网络恐怖主义与“一带一路”网络安全合作*

汪晓风

【内容提要】 网络恐怖主义是网络空间与经济社会运行融合和国际恐怖主义演变两大趋势互动的结果，当前网络恐怖主义主要表现为宣扬恐怖理念、招募组织成员、发布恐怖信息、传授恐袭技能等网络支恐活动。对“一带一路”合作而言，网络恐怖主义意味着助推地区恐怖主义势力发展，阻碍信息基础设施互联互通，干扰“一带一路”合作社会基础等不利影响。推动反恐和网络安全合作，可以提升“一带一路”倡议在促进共同安全方面的吸引力，保障“一带一路”合作项目顺利实施，预防恐怖主义在网络空间滋生和蔓延。作为“一带一路”倡议发起国，中国可以通过区域反恐合作和网络安全合作，建立打击网络恐怖主义的共识，促进应对网络恐怖主义的政策协调和机制合作。

【关键词】 “一带一路” 网络恐怖主义 反恐合作 网络安全合作

【作者简介】 汪晓风，复旦大学美国研究中心、复旦大学台湾研究中心副研究员

【中图分类号】 D815.5

【文献标识码】 A

【文章编号】 1006-1568-(2016)04-0116-17

【DOI 编号】 10.13851/j.cnki.gjzw.201604007

* 本文系国家社科基金一般项目“美国棱镜计划的系统分析及综合应对研究”（项目号：15BGJ049）的阶段性成果。感谢《国际展望》匿名评审专家及编辑部的宝贵意见和建议，文中错漏由笔者负责。

近年来，恐怖主义的发展日益与网络空间相融合，恐怖主义势力越来越频繁地使用互联网来传播恐怖主义理念、招募战斗人员和支持者、散布恐怖信息、施加政治影响，演化出以网络支恐为核心的网络恐怖主义形态，对国际社会构成新型威胁。同时，恐怖主义势力也从未放弃对关键信息基础设施和重要网络系统发动网络攻击的企图，给网络空间安全带来潜在风险。“一带一路”倡议覆盖亚、欧、非六十余个国家，是恐怖主义势力聚集和恐怖主义活动活跃的地区，防范和应对网络恐怖主义应当成为“一带一路”区域合作的重要内容。中国既面临恐怖主义的威胁，也是跨国网络攻击的受害者，作为“一带一路”倡议发起国，可在推动“一带一路”沿线国家合作应对网络恐怖主义方面发挥主导作用。笔者将重点探讨网络恐怖主义的演变和网络支恐活动的主要表现，网络恐怖主义对“一带一路”合作的影响，以及在“一带一路”倡议框架下应对网络恐怖主义的合作路径。

一、“一带一路”倡议面临网络恐怖主义威胁

作为网络与恐怖主义相结合的产物，网络恐怖主义是网络空间与世界经济社会运行日益融合和国际恐怖主义发展两大趋势互动演变的产物：一方面，互联网应用范围不断扩大和人类社会日益依赖网络空间，为网络恐怖主义提供了滋生的土壤；另一方面，面临国际社会联合打击压力，恐怖主义势力寻求利用新技术手段争取支持者和扩展影响力，也推动了网络恐怖主义的兴起。网络恐怖主义既是“一带一路”沿线国家正在面临的现实威胁，也是“一带一路”合作顺利推进需要化解的潜在风险。

（一）网络恐怖主义的演变

早在 20 世纪 90 年代中期互联网开始发展之初，一些国家就非常警惕关键信息基础设施和重要网络系统成为恐怖袭击目标的可能，并采取措施遏止恐怖主义和激进分子利用互联网来扩展恐怖和极端活动的能力，而这正是网络恐怖主义通过互联网制造社会恐慌和支持恐怖主义活动的主要体现。

作为互联网创始国和高度网络化的国家，美国在积极推广互联网应用的

同时，也认识到需要防范恐怖主义对计算机网络系统发动攻击的可能。巴里·科林（Barry C. Collin）首先提出网络恐怖主义的概念，并将其界定为网络与恐怖主义结合的产物。[①] 克林顿政府非常重视对关键信息基础设施的保护，重点是防止对关键信息基础设施的恐怖主义攻击，同时阻止恐怖主义分子获得先进的信息通讯技术。美国 1996 年《参与和扩展的国家安全战略》指出，要尽力防止恐怖主义和大规模杀伤性武器等破坏性力量对美国的重要信息系统构成威胁。[②] 1999 年《新世纪国家安全战略》认为，恐怖主义分子、犯罪集团或敌对国家可能发动网络攻击，从而对美国国家安全构成跨国威胁，“国家关键基础设施面临各种威胁，除了物理的攻击或破坏，还有来自恐怖主义分子或犯罪集团以及敌对国家的网络攻击威胁”，“各种复杂技术越来越容易获取意味着流氓国家和恐怖主义分子可以得到更大的破坏能力。”[③] “9·11”恐怖主义事件发生后，小布什政府将防止恐怖势力发动网络攻击作为反恐战略的重要内容，奥巴马政府则将恐怖主义和网络攻击提高到国家安全威胁的最高层级。美国的政策演变清晰地反映出网络恐怖主义的发展脉络。

