子的避难所，境外反恐成为难点。针对境外恐怖组织和潜逃至境外的恐怖分子中国目前在管辖等问题方面存在诸多障碍，缺乏与国际社会间的必要的司法合作和司法协助，因此国际司法沟通交流机制尚待进一步加强。

四、中国应对网络恐怖主义的法律途径

（一）加强网络防恐立法

1、明确界定网络恐怖主义法律概念

26) 陆旭：《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》2015年第6期，第65页。

随着“网络社会”和“信息社会”的发展，规制网络恐怖主义已经是急需面对的问题。但是目前中国相关的法律法规中，并未对网络恐怖主义作出明确的定义，且在目前现有的法律法规中自身的衔接问题也有待进一步加强。明确的定义能够区别于一般的黑客犯罪、恐怖活动犯罪和网络犯罪，能够在司法实践中为司法人员的定罪量刑提供明确的依据，因此对于网络恐怖主义的概念界定须从恐怖主义和网络犯罪的定义入手。

国际范围内对于恐怖主义尚未形成统一的界定。查阅有关资料，区域性条约中对于恐怖主义的定义分为三种类型。第一类为描述型，即直接定义恐怖主义的概念。如1937年于日内瓦签订的《防止和惩治恐怖主义公约》中对于恐怖主义的定义为直接反对一个国家，而其目的和性质是在个别人士、个人团体或公众中制造恐怖的犯罪行为。[27]第二类为列举型，列举全球性反恐条约规制的行为或列举具体的犯罪行为。如1999年《独立联合国家打击恐怖主义合作条约》等。第三类为综合型，既包括对于恐怖主义的定义又包括对恐怖主义犯罪的列举。如1998年《阿拉伯国家联盟制止恐怖主义公约》在第1条概念中明确了恐怖主义的定义，此外又将6个国际条约的具体行为涵盖在恐怖主义犯罪中。

针对于网络犯罪，联合国颁布的《联合国打击跨国有组织犯罪公约》第二十九条h项关于培训和技术援助的对象明确包括打击借助于计算机、电信网络或其他形式现代技术所实施的跨国有组织犯罪的方法。《网络犯罪公约》没有对网络犯罪进行定义，但从公约的序言中可以看到《网络犯罪公约》的重点规制领域落脚在刑事领域，认定的网络犯罪与计算机网络和数据相关。

中国《反恐怖主义法》第三条中对于恐怖主义的定义是指通过暴力、破坏、恐吓等手段，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，以实现其政治、意识形态等目的的主张和行为。中国刑法将网络犯罪的规制落实在具体的犯罪中如组织、领导、参加恐怖组织罪、帮助恐怖活动罪、准备实施恐怖活动罪、宣扬恐怖主义、非法侵入计算机信息系统罪、拒不履行信息网络安全管理义务罪等罪名。对于网络犯罪中国学者目前尚未形成统一概念。存在有对象说、工具说和这折中说三种理论。对象说为狭义的界定网络犯罪概念，将网络视为犯罪对象。工具说是将网络作为犯罪的工具。折中说涵盖了将网络作为对象和工具的情形。

分析前述国际条约以及中国《反恐怖主义法》的定义可看出，区别于传统恐怖主义犯罪，网络社会中的恐怖主义犯罪突破了地域空间的限制，中国已有法律中的恐怖主义定义已不能完全规制网络恐怖主义，须在恐怖主义定义下另行界定网络恐怖主义及其行为。

通过对比区域性条约，对于恐怖主义的内涵综合型定义更为合理和完善，既包括对恐怖主义的直接定义又包括了具体犯罪行为，且明确涵盖国际社会中通用反恐条约规制的具体行为。结合中国立法情形以及本文第2.1节中对于网络恐怖主义定义的综述研究，笔者倾向于在法律界定下以学者王秀梅,魏星星的定义为基础并结合折中说的观点，在恐怖主义犯罪的框架下，基于政治目的、宗教目的以及其他目的，主体范围明确涵盖个人、组织和团体，打击行为既包括工具型网络恐怖主义又包括目标型网络恐怖主义。危害结果包括造成的经济损失、社会恐慌等。且社会恐慌既包括网络社会的恐慌以及向外延申的现实社会恐慌。在执行定义中规制计算机犯罪、组织、策划、参加、帮助、资助恐怖主义、网络宣扬恐怖主义等具体犯罪以及中国所加入的国际反恐条约所打击的犯罪行为。

2、完善网络恐怖主义法律体系

根据前述目前中国形成了以《反恐怖主义法》和《刑法》为核心，以《网络安全法》为补充的反恐法律体系，但是相较其他国家而言体系仍然较为单薄。中国应在将网络安全问题作为重要的国家安全战略性问题的基础上，继续完善网络反恐立法体系。

一方面完善关于网络宣扬恐怖主义犯罪刑罚，结合中国近几年实践中关于恐怖主义的裁判案例，大多数案件集中在宣扬恐怖主义、极端主义罪名之上，而对于此类犯罪各地法院量刑差距较大。因此在《刑法修正案（九）》第一百二十条的基础上，可进一步细化宣