对网络恐怖主义的早期关注主要是对恐怖主义分子发动网络攻击的担忧，认为恐怖主义分子可能通过入侵计算机系统、植入特洛伊木马和传播恶意病毒等方式，中断水利、电力、电信、金融等关键基础设施的运行，引发社会动荡和经济损失，或操控水坝和化工厂等设施的控制系统，制造重大安全事故和大规模人员伤亡。然而，迄今为止尚未有恐怖主义分子对关键信息基础设施和重要网络系统发动网络攻击、并造成重大经济损失和人员伤亡的实例。对这一现象，有两种解释：一是各国的严格保护使恐怖主义分子难以下手，因为那些关乎国计民生和国家利益的关键信息基础设施都是各国政府的保障重点，对支撑其运行的重要网络系统也采取高度严密的保护措施，甚

[①] Barry C. Collin, “The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge,” *Crime & Justice International*, Vol. 13, Issue 2, 1997, p. 16.

[②] U.S. White House, *A National Security Strategy of Engagement and Enlargement*, Washington, D.C., February 1996, p. 26.

[③] U.S. White House, *A National Security Strategy for a New Century*, Washington, D.C., December 1999, p. 14.

至从物理上与互联网隔离；二是恐怖主义分子之所以迄今未能成功实施对关键信息基础设施和重要网络系统的网络攻击，是因为恐怖主义组织无法获得组织大规模和高水平网络攻击的技术、人员和能力。在诸如利用震网病毒破坏伊朗核能设施、发动网络攻击致使爱沙尼亚和格鲁吉亚全国网络长时间中断运行等案例的背后，都有大国政府的支持和参与，而个人黑客、网络犯罪集团或是恐怖主义组织尚未掌握发动这种国家层级网络攻击的能力。

恐怖主义组织和恐怖主义势力转而越来越乐于和善于利用互联网作为支持恐怖主义活动的途径和手段，从基地组织通过网络聊天室和电子邮件与支持者联系、在新闻网站和论坛上发布恐怖主义信息、通过网络媒体公布斩首画面和基地首领本·拉登的音视频讲话，到“伊斯兰国”制作精美招募宣传广告、以网络支付和数字货币募集、运作和转移资金、通过云存储保存和分发培训录像、在社交媒体上与支持者互动等等，恐怖主义组织利用互联网进行信息传播、资金管理和在线交流越来越熟练，因此网络支恐活动逐步成为当前网络恐怖主义的主要表现方式，如何协调各方政策立场和形成联合行动能力，有效应对这类“软恐怖”活动是对当前国际反恐合作机制的新挑战。

（二）网络支恐活动的主要表现

网络支恐是当前网络恐怖主义的主要表现，即恐怖主义分子利用互联网开展招募、宣传、策划、洗钱、组织恐怖主义袭击等活动，这已经成为全球恐怖主义发展变化的重要特点，“一带一路”沿线的部分国家甚至成为网络支恐活动的策源地。

首先，宣扬和传播恐怖主义理念。当今世界是一个开放和多元的社会，信息来源广，传播速度快，恐怖主义组织认识到瞒骗和煽动已不能获得长期支持，需要对其核心理念和政治诉求进行包装，融入宗教、民族、文化和情感等易于传播和触及内心的内容，并赋予手段和目标的正当性和神圣色彩。互联网开放的信息发布机制和便捷的互动传播应用为恐怖主义宣扬扩展其理念诉求提供了便利。近年来，恐怖主义组织积极探索网络传播规律，寻找在海量信息中接触受众和保持黏性的方法。例如，“伊斯兰国”将系统阐述“建国”理念和实现途径的内容发布在其官方网站上，同时利用公共网络平

台推送短平快的言论信息。又如，联合国安理会认定的恐怖主义组织“东突厥斯坦伊斯兰运动（东伊运）”也很擅长运用网络进行恐怖主义支持活动，该组织运行的“以色列之声”宣传中心利用网络存储及分发暴力恐怖主义和宗教极端内容的资料信息。据中国公安部数据，“东伊运”从 2010 年到 2014 年在互联网上发布的恐怖主义音视频就高达 282 部，且数量逐年增多。[①] 恐怖主义组织还通过社交媒体向一些政府叫板，要求进行公开的“政策辩论”。

其次，招募恐怖主义组织战斗人员和追随者。互联网应用特别是社交媒体的普及，为恐怖主义组织通过网络平台招募新成员提供了非常有效的途径。据《纽约时报》报道，至 2015 年 8 月，估计有超过 4 000 名西方人奔赴叙利亚和伊拉克，其中女性超过 550 名。为了吸引年轻女孩，“伊斯兰国”精心拍摄了大量手拿武器、相貌英俊的圣战分子照片，加上富有诗意和浪漫气息的文字，让一些西方女孩认为有机会与帅气的极端武装人员相恋。对这些女孩而言，加入“伊斯兰国”是一种从父母及令她们失望的西方社会中解脱出来的途径。对“伊斯兰国”而言，招募到西方女性对提振士气大有帮助，因为可以显示圣战的吸引力，他们还可以用这些女孩来诱使更多追随者，“看，这些女孩选择圣战而非西方。”那些西方女孩用宗教和极端方式表达自己的叛逆，在她们的世界中，伊斯兰信仰就是朋克和摇滚，戴头巾则是解放自我，胡须则意味着性感。[②] 可见网络恐怖主义在利用虚拟空间和快捷网络宣传方面已经具有很强的系统性和煽动力。

第三，散布传播恐怖主义信息，施加政治和社会影响。恐怖主义采取所有手段的核心目的都是为了制造恐怖，而通过对社交媒体工具和云存储空间的恰当使用，可以达到放大恐怖效果和扩展传播范围的目的。因此，不难理解恐怖主义组织为何特别积极地认领各种具有强烈震撼效应的灾难、爆炸和恐怖主义袭击事件。随着网络技术的发展，恐怖主义组织越来越擅长运用最新的多媒体设计和制作技术，最大限度地将斩首、残杀和战斗的血腥和恐怖

[①] 2014 年 11 月 20 日中国公安部网络安全保卫局局长顾建国在乌镇互联网大会上的讲话，网络视频见 http://www.wicnews.cn/system/2014/11/19/020368140.shtml。

[②] Katrin Bennhold, “Jihad and Girl Power: How ISIS Lured 3 London Girls,” *The New York Times*, August 18, 2015, p. A1.

主义的场面渲染出来，从而对受害者家属、当事国和国际社会造成强烈的心理冲击。恐怖主义组织对于能够施加政治影响的技术和手段都毫不迟疑地加以使用。有评论认为，互联网特别是社交媒体已经成为“伊斯兰国”对国际社会和各国政府展开宣传战和心理战的场所。例如，2013 年 4 月 23 日，自称“叙利亚电子军”（Syrian Electronic Army）的恐怖主义组织侵入美联社推特官方帐号，并发推文称“白宫发生两次爆炸，奥巴马受重伤”，这一消息导致美国社会恐慌和股指大幅波动。[①] 由于互联网的开放性和一些国家给予网络传播不受约束的自由，恐怖主义组织在开放的社交媒体平台上发布信息和建立链接，将大量恐怖主义音视频资料存储在云存储空间，既规避了法律限制，又可以最大限度地扩大传播效果。

第四，传授恐怖主义技术技巧，训练恐怖主义袭击能力。恐怖主义组织通过录制音视频、编制手册教材，详解枪械、弹药、毒品等恐怖主义工具的制造和爆炸、绑架、恐吓等恐怖主义手段的运用，通过社区论坛发布、电子邮件群发、网络课堂教学等途径进行传播。如“东伊运”在推特上开设账户，并在专门时段详细介绍多种炸药的制作方式，节目音频被录制下来，作为恐怖主义技术训练教材转发。[②] 对于恐怖主义组织而言，通过网络传播暴恐手段，可以最大限度地扩大接受训练者的范围，并能解决传统恐怖主义训练活动组织周期长、费用高、风险大等问题。此外，恐怖主义分子还可以通过在线互动，将恐怖主义技术和工具的使用技巧和效果告知其他恐怖主义组织成员，达到相互学习的目的。

由于互联网发展提供的便利条件，网络恐怖主义团体运用网络进行支恐活动的能力、灵活度和影响力都在不断增强，而国际社会对于网络恐怖主义认知理解的差异、网络安全国际治理机制的缺失、各国互联网管理政策的差异，都给网络恐怖主义的滋生和蔓延留下了活动空间。

（三）网络恐怖主义对“一带一路”合作的威胁

[①] Stuster J. Dana, “Syrian Electronic Army Takes Credit for Hacking AP Twitter Account,” *Foreign Policy*, April 23, 2013, http://foreignpolicy.com/2013/04/23/syrian-electronic-army-takes-credit-for-hacking-ap-twitter-account/.

[②] 转引自 2014 年 11 月 20 日中国公安部网络安全保卫局局长顾建国在乌镇互联网大会上的讲话，网络视频见 http://www.wicnews.cn/system/2014/11/19/020368140.shtml。