27) 田溪：《恐怖主义定义界定问题分析》,《法制博览(中旬刊)》2012年第5期，第243页。

扬恐怖主义和极端主义犯罪的量刑标准。首先考虑宣扬材料的性质、视频时长，宣扬材料中是否有明显的分裂祖国、宣扬圣战、试图吸引观看者参与、危害中国安全等内容，且此类内容都应得到充分的评价。其次宣扬一词即意味着需要受众和途径，因此受众人群的性质、数量、年龄等因素都应该得到充分的评价。同时也要考虑所采取的宣扬途径是否为主流的、使用人数较多的通讯社交平台。最后需要酌情考虑行为人的动机、过往表现，结合行为人本身是否是初犯，过往有无类似行为等因素评价是否出于“明知”的罪过心理。实践中存在仅仅出于“猎奇”心态分享一些“斩首”类视频的案例，对这些案例则不应矫枉过正，情节轻微的不应以犯罪论处。

另一方面《网络安全法》须明确网络服务供应商的责任。韩国2012年发布《信息通信网使用推进及信息保护等相关法律》规定若服务供应商不拦截与恐怖主义相关的责任则可能被追责。美国从1996年开始出台多个法律、总统令等不断加强保障美国信息基础设施、弥补网络漏洞安全，促进信息技术发展，提升对抗网络风险能力。中国须在国家网络空间安全战略的指导下完善相关的配套法律法规。首当其冲的即为出台正式的关于关键信息基础设施相关的法律，可借鉴美国经验，覆盖重要民生领域，确立优先级，建立风险评估体系，建立重点行业的标准。

3、推进“禁止令”在网络防恐中的应用

中国《刑法》第38条规定判处管制的犯罪分子根据具体情形可同时规定其禁止进入特定区域和场所。目前中国法律法规中，关于禁止令规定在最高人民法院、最高人民检察院、公安部、司法部印发的《关于对判处管制、宣告缓刑的犯罪分子适用禁止令有关问题的规定(试行)》通知的第四条中，规定了行为人禁止进入包括网吧在内的娱乐性场所和公共场所。该条的规定已经落后于时代的发展，禁止进入网吧仅能从物理上控制犯罪分子，但是在互联网获得极大普及的今天，此种物理禁止发挥的作用微乎其微。

因网络隐蔽和迅捷的特点，网络成为恐怖主义迅速发展的重要媒介和手段。因此有学者提出可适当扩大禁止令在网络恐怖主义犯罪惩治中的适用，应当扩大刑法意义上的“场所”、“区域”的内涵以使禁止令能在网络犯罪中有所作为。[28]若能在恐怖分子惩治方式中扩充网络领域的禁止令则能在较大程度控制网络恐怖主义的发展，切断网络联络和传播的途径，有效防止再犯。可结合具体案件事实和实践经验，根据犯罪分子的犯罪手段方式及借助的社交平台禁止其进入该特定网络领域。形成关于犯罪分子主要社交平台和网络活动领域的登记备案制度，以供有权机关及时监控，如有变更须随时报告有权机关。

“禁止令”制度在网络空间的适用目前问题较多面临较大挑战，且需要较强的技术支持以及相对应的网络准入性规范，但仍不失为是打击网络恐怖主义的重要法律手段，笔者此处也仅作为一种应对网络恐怖主义解决思路。

（二）完善立法应对制度

1、信息过滤和网络监管

网络和大数据的迅速发展使得网络信息呈现海量式递增，给与了恐怖主义较大的传播空间，恐怖组织和恐怖分子将信息隐藏在繁杂的网络节点中，且海量数据中大部分为非结构化数据，恐怖分子的加密技术进一步加大了网络信息的甄别难度。

一方面，立法要建立信息的分级制度，对恐怖信息进行筛选。由于中国网络恐怖主义主要源自境外恐怖势力的信息输入和诱导，因此要更为注重拦截和过滤境外恐怖信息。2019年12月1日正式实施的《信息安全技术网络安全等级保护安全设计技术要求》将网络安全等级分为4级[29]，对通用等级保护安全技术框架的定级系统分为5级。5级定级系统均设

28) 陆旭：《网络服务提供者的刑事责任及展开——兼评<刑法修正（九）>的相关规定》，《法治研究》第2015年第6期，第65页。

置了安全区域边界进行信息的层层过滤，针对整个系统设定了跨定级系统安全管理中心保障不同级别定级系统之间的安全连接。因此可在此定级框架的基础上在每一级别定级系统的信息过滤中特别加强对于恐怖信息的甄别，通过5级定级系统的安全通信网络层层筛选，识别异常网络活动，及时截获恐怖信息，从源头控制恐怖音频视频的传播。可进一步在提炼出的有效的与恐怖活动相关的信息基础上，通过大数据智能化分析手段详列恐怖组织和恐怖分子常用的网站平台和代码，将行为模式还原成数据指标，进而锁定现实恐怖分子，中断行动进程加强定点打击力度。

另一方面，对于网络监管需要落实网络经营者关于监管信息的责任，扩大网络经营者对于网络恐怖信息传播的监测的责任与义务。根据《网络安全法》第七十六条的规定，网络运营者除包括网络服务提供者外，还包括网络的所有者和管理者，主体概念更为广泛。而《反恐怖主义法》第十八条、第十九条的规定中只有互联网服务的提供者在发现含有恐怖主义、极端主义内容的信息的，负有应当立即停止传输，保存相关记录，删除相关信息，并向相关部门和机关报告的责任。网络信息的监管责任扩大到全部的网络经营者，才能够更有效的实现实现动态信息监测，因此对于网络信息规制主体需要进一步的完善和补充，进而和《网络安全法》的规定进行衔接，细化在网络检测中网络安全认证、检测、风险评估等具体义务。

2、完善信息情报制度

首先，信息情报制度的完善需要通过法律明确主管部门。信息时代的反恐绝非仅靠一个部门即可解决的，需要以核心部门为中心，进而建立与恐怖活动犯罪调查相关的各个机构之间的协调机制和信息共享制度。[30]《反恐怖主义法》第四章关于情报制度中规定收集情报的主体为公安机关、国家安全机关和其他有关部门。《国家情报法》第五条规定国家安全机关、公安机关情报机构、军队情报机构开展情报行动，其余各国家机关与国家情报工作机构密切配合。但《网络安全法》第五十一条规定国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作。对比发现，《反恐怖主义法》和《国家情报法》在情报制度的主管部门是相同的，但是网络恐怖主义信息显然会影响网络安全，根据《网络安全法》的规定国家网信部门也有权利进行收集和分析。为了情报制度主体间的一致性，可在实践操作中明确以公安机关和国家安全机关为核心构建反恐情报平台，国家网信、金融、交通等部门协助，进而破除部门的壁垒，有效的共享和整合信息，拓宽情报信息搜集的途径，建立多样的数据库和分层级的信息情报系统，完善多元化的反恐情报信息制度。

此外，无论是《反恐怖主义法》还是《国家情报法》仍需进一步强化普通大众和企业对于完善信息情报制度中的角色。加强全民协同参与网络反恐机制和联动机制，鼓励信息举报制度，积极引导群众自觉举报网络恐怖信息。可借鉴国外经验加大对恐怖信息举报制度的物质投入，强化网络用户在监管体系中的参与感。如美国对于提供“伊斯兰马格里布基地组织”、“西非圣战统一运动”组织等几个恐怖组织的头目下落提供2300万美元作为奖励。[31]

3、建立有效应急响应机制

网络响应机制包括事前预警、事中应对和事后惩戒及恢复。目前中国《网络安全法》、《反恐怖主义法》已初步规定了网络应急机制，但立法需要继续细化事前、事中及事后的方案。对于网络恐怖主义预先的应急准备首当其中，应当设立专门的网络应急部门，结合信息情报制度，建立预先应急响应机制。

29) 第五等级保护对象特殊，需要特殊的管理模式和安全设计技术要求，因此不在此标准中。

30) 赵秉志、杜邈：《在联合国法律框架内进行反恐斗争——“全球反恐法律框架”学术研讨会综述》，《法学杂志》2008年第3期，第21页。

31) 应晨林：《完善我国网络反恐立法的思忖》，《网络空间战略论坛》2015年第8期，第46页。

中国可借鉴美国较为完善的响应机制立法经验，并结合中国网络反恐实践经验制订专门《网络应急响应框架》，区分不同网络领域的响应模式，明确规定响应主体机构，协调不同部门，结合中国省市县乡的行政区划分区域、分级别的建立网络应急响应机制。构建多元化的应急响应平台，设立专门的国家网络恐怖主义应急机构，行业应急管理部门，地方政府应急管理部门，明确其职责，实行网络安全动态监控管理。[32]充分结合事前预警、事中应对和事后惩戒和回复的响应目的和响应模式，以非常规性突发事件为目标，迅速及时的应对突发事件，提高响应能力的灵活性和高效性，解决中国应急响应能力的短板和问题。

（三）重点地区和重点人员防控制度

1、建立恐怖信息公开制度

反恐信息公开是网络反恐的重要方式，及时公布包括恐怖组织和个人名单在内的信息能够进一步加强公众的反恐认知，调动群众参与反恐战线。截至2019年12月31日，中国公安部共发布了三批恐怖活动人员名单，共计25名恐怖分子。此外还公布了4个恐怖组织，即东突厥斯坦伊斯兰运动、东突厥斯坦解放组织、世界维吾尔青年代表大会、东突厥斯坦新闻信息中心。[33]

2005年英国伦敦发生爆炸案后英国加快了反恐信息的宣传力度，一方面英国军情5处印制发放《预防恐怖主义》书册，向群众普及反恐信息以及如何应对网络恐怖袭击的建议。此外，英国政府为鼓励和引导公众的参与，除军情5处外联合多个政府部门，在网络进行反恐宣传，发布恐怖威胁预警信息。韩国信息通讯部专门设立“预防网络恐怖袭击日”,即为每月的15号，促使政府、企业和民众对计算机和网络系统进行周期性检查,及时发现漏洞警惕网络袭击提高预防网络袭击的预防能力。2018年泰国防部建立“天网”全新资料库，旨在使得国家能及时追踪在本国境内的外国人。[34]