“一带一路”沿线国家处于恐怖主义势力聚集和恐怖主义活动频繁的高风险地区，网络恐怖主义既是各国共同面临的现实威胁，也是区域合作有效展开的潜在障碍。

首先，网络恐怖主义的首要影响在于助推恐怖主义势力，威胁区域和平与稳定。“一带一路”倡议顺利推进的前提是一个和平稳定的地缘政治和安全环境。根据经济与和平研究所（Institute for Economics and Peace）《全球恐怖主义指数 2015》的数据，2014 年全球范围受恐怖主义影响指数排名前十位的国家几乎都在“一带一路”沿线区域。[①] 其中，伊拉克、阿富汗、巴基斯坦、叙利亚分列 1、2、4、5 位，印度、也门、泰国、菲律宾、乌克兰、埃及等多个“一带一路”沿线国家的恐怖主义影响指数也都在前 20 位，中国列第 22 位。这意味着“一带一路”合作顺利推进面临的首要安全威胁和地缘政治障碍就是恐怖主义，而当前最活跃的恐怖主义组织“伊斯兰国”又最善于运用网络支持恐怖主义活动。此外，“伊斯兰国”的网络支持者也主要分布在“一带一路”区域，美国布鲁金斯学会（Brookings Institution）的一份报告指出，从 2014 年 9 月到 12 月，推特上至少有 4.6 万个活跃的“伊斯兰国”支持者账户，这些账户既有“伊斯兰国”成员，也有与“伊斯兰国”并无直接联系但积极从事转发和传播“伊斯兰国”的宣传材料和招募信息的孤立支持者；从地理数据来看，最活跃的用户分布在沙特阿拉伯、叙利亚、伊拉克和美国。[②] 这都表明，与网络融合已经为恐怖主义提供了更多活动空间，对“一带一路”合作而言意味着长期和持续的隐忧。

其次，网络恐怖主义的直接影响在于威胁“一带一路”倡议的互联互通合作。“一带一路”沿线区域涉及国家众多，各国自然资源禀赋和政治文化传统千差万别，经济发展水平和基础设施状况各异，投资环境和市场容量也各有千秋。“一带一路”倡议将这些国家连接在一起，需要推出一系列有吸

[①] *Global Terrorism Index 2015: Measuring the Impact of Terrorism*, IEP Reports, No. 36, Sydney, New York and Mexico City: Institute for Economics and Peace, November 2015, http://economics andpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf.

[②] Cole Bunzel, “From Paper State to Caliphate: The Ideology of the Islamic State,” *Brookings Institution*, March 2015, http://www.brookings.edu/research/papers/2015/03/ideology-of-islamic-state.

引力、互补型、可持续的合作项目。“数字丝绸之路”构想是指促进“一带一路”沿线国家在数据信息服务、互联网业务和国际通信业务的互联互通的项目。[①] “数字丝绸之路”建设包括共同推进跨境光缆和洲际海底光缆等通信干线网络建设、完善空中和卫星信息通道、提高区域国际通信互联互通水平，扩大信息交流与合作，构建畅通、便利和开放的区域信息空间。显然，包括“数字丝绸之路”在内的互联互通项目需要置于完备的安全保障之下。如前所述，尽管迄今未有恐怖主义组织针对关键信息基础设施发动大规模网络攻击的案例，但显然恐怖主义势力并不会排斥或放弃这种选择，并将竭力获取相应的网络攻击能力。而对关键信息基础设施和重要网络系统的全方位保护往往需要巨大资金投入和人力支持，在政府治理不足或安全防范不到位的国家和地区，对关键信息基础设施直接的物理破坏也是一大隐忧。

第三，网络恐怖主义的长期影响在于干扰地区社会发展进程，威胁“一带一路”倡议的社会基础。网络恐怖主义的传播受众和宣传对象主要是年轻人。在一些社会转型或经济形势不稳的国家，部分年轻人由于对家庭、教育和就业的不如意及对社会秩序的不满，往往滋生报复社会和特定人群的心理，恐怖主义组织就针对这些年轻人精心描绘出一个可以随心所欲、摆脱规则束缚的理想世界，而发动袭击、毁灭和杀戮是到达该世界的必由之路，非常有蛊惑力的宣传往往促使一些涉世未深的年轻人以及被主流社会边缘化的人群投向恐怖主义组织。网络恐怖主义宣扬的理念是扭曲的、目标是荒诞的、手段是残暴的，但却极具诱惑力。在一些“一带一路”沿线国家，政治秩序不稳、社会思潮混乱、年轻人失业率居高不下，为网络恐怖主义滋生和蔓延提供了现实土壤。即便在与“一带一路”倡议相连接的欧洲发达国家，由于经济不景气造成的对社会不满，由于就业压力引发的民族主义排外情绪，也可能被恐怖主义势力利用，在网络空间形成合流。而这种可能为恐怖主义提供源源不断新生力量的社会发展进程，对于“一带一路”倡议的推进是非常不利的，“一带一路”倡议和进程已被一些恐怖主义组织宣扬为是经济资源掠夺和文化传统入侵。

[①] “数字丝绸之路”构想是中国国务院《周边国家互联互通基础设施建设规划》的一部分，由工业和信息化部参与制定，于 2014 年 11 月完成规划。

二、“一带一路”倡议下共同应对网络恐怖主义的意义

“一带一路”倡议是中国推动区域合作共赢和共同发展的战略构想，涵盖产能互补、交通基础设施建设、信息基础设施互联互通等广泛领域的合作，这些合作倡议与区域国家寻求发展的共同愿望和切实需求相契合，因而受到国际社会的广泛关注和沿线国家的普遍欢迎。但迄今为止推出的“一带一路”合作构想主要侧重基础设施和经贸合作，能否及如何设置安全议题尚未纳入议程。也有观点认为，“一带一路”倡议应充分重视地缘政治冲突、恐怖主义、有组织犯罪等各种地区安全问题，并从提供安全公共产品的角度加以应对。[①] 从网络恐怖主义对地区安全和区域合作的影响来看，在“一带一路”倡议中纳入共同应对网络恐怖主义的内容不仅必要，而且可行。