中国可借鉴域外的信息公开制度，对公众进行充分预警提醒。公众参与在反恐体系中占有重要地位，若没有充分的知悉则难以激发公众的参与。目前除公安部的官方网站外，西北政法大学反恐怖主义法学院和反恐怖主义研究院建立的“反恐信息网”是能够直接查询反恐信息的网络媒介。[35]但该网站公布的主要内容集中于反恐调研成果、工作动态、人才培养等领域。因此在实现内控的基础上，在和平时期需要进一步关注国际恐怖主义发展的趋势。可在已有的关于反恐信息网站的基础上添加或另行建立网站公开合法的恐怖信息，公开的内容根据国家安全需要可进行一定的限制。建议及时跟进和更新国内以及国际恐怖组织和恐怖人员名单，境外主要社交平台的恐怖组织账号，境内外恐怖主义相关案件，汇总中国有关恐怖主义的法律法规以及世界主要国家和地区的主要反恐法律法规和工作进展，引起公众重视。

此外，也可加强媒体公开反恐信息的力度。2019年年末开始中国陆续通过“新浪微博”、“CCTV官方网站”、“哔哩哔哩”、“腾讯视频”等多个社交平台和视频门户网站发布反恐纪录片和宣传片，2019年12月6日CGTN发布《中国新疆，反恐前沿》，次日发布英文纪录片《幕后黑手一“东伊运”与新疆暴恐》。12月27日北京市反恐办推出国内首部剧情式反恐主题公益宣传片《如果时间可以倒流》，均有较好的反响。截至2020年1月2日仅“央视新闻”官方媒体通过“新浪微博”社交平台发布的《中国新疆，反恐前沿》观看量达就达4224万，转发评论点赞共计近4万人次。[36]可见网络宣传方式能够得到较好的反馈，能够及时

32) 舒洪水、党家玉：《网络恐怖主义犯罪现状及防控对策研究》,《刑法论丛》2017年第3期，第409-411页。
33) 倪春乐：《比较与借鉴:论恐怖主义犯罪追诉中的恐怖组织认定》,《中国人民公安大学学报(社会科学版)》2012年第1期，第121页。
34) 宋汀、曹伟：《2018年上半年国际恐怖主义态势报告》,《中国信息安全》2018年第9期，第89页。
35) 反恐信息网：https://cati.nwupl.edu.cn/。
36) 截至2019年1月2日新浪微博“央视新闻”官方用户发布的《中国新疆，反恐前沿》视频状态下显示的观看及评论点赞转发数量。

方便大众了解恐怖活动，能够正确引导舆论，因此须秉持开放意识，进一步加大主流社交平台和网站的信息公开力度。

2、重点地区建立独立防恐体系

中国新疆地区是反恐的重点区域，2017年之前恐怖暴乱频发，同样也是境外“东伊运”组织的重要目标地区，此前新疆地区的恐怖主义形式呈现向内地转移的趋势，因此加强新疆地区的网络防控体系对于整体反恐具有重要意义。

首先针对新疆地区的宗教主义和极端主义特点，落实《新疆维吾尔自治区宗教事务条例》，深入研究新疆地区宗教问题，提高宗教条例的实践操作性，实现宗教管理去极端化，改变以往对宗教“三不管”的态度，通过新媒体和互联网加强新疆地区正确宗教思想的普及。其次在网络恐怖主义发展的趋势下，完善网络反恐预案和地方性响应机制，新疆作为反恐重点区域须建立以预防为主的反恐响应机制，总结反恐经验对事件进行科学性分级，针对不同级别制订不同的反恐预案。加强网络侦察技术，及时定位防止恐怖分子转移。也需要完善基层网点建设，加强对利用网络进行犯罪的宗教极端组织的监管、筛选，及时掌握重要线索。[37]最后在反恐体系中要发挥社区和街道的作用，社区和街道对小范围情况更为熟悉，能够充分掌握本区域的人员情况，易于开展宣传教育工作，加强基层群众情报力量，通过小的节点连接新疆地区整体独立的反恐体系。

3、重点人员的个人信息监控

基于“打早、打小、打苗头”的反恐政策[38]，需加强重点人员的信息监控，预防实施恐怖活动。目前中国已经公布三批恐怖分子和人员的名单，在信息监控的网络反恐措施下着重加大名单人员和相关组织的持续性监控，可通过条例制订详细的恐怖活动组织和人员认定的办法，规制认定的程序、监督和救济制度等。[39]分析形成机制和联络机制，保存电子证据，为进一步的网络反恐机制奠定基础。也要对可疑人员进行筛选、分析和预先研判，注重日常信息监控，建立个人信息库，记录包括个人身份、家庭关系、身体特征、教育程度等等信息，分析日常活动特点，对其曾经使用过的媒介、软件和网站进行重点追踪和侦察，建立长期有效的信息监控机制。由于传播恐怖信息是网络恐怖主义的重要表现形式，近年来中国司法实践中恐怖主义相关案件大多数属于网络宣扬恐怖主义、极端主义犯罪，因此建立重点地区网络宣扬恐怖主义、极端主义的犯罪分子数据库是个人信息库的重要组成部分，可根据犯罪分子的犯罪行为和受众人群，在刑罚执行完毕或缓刑期间及结束后的合理期限内持续对此类人员进行监测，防止重复犯罪，起到警示作用。

（四）借鉴域外立法防治经验

1、完善中国网络安全审查制度

互联网逐渐成为反恐斗争中的重地，落实和完善网络安全审查能够提高网络产品和服务的准入规则，可从审查层面切断网络恐怖主义信息传播的途径，扩大防范的范围。

中国从《网络安全法》至2017年发布的《网络产品和服务安全审查办法（试行）》再至2019年发布的关于《网络安全审查办法（征求意见稿）》（以下简称征求意见稿）可见中国网络安全审查制度正在逐步成型并成为独立的规制对象。征求意见稿第一条明确实施目的

37) 陈旻祥：《边疆民族地区宗教极端主义问题及其对策研究》，《法制与社会》2019年第24期，第225页。
38) 大河网：《打早、打小、打苗头，中国反恐思路已明晰》：http://newpaper.dahe.cn/hnsb/html/2014-05/08/content_1071654.htm?div=-1。
39) 师维、孙振雷、孙卫华、张桂霞：《中国反恐怖主义法研究》，中国人民公安大学出版社2016年版，第73页。

在于提高关键信息基础设施安全可控水平，第二条明确规制对象为关键信息基础设施运营者采购的网络产品和服务。具体来看相较其他互联网发达国家，中国的网络审查制度上尚在初级阶段，目前已有的征求意见稿也仅限于关键信息基础设施领域。首先在征求意见稿中需对于不同产品和服务进行分类分级，可借鉴美国经验，区分模块，详列类别。其次针对中国在大力推进5G技术的发展趋势下，需要逐步分析更为复杂的供应链风险、水平参差不齐的网络运营者风险以及任意时间境外势力恶意打压风险。建立评估标准，强调标准评估的持续性，要综合考虑产品和服务的整个生命周期进行评测。最后规制供应链也需要细化供应链审查的标准和规则，防止恶意程序和病毒的植入，防止产生安全漏洞，避免“蠕虫式”的勒索病毒事件的再次发生，打击网络恐怖主义。

2、建立数据隐私和安全制度

网络监测和情报制度的建立事实上是包括个人数据隐私权在内的数据安全向国家安全让渡的体现，这种让渡并非是无条件无约束的，打击网络恐怖主义同时也要注重保障人权，在收集情报信息的同时也要平衡保障数据隐私和安全。尤其是在中国个人数据隐私安全面临较大威胁，在市场中个人数据信息付费即可获得，这也为恐怖组织的预备行为中取得相关个人信息提供了便利。出于正当目的实施的信息截取和监测行为均须在法律的规定下，执行机关和可获得数据的范畴须有明确的法律规定、操作规范、保密原则和违反的责任机制。

中国目前尚未出台关于个人数据安全和隐私的专门法律法规，相关内容都呈现零散的分布特点。中国刑法对于网络恐怖主义犯罪的规制重点之一在于打击计算机类型的犯罪，但与此同时在“大数据”发展的背景下，忽视了信息数据的保护，其不足愈发突显。[40] 关于保障个人数据安全和隐私的内容均在《反恐怖主义法》和《网络安全法》中有体现，但是关于数据安全的规制与网络安全的规制立法不完全匹配，尚待进一步完善。2013年实施的《电信和互联网用户个人信息保护规定》仅限于用户姓名、出生日期、身份证件号码等个人信息，规制的领域也仅限于电信和互联网用户，规制的个人数据安全和领域缺乏全面性。

中国可借鉴欧盟《通用数据保护条例》的规定形成个人数据和隐私权保护的立法意识，与《网络安全法》相匹配制订数据保护法律规范，平衡网络监测和数据保护，设置类似欧盟“数据保护官”的部门或者专门的数据保护工作组负责数据隐私安全。明确数据保护范畴和个人数据的权利，完善隐私政策，规制公共部门使用数据的权利的理由，规范术语的标准，防范数据风险，完善法律法规间的衔接和网络反恐立法体系。此外也可借鉴《通用保护条例》对于处理者的规制，增加了中国网络服务平台和网络信息提供者的义务，要求处理者具备数据保障措施、记录处理活动、承担数据泄露相应义务等，进一步保障数据安全。[41]

3、加强对网络黑客的处罚力度

互联网时代下黑客逐步呈现和网络恐怖主义逐渐相结合的趋势，恐怖组织加强招募吸引擅长计算机技术人员，黑客攻击基于低成本、跨国境的优势能够实现攻击的最大化。

中国目前没有针对网络黑客的规定，没有针对恐怖活动利用黑客工具的规制制度。对黑客的惩治可通过其采取的不同手段确定不同罪名，如通过网络进行诈骗的犯罪行为规制为诈骗罪，侵入计算机系统造成破坏的犯罪行为规制为破坏计算机信息系统罪，通过网络方式进行恐怖主义活动的根据其活动的目的、方式确认不同的恐怖活动罪名。基于网络黑客明显的计算机专业技术优势，若发动网络恐怖袭击则造成的危害巨大，因此应加大对以黑客身份实施网络恐怖主义犯罪的处罚力度。此外要完善计算机系统的安全防护、提升

40) 于冲、黄晓亮、李源粒、李晓明：《网络犯罪的刑法回应与罪名架构（笔谈）》，《中国政法大学学报》2015年第4期，第46页。

41) 王翔：《欧盟<通用数据保护条例>(GDPR)解读》，《法制博览》2018年第12期，第195页。

安全管理系统，[42]从以往线下实施恐怖活动的人员查处转向网络黑客的查处，研究分析网络黑客技术群体，实时跟进国际反黑客技术的发展遏制网络黑客和恐怖主义相结合的趋势。