（一）在“一带一路”倡议框架下应对网络恐怖主义的必要性[②]

一方面，“一带一路”倡议需要全方位的安全保障，遏制网络恐怖主义的活动可以为合作项目的顺利实施和共享设施的稳定运行提供更好的支持，这可以归结为一种保障性作用。

如前所述，对网络空间进行破坏或加以利用是网络恐怖主义的两大表现。因此，打击网络恐怖主义既可以阻止恐怖主义势力攻击信息基础设施，也可以削弱恐怖主义势力利用网络组织和支持恐怖主义活动的能力。关键基础设施的互联互通是“一带一路”倡议的重点合作领域，而信息基础设施又是关键基础设施的核心和枢纽，网络空间与信息基础设施更广泛的连通性和更便利的互操作性是一种普遍需求。这一趋势一定程度上赋予人们通过信息系统管理大规模关键基础设施的能力，也使得在信息化程度比较高的国家和行业中跨部门和跨国界存取海量数据成为事实和进一步发展的方向。“一带一路”倡议也可以看作是一个将区域以及全球的先进经验和最佳实践逐步推

[①] 参见刘海泉：《“一带一路”战略的安全挑战与中国的选择》，载《太平洋学报》2015年第2期，第74-77页。

[②] 感谢匿名评审指出共同应对网络恐怖主义对“一带一路”倡议的保障性作用和预防性作用。

广普及的过程，中国政府明确将加强与“一带一路”沿线国家的网络发展合作，以图打通“一带一路”覆盖区域的“血脉经络”。[①] 在这一开放程度高的环境中，一些重要信息系统往往成为别有用心者觊觎的目标，而网络系统互操作性强的特性也给恶意攻击者以可乘之机，恐怖主义势力一直在网络空间或通过网络寻找可以造成社会恐慌和带来巨大损失的机会。因此，对于“一带一路”倡议的过程、成果和以互联互通联结起来的一体化基础设施，需要不断提高区域性安全公共产品的供给。只有这样，推进“一带一路”倡议的数据、信息、运输、交通、物流才能获得更安全的环境。

网络恐怖主义已经将网络空间作为联络、组织和运行的场所。近年来一系列重要的恐怖主义袭击事件都显示，恐怖主义组织对网络的运用频率不断提高。如 2015 年 11 月 13 日，法国巴黎系列恐怖主义爆炸事件后，“伊斯兰国”公布了一份安全手册，其中包含使用加密浏览器和邮箱进行沟通，利用脸书和推特的注意事项等。“伊斯兰国”还在跨平台即时通讯工具 Telegram 中创建了一个帮助桌面，为组织成员和支持者提供技术支持和实时指导，这充分显示恐怖主义组织对网络空间的依赖性在逐步增强。因此，促进区域网络安全合作和共同打击网络恐怖主义，防止网络空间成为恐怖主义势力藏匿和活动的场所，也将为“一带一路”合作提供安全保障。

另一方面，“一带一路”倡议是一个不断推进的长期进程，打击网络恐怖主义可以降低因利益纠纷、社会矛盾和国家间分歧引发激进主义和恐怖主义势力在网络空间滋生和蔓延的几率，这可以归结为一种预防性作用。

网络空间的发展创造了一个开放性的平台，其广泛连接、快速传播和信息冗余的特性，往往使反政府和无政府的极端思想更易于得到推崇和效仿。而网络恐怖主义正是利用这一特性，将社交媒体和即时通讯等网络应用作为其宣传造势的平台。“一带一路”倡议基于区域国家自然禀赋互通和竞争优势互补的便利条件，不断发现和扩展利益交汇点。但一个不容忽视的事实是，区域国家的政治制度、社会文化和意识形态存在着巨大差异。在这样的环境中推动合作，将面临更为复杂的政治和舆论阻力，各社会群体对“一带一路”

[①] 鲁炜：《坚持尊重网络主权原则 推动构建网络空间命运共同体》，载《求是》2016 年第 5 期，第 35 页。

倡议的认知不一，甚至有人将“一带一路”倡议看作中国意图控制亚洲的“新马歇尔计划”。[①] 实际上，认知差异并不会构成不可逾越的障碍，而利用认知差异诱导极端情绪，则是网络恐怖主义善用的手法。因此，共同打击网络恐怖主义，可以促进在区域内建设开放、安全和共享的网络空间，压缩网络上极端势力和恐怖主义的活动空间。

预防性作用还可体现在对于其他网络相关风险的防范上，如发展区域网络金融和在线支付等的互联互通是“数字丝绸之路”的重要内容，而恐怖主义组织也日益频繁地通过网络途径进行筹措、转移和分发资金。因此，网络基础设施越完善，网络应用越丰富，对于监控和整治网络不法行为的能力要求也就越高，共同打击网络恐怖主义也是在区域内促进这种能力建设的一个重要方面。

（二）在“一带一路”沿线国家合作应对网络恐怖主义的可行性

网络恐怖主义的负面影响对于“一带一路”倡议的推进是不利因素。但从积极角度看，“一带一路”倡议是区域综合发展战略，共同应对网络恐怖主义也有可能成为推动“一带一路”倡议的推动力，如：恰当设置议程，促进区域形成合作应对网络恐怖主义共识，塑造有助于反恐和网络安全合作的“一带一路”文化，等等。建立区域网络治理公共政策协调机制，将有助于压缩网络恐怖主义的活动空间，从而形成更富有吸引力的“一带一路”合作预期。

一方面，“一带一路”倡议是开放性的合作构想，只要有助于区域国家经济和社会发展、有助于地区和平与稳定的合作都可考虑纳入“一带一路”倡议的合作框架。汇聚遭受恐怖主义威胁、有共同应对恐怖主义意愿的政府、组织和机构，构建行之有效的预防打击网络恐怖主义的机制，也符合“一带一路”倡议关于构建弹性开放和包容合作的精神；而由“一带一路”合作供给网络安全和打击恐怖主义的公共产品，将反过来促进“一带一路”倡议的黏性和活力。尽管“一带一路”倡议是促进区域经济、贸易和金融合作的构

[①] Michele Penna, “China’s Marshall Plan,” *World Politics Review*, December 9, 2014, http://www.worldpoliticsreview.com/articles/14618/china-s-marshall-plan-all-silk-roads-lead-to-beijing; “China"s Marshall Plan: Xi Jinping Bids to Take Leadership away from the U.S.,” *Wall Street Journal*, November 11, 2014, http://www.wsj.com/articles/chinas-marshall-plan-1415750828.

想，安全议题并没有成为当前倡议的核心内容。但无论是促进互联互通的关键基础设施建设，还是削减关税壁垒促进市场公平的经贸合作，或是增加区域国家之间的政治互信，都有其内含的安全保障需求；甚至一个国家的政治安全环境也是能否得到投资机会的首要条件。

另一方面，网络恐怖主义跨越网络安全与恐怖主义两大领域，都是威胁当今国际和平与稳定的全球性公共问题，但相关认知差异较大且各方政策协调较弱，以“一带一路”倡议的合作模式或可探求有效化解网络恐怖主义攻击和网络恐怖主义传播威胁的可行之路。

就维护网络安全而言，既包括整个网络环境的连通、稳定和安全，也包括数据处理、存储和传递的完整、保密和安全，应对既可能攻击关键信息基础设施、也可能进行网络支恐活动的网络恐怖主义。无论是网络安全国际治理机制的建设，还是各国政策法规对网络行为合法性的规定，都远远不能适应网络恐怖主义不断蔓延的现实。推动网络安全国际合作面临的最大障碍是，各国政府难以在网络行为规则上达成一致。例如，网络自由表达是一个普遍接受的原则，但如何不使网络信息传播威胁社会稳定和政治秩序，区域各国的认知和政策就有很大差异，特别是 2011 年西亚北非的“阿拉伯之春”促使域内国家普遍谨慎看待网络空间的信息传播。对于阻止和防范为恐怖主义提供支持和便利的网络活动，国际社会已经达成了较多共识。联合国安理会 2129 号决议《恐怖主义行为对国际和平与安全的威胁》显示，国际社会对于打击网络恐怖主义持一致支持态度；该决议对恐怖主义分子通过互联网实施煽动、招募、资助或策划活动等恐怖主义行为表示严重关切，明确要求联合国反恐机构会同各国政府和有关国际组织加强对网络支恐活动的打击力度。[①]

就打击恐怖主义而言，区域国家在是否认定一些实施暴恐行为的组织为恐怖主义组织的问题上，也往往根据其自身利益诉求和历史渊源而采取不同的标准，这为打击恐怖主义的区域合作设置了障碍。而对于网络恐怖主义的

[①] 《恐怖主义行为对国际和平与安全的威胁》，联合国安全理事会第 2129（2013）号决议，2013 年 12 月 17 日，http://www.un.org/zh/documents/view_doc.asp?symbol=S/RES/2129(2013)。

行为，无论网络支恐或网络攻击，在绝大多数国家都被认定为违法犯罪行为，都可以在双边刑事司法互助的框架下达成合作。如果区域国家在合作打击网络犯罪的层次上打击网络恐怖主义的活动，也可以大大削弱恐怖主义的活力和影响力。

三、“一带一路”合作应对网络恐怖主义的路径

网络恐怖主义难以得到有效遏制有多方面的原因，包括网络空间的虚拟特性和网络活动的跨国特性、各国政府网络治理理念和网络治理能力的明显差异、全球和区域网络安全合作缺失等。在“一带一路”沿线国家所构成的区域，这些因素尤为明显。应对网络恐怖主义需要综合治理，既要从反恐合作角度打击网络恐怖主义，也要从网络安全合作角度促进区域国家网络空间公共政策协调。