（五）开展国际反恐合作

1、反恐警务交流及刑事司法合作

深化国际网络反恐警务交流是打击全球性的网络恐怖主义必不可少的措施。1923年国际刑事警察组织（ICPO）在维也纳成立，1984年中国加入该组织。ICPO成立至今在打击国际犯罪领域居于重要地位。中国在充分履行责任的基础上可借助ICPO和联合国的平台，深化国际警务交流。首先结合国际司法实践和中国的反恐经验，完善国际网络反恐联合侦察合作方式，通过签订双边或多边的国际条约引导建立网络警察，实现网络巡逻常态化管理，拦截、分析、预警网络恐怖主义信息。在发生网络袭击事件时在有效时间内实现迅速应对和解决。结合线上线下恐怖主义趋势探索联合侦察模式，满足反恐的实践需求，保证事前、事中、事后均能实现作用最大化。其次加强网络反恐警务的技术交流，技术手段永远是首当其冲的重要方式，在警务领域不断更新反恐技术，研发网络防御工具，可建立国际性或区域性的网络警务技术开发研究合作交流培训，加快技术发展同时加强警务人员技能。最后配合国际警务制度制订完善国内的网络警务操作规范，衔接国内外的交流模式，完善警务交流体系。

2、倡导建立网络反恐公约

网络恐怖主义既是网络犯罪的分支，又从属于恐怖主义，随着互联网的普及，国际社会不断加强恐怖主义和网络犯罪的应对，因此针对中国网络恐怖主义的法律规制须借鉴国际社会现有的条约和解决机制。

在国际合作方面，首先中国应充分吸收现有国际条约和协商机制的经验。如《网络犯罪公约》，一方面对国际合作做出了突出贡献，对引渡、司法协助、数据保护等领域进行了规制，促进了成员国间的共享信息，为缔约国打击网络犯罪提供了直接的国际法依据，也为其他国家或地区的相关立法提供了借鉴作用。但另一方面网络犯罪公约制订至今近二十年，其内容有明显的滞后性，无法应对网络恐怖主义。因此中国在积极倡导建立国际性或区域性的顶层设计、网络反恐公约和反恐协调机制时，须促进消除国界壁垒制订专门的网络恐怖主义犯罪罪名，全面规制目标型网络恐怖主义和工具型网络恐怖主义。且规制要切合实际，能够有效提高公约实践执行能力。其次充分发挥已加入的条约组织，借助上合组织、“一带一路”建设，世界互联网大会等既有的组织或平台平衡发展网络反恐的治理模式。如上合组织成员国间的“互联网警察机构”，既能应对突发网络袭击，还能综合分析收集的情报，进而强化网络反恐的侦擦水平。针对2019年12月联合国大会通过打击网络犯罪的提案出现的反对声音，实质上在于如何平衡国家独立的网络主权和国际统一的网络监管权，以及发达国家和发展中国家互联网水平差距。在应对网络恐怖主义领域，国家让渡一部分主权，不仅不会威胁到国家的主权和根本利益，反而有助于实现国家利益的最大化。[43]无论是国际性组织还是地域性组织制订统一的网络恐怖主义规制条约合理让渡部分监管权是必然趋势。此外为平衡国家间的反恐力量差距，提高整体网络对抗能力，可建立国家间的帮扶模式，对于各国互联网发展水平进行划分，由互联网水平等级较高的国家帮助等级较低国家建立网络防护体系,并且要根据不同水平等级确认共同但有区别的责任。中国在推动国际网络前可通过点对点的合作带动面对面的合作，消解网络犯罪治理政策方面的体系分歧，为联合国治理机制的实施消除前期障碍。[44]

42) 皮勇：《网络恐怖活动犯罪及其整体法律对策》,《环球法律评论》2013年第1期，第9页。

43) 郑远民、朱红梅：《非传统安全威胁下国际法律新秩序的构建》,法律出版社2014年版，第186页。

44) 蔡高强、焦园博：《论联合国框架下网络犯罪国际治理的中国立场》,《中央民族大学学报(哲学社会科学版)》2019年第2期，第130页。

3、国际条约中的中国立场

对于反恐国际条约的加入与否以及相关条款的保留，中国须充分考量国家利益以及国家安全。在中国已加入的反恐国际条约中，对于部分条约的特定条款，中国持保留态度。反恐条约中中国在争端解决机制、中国特别行政区方面维持了原有权利以及行动自由状态。中国对于争端解决机制是呈现消极谨慎态度的，秉承中国一贯主张的对话方式，主张通过谈判等外交途径解决。

网络恐怖主义的发展趋势要求各国加强反恐国际合作和反恐共识，借助联合国的平台，突破意识形态和国界的壁垒，应对网络恐怖主义的周期性回流。未来中国须不断加强网络领域的国际反恐合作的主导能力，以中国和俄罗斯为代表的国家已向联合国提出建立国际性网络犯罪公约的提案，在未来国际谈判中既要坚持中国立场又要代表广大发展中国家立场，以国家安全和利益为核心。中国总体针对于国际反恐和打击犯罪条约执行效果较好，在对于条约的保留针对反恐和打击网络犯罪领域可采取更为积极的态度，平衡国家责任和国际社会责任，若必须声明对于争端解决机制的保留，则须提高说理性和透明性，减少对保留的笼统性表达。更为主动的倾向于“规则取向”，未来跨国性的网络恐怖主义案例中可提高对于国际法院在解决国际争端中的比例，以期更好的发挥中国角色。

网络反恐在实操性层面，笔者认为重点可先聚焦在刑事管辖权领域，中国传统的刑事管辖权在空间效力上以属地管辖原则核心，同时兼以属人管辖、保护管辖、普遍管辖原则。中国刑事管辖权的空间效力并不能适应网络恐怖主义犯罪的跨国性特点，以上四种管辖都存在一些限制，且属地管辖中行为地和结果地易于出现分歧。因此确立危害中国安全的网络犯罪的管辖权需要一定的立法标准，可以实害联系原则为基础，结合行为地和结果地共同确立管辖权。实害联系原则主张网络犯罪的管辖以犯罪行为对本国国家或公民的实际的“侵害或影响之关联性”为标准来确定是否具有刑事管辖权。[45]根据网址、域名、服务器所在地确定犯罪行为地，根据被侵入的系统、终端等确认结果地。互联网打破地域的物理界限，网络恐怖主义行为一旦发生，易出现多个行为地和多个结果地的情形。即便能够通过前述行为地和结果地的标准确认和区分，在之后的对于网络恐怖主义的犯罪规制中易产生管辖权的冲突，增加中国网络恐怖主义的治理难度。因此未来中国可根据实害联系原则，积极建立多边的协商机制，以直接故意的实害行为以及实害程度作为协商标准，防止各国在网络恐怖主义犯罪中管辖中的过度。

五、结语

互联网与社会活动愈发密切，大到国家治理小至个人生活都需要互联网的支持，近些年大数据、云计算等技术蓬勃发展，世界经济的发展愈发倚重互联网。但网络的发展是机遇和风险并行的，快速发展的结果也暴露出较多的网络安全问题以及网络风险隐患，其中恐怖主义与网络的结合对国家安全带来了严重威胁。

中国的恐怖主义呈现出民族分裂势力、宗教极端势力和暴力恐怖势力相结合的趋势，境外势力指导干预资助的特点明显，目前呈现的是工具型网络恐怖主义，即境外恐怖势力通过网络线上指导境内恐怖组织线下发动袭击的模式。2015年前后中国以新疆为中心的恐怖活动频发，严重的破坏了社会安定。中国虽然目前还未发生大规模的网络恐怖主义袭击事件，但是仍要高度警惕，做好防范工作，完善相关立法、总结经验加强重点地区反恐力度，建立健全情报制度，加强国际合作，保证信息公开，正确引导舆论，发展技术力量，整合资源形成各机构间多元化的打击防范体系。

在中国大力发展5G通讯技术的背景下，突破网络无序化和无边界的困境，实现网络恐怖主义有序化的防范和打击需要更全面的制度和技术支持，须立足中国国情，借鉴域外经验，完善立法体系，引导促进建立完善的一体化网络反恐模式。

45) 于敏：《对刑事管辖权新理论的思考》,《全国商情(理论研究)》2009年第22期，第128页。

[参考文献]

[1] 蔡高强、焦园博：《论联合国框架下网络犯罪国际治理的中国立场》,《中央民族大学学报(哲学社会科学版)》2019年第2期。
[2] 陈旻祥：《边疆民族地区宗教极端主义问题及其对策研究》,《法制与社会》2019年第24期。
[3] 陈钟：《论网络恐怖主义对国家安全的危害及其对策》,《江南社会学院学报》2004年第3期。
[4] 贾宇：《中国反恐怖主义法律问题研究》，中国政法大学出版社2018年版。
[5] 康均心、虞文梁：《大数据时代网络恐怖主义的法律应对》,《中州学刊》2015年第10期。
[6] 刘仁文：《刑事法治视野下的社会稳定与反恐》，社会科学文献出版社2013年版。
[7] 陆旭：《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》2015年第6期。
[8] 倪春乐：《比较与借鉴：论恐怖主义犯罪追诉中的恐怖组织认定》,《中国人民公安大学学报(社会科学版)》2012年第1期。
[9] 盘冠员、章德彪：《网络反恐大策略—如何应对网络恐怖主义》，时事出版社2016年版。
[10] 皮勇：《网络恐怖活动犯罪及其整体法律对策》,《环球法律评论》2013年第1期。
[11] 皮勇、杨淼鑫：《互联时代的微恐怖主义及其治理——兼评<刑法修正案(九)>和<反恐怖主义法>相关条款》,《刑法论丛》2016年第3期。
[12] 师维、孙振雷、孙卫华、张桂霞：《中国反恐怖主义法研究》，中国人民公安大学出版社2016年版。
[13] 宋汀、曹伟：《2018年上半年国际恐怖主义态势报告》,《中国信息安全》2018年第9期。
[14] 舒洪水、党家玉：《网络恐怖主义犯罪现状及防控对策研究》,《刑法论丛》2017年第3期。
[15] 田溪：《恐怖主义定义界定问题分析》,《法制博览(中旬刊)》2012年第5期。
[16] 王娜：《网络恐怖主义犯罪的刑事立法应对》,《犯罪学论坛（第二卷上）》，2015年。
[17] 王翔：《欧盟<通用数据保护条例>(GDPR)解读》,《法制博览》2018年第12期。
[18] 王秀梅、魏星星：《打击网络恐怖主义犯罪的法律应对》,《刑法论丛》2018年第3期。
[19] 王志祥、刘婷：《网络恐怖主义犯罪及其法律规制》,《国家检察官学院学报》2016年第5期。
[20] 应晨林：《完善我国网络反恐立法的思忖》,《网络空间战略论坛》2015年第8期。
[21] 于敏：《对刑事管辖权新理论的思考》,《全国商情(理论研究)》2009年第22期。
[22] 于冲：《网络犯罪罪名体系的立法完善与发展思路——从97年刑法到<刑法修正案(九)草案>》,《中国政法大学学报》2015年第4期。
[23] 于冲、黄晓亮、李源粒、李晓明：《网络犯罪的刑法回应与罪名架构（笔谈）》,《中国政法大学学报》2015年第4期。
[24] 张家栋：《当代恐怖主义的宗教根源》,《国际观察》2006年第2期。
[25] 郑远民、朱红梅：《非传统安全威胁下国际法律新秩序的构建》，法律出版社2014年版。