（一）应对网络恐怖主义的反恐合作

网络恐怖主义首先是恐怖主义的一种表现形式，因而在“一带一路”沿线区域促进反恐合作，是防范和遏制网络恐怖主义影响的有效途径。这可以从两个方面加以考虑。

一方面，促进区域共同安全理念与“一带一路”倡议相结合。发展和安全是“一带一路”合作的两大驱动力。从发展角度看，共建“一带一路”“顺应世界多极化、经济全球化、文化多样化、社会信息化的潮流，秉持开放的区域合作精神，致力于维护全球自由贸易体系和开放型世界经济。”[①] 从安全角度看，“一带一路”沿线国家中，部分国家政局不稳，部分地区极端势力和恐怖主义势力强大，部分国家的经济和社会发展深受恐怖主义之害。因此，以“一带一路”倡议为契机，在“一带一路”沿线区域形成应对网络恐怖主义的共识，有助于地区安全和稳定，也可以为“一带一路”倡议的推进提供更为广泛的动力。将对地区和平与发展构成共同威胁的网络恐怖主义纳

[①] 中国国家发改委、外交部、商务部：《推动共建丝绸之路经济带和21世纪海上丝绸之路的愿景与行动》，2015年3月28日。

入“一带一路”倡议，不仅能够加深“一带一路”沿线国家的发展共同体意识，也能够促进地区安全共同体意识，进而形成更具感召力和凝聚力的命运共同体意识。这种命运共同体意识与中国政府构想从亚洲到世界的未来发展趋势是一致的，“面对风云变幻的国际和地区形势，要把握世界大势，跟上时代潮流，共同营造对亚洲、对世界都更为有利的地区秩序，通过迈向亚洲命运共同体，推动建设人类命运共同体。”[①]

另一方面，促进将打击网络恐怖主义纳入现有全球和区域反恐合作议程。上海合作组织是区域反恐合作的重要机制，也在探索合作应对网络恐怖主义中积累了一些经验。2006 年 6 月，上海合作组织各国元首签署《关于国际信息安全的声明》，指出“各成员国在国际信息安全的关键问题上立场相近，愿在本组织框架内共同努力，应对新的信息挑战和威胁”，声明还决定建立成员国国际信息安全专家组，制定信息安全行动计划。2008 年 5 月，上海合作组织成员国国防部签署合作协定，决定加强应对地区安全面临的新挑战、新威胁的行动，各国国防部制订并落实在相关领域加强合作的具体计划，包括打击“三股势力”的合作以及保障国际信息安全行动计划。2009 年 6 月，上海合作组织成员国签署《保障国际信息安全政府间合作协定》。2013 年上海合作组织成员国元首签署《关于构建持久和平、共同繁荣地区的宣言》，强调成员国反对将信息和通信技术用于危害成员国政治、经济和社会安全的目的，防止利用国际互联网宣传恐怖主义、极端主义和分裂主义思想的一致立场。上海合作组织在多边合作应对网络安全和恐怖主义相结合方面的实践和探索，可以为“一带一路”倡议框架下的反恐合作提供经验参考和平台支持。

（二）应对网络恐怖主义的网络安全合作

“一带一路”沿线国家合作加强网络安全防御的能力建设，有助于提升区域整体网络安全水平，这种安全能力既包括技术手段，也包括政策协调和制度安排，还包括网络威胁信息和最佳实践的共享。

首先，在“一带一路”沿线区域形成打击网络恐怖主义共识。恐怖主义

[①] 习近平：《迈向命运共同体 开创亚洲新未来——在博鳌亚洲论坛 2015 年年会上的主旨演讲》，载《人民日报》2015 年 3 月 29 日，第 2 版。

是世界经济社会运行肌体上的一颗毒瘤，网络恐怖主义则是其新变种，应对网络恐怖主义不仅需要继续推动国际反恐合作，还需要应用网络安全治理的新途径和新方法。防范恐怖主义势力破坏网络或利用网络的活动，一个很大的障碍是恐怖主义势力利用网络途径传播极端理念与网络言论自由难以区分，在一些国家甚至受到法律保护。2014 年 12 月，印度警方以涉嫌发布“伊斯兰国”的残忍信息为由逮捕了推特（twitter）博主迈赫迪 •比斯瓦斯（Mehdi Masroor Biswas）。比斯瓦斯运营的推特账号有 1.77 万粉丝，发布数千条和“伊斯兰国”有关的推文，月浏览量超过 200 万次，该账号实际上充当了“伊斯兰国”的宣传窗口和恐怖主义分子间的沟通桥梁。比斯瓦斯在推特上的活动危害极大，但比斯瓦斯既不是恐怖主义分子，与“伊斯兰国”也没有直接联系。印度学者阿贾•萨尼（Ajai Sahni）表示，印度现有法律难以对比斯瓦斯定罪，“审判过程将会非常漫长，……而且印度并没有取缔‘伊斯兰国’。”[①] 对于这类危害极大的网络支恐行为，应当从促进区域国家间网络安全立法和网络管理政策的协调着手，阻止通过网络传播暴力恐怖主义信息，压缩以网络自由表达为名行网络支恐之实等网络恐怖主义行为的生存空间。