[26] 赵秉志、杜邈：《在联合国法律框架内进行反恐斗争——“全球反恐法律框架”学术研讨会综述》,《法学杂志》2008年第3期。
[27] 周展：《文明冲突、恐怖主义与宗教关系》, 东方出版社2009年版。
[28] 朱雁新：《国际法视野下的网络主权问题》,《西安政治学院学报》2017年第2期。
[29] 朱永彪、任彦：《国际网络恐怖主义研究》, 中国社会科学出版社2014年版。
[30] 朱永彪、杨恕：《网络恐怖主义问题初探》,《中州学刊》2006年第5期。
[31] John Arquilla, David F. Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001. Santa Monica, California.
[32] Nicholas Tsagourias, Russell Buchan, Research Handbook On Internet Law and Cyberspace, Eward Elgar Publishing.
[33] Weimann, Gabriel, Terrorism in cyberspace: the next generation, Woodrow Wilson Center Press, 2015.

[中文摘要]

中国对网络恐怖主义的法律规制研究*

马光** · 白雅慧***

美国“9.11”事件开启了全球反恐的序幕，恐怖主义逐渐成为重要的国际安全问题，影响社会和谐稳定，威胁人民生命财产安全。近几年，随着互联网发展进程的加快，恐怖主义和网络逐步结合，网络恐怖主义成为恐怖主义新的发展态势。目前中国网络恐怖主义仍属于工具型网络恐怖主义，即通过互联网实现线上联络和线下打击的恐怖主义模式。《刑法》、《反恐怖主义法》、《网络安全法》等法律为中国预防和打击恐怖主义提供了坚实的法律基础，但是对比国际立法应对措施中国仍有一定不足。首先，结合中国宗教特点和地区特点，列举目前网络恐怖主义的定义、通过实例逐一说明中国网络恐怖主义的特点和表现形式，突出网络在中国恐怖主义活动中呈现工具性作用。其次，基于目前重点立法领域分析中国网络恐怖主义的立法现状进而提炼存在的问题。最后，在分析前述问题的基础上提出相应的法律规制建议，在全球化的背景下中国须立足历史经验，吸收国际先进立法经验，完善中国的网络恐怖主义法律规制体系。

关键词：网络，恐怖主义，立法，规制，网络安全

* 本文系浙江大学“人工智能与法学专项课题”和“国际合作区域拓展计划-一带一路国家合作项目经费”研究成果。
** 马光，浙江大学光华法学院副教授，律师
*** 白雅慧，浙江大学光华法学院国际法研究生，通讯作者

[Abstract]

Research on Legal Regulations of Cyber Terrorism in China

Ma Guang* · Bai Yahui**

The "9.11" incident in the United States mark the beginning of the prelude of global anti-terrorism. Terrorism has gradually become an important international security issue, affecting social harmony and stability, threatening the safety of people's lives and property. With the acceleration of the development of the Internet, terrorism and the Internet are gradually being combined, and cyber terrorism has become a new development trend of terrorism. At present, China's cyber terrorism is still a tool type cyber terrorism, that is, the mode of online contact and offline attack through the Internet. Laws such as the “Anti-Terrorism Law” and “Network Security Law” provide a solid legal basis for China to prevent and combat terrorism. , but compared with international legislative response measures, China still has some deficiencies. Firstly, combining the characteristics of China’s religions and regions, the current definition of cyber terrorism is enumerated, and the characteristics and manifestations of cyber terrorism in China are illustrated one by one through examples, highlighting the instrumental role of cyber in our terrorist activities. Secondly, based on the current key legislative fields, this article analyzes the current status of China's cyber terrorism legislation and refines the existing problems. Finally, based on the analysis of the aforementioned issues, this article propose corresponding regulatory recommendations. In the context of globalization, China must base its historical experience, absorb advanced international legislative experience, and improve our cyber terrorism regulatory system.

Key words: Network, Terrorism, Legislation , Regulate, Cyber Security

* Ma Guang, Associate Professor of Guanghua Law School of Zhejiang University, Lawyer
** Bai Yahui, Graduate student of Guanghua Law School of Zhejiang University, Corresponding Author