其次，在“一带一路”区域倡导网络空间国际行为准则。建立国际共享的网络空间行为准则是实现网络空间治理的重要途径，是构建网络恐怖主义无法立足的网络环境的必要条件，也是共同应对网络犯罪和网络恐怖主义的基础。由于主要网络大国在网络战略上的理念、利益和目标各异，国际社会制定网络空间行为准则的努力迄今收效甚微。中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦等国于 2011 年向联合国大会提交了一份《信息安全国际行为准则》议案，提案的核心是尊重各国在网络空间的主权，发挥联合国在网络规则制定上的主渠道作用。[②] 针对网络恐怖主义不断蔓延的形势，议案建议“合作打击利用信息通信技术包括网络从事犯罪和恐怖主义活动，或传播宣扬恐怖主义、分裂主义、极端主义的信息，或其他破坏他国政治、经济和社

[①] Ajai Sahni, “The Hatred Comes Home,” *South Asia Intelligence Review*, Vol. 13, No. 25, December 22, 2014, http://www.satp.org/satporgtp/sair/Archives/sair13/13_25.htm.

[②] 马晓天：《网络安全离不开国际合作》，载《人民日报海外版》2012 年 5 月 30 日，第 1 版。

会稳定以及精神文化环境信息的行为。”[①] 美国国会有议员认为“该行为准则为一国政府排他性地控制（本国）互联网资源寻求国际合法性，对互联网信息自由流动构成了威胁，并将损害自由表达的权利”。[②] 2015 年 1 月，中国、哈萨克斯坦、吉尔吉斯斯坦、俄罗斯、塔吉克斯坦、乌兹别克斯坦等国将该行为准则更新后再次提交联合国大会，美国政府仍以“使政府控制网络资源合法化和限制网络基本自由”为由表示担忧，[③] 美国的固执己见已经阻碍了网络空间安全治理的国际合作进程。由于该行为准则提案国均为“一带一路”沿线国家，在应对网络恐怖主义问题上已有广泛的一致意见，可推动该议案关于网络安全行为准则的内容在“一带一路”沿线区域的双边和多边议程进行广泛讨论，进而扩大共识。

第三，在“一带一路”沿线区域共享网络安全治理最佳实践。网络空间的开放性和管理滞后于技术发展的现实，往往被网络恐怖主义所利用。迄今为止，各国治理网络空间的政策法规都不尽完善，网络应用和信息传播的技术性特征也使得一些国家在应对网络突发事件和跨境网络监管时显得无能为力或无从下手。因此，将一些行之有效的政策法规、制度设计、应对方案、技术手段在区域层面进行推广，有助于增强各国网络空间治理能力，提升区域应对网络恐怖主义的整体水平。针对中国境内恐怖主义、分裂主义和极端主义“三股势力”运用网络传播恐怖主义音视频和相互勾连的态势，中国政府出台一系列打击通过包括网络途径在内的传播恐怖主义音视频的政策措施，对恐怖主义音视频的界定、传播、持有、存储作出了具体规定。应当说，中国建立了相对完善的立法和行政措施，对网络恐怖主义内容进行了清晰的界定，对可能为网络支恐活动利用的网络平台加强了管理，要求社交媒体和

[①] 联合国大会文件：《信息安全国际行为准则》（A/66/359），2011 年 9 月 12 日，http://www.un.org/zh/documents/view_doc.asp?symbol=A/66/359。

[②] U.S. House, 112th Congress, *H.RES.628 - Expressing the Sense of the House of Representatives that the United States Should Preserve, Enhance, and Increase Access to an Open, Global Internet*, April 19, 2012, https://www.congress.gov/bill/112th-congress/house-resolution/628.

[③] 美国国务院副发言人玛丽·哈夫（Marie Harf）在 2015 年 3 月 2 日例行记者招待会上回答关于中俄《信息安全国际行为准则》问题时的表态。Marie Harf, Deputy Spokesperson, Daily Press Briefing, Washington, D.C., March 3, 2015, http://www.state.gov/r/pa/prs/dpb/2015/03/238132.htm.

网络存储的运营者及时清理恐怖主义音视频和文字内容，有效地打击了网络恐怖主义的影响力和活跃度。将这些行之有效的方法在“一带一路”沿线国家加以交流和推广，可以提升整个地区应对网络恐怖主义的水平。

结 束 语

“一带一路”倡议是中国政府基于塑造和平发展、互利共赢理念的区域合作构想，是中国国家发展战略的外向延展，扩大和深化对外合作、确立开放发展新方向的重大布局。能否契合和满足区域国家对发展与和平的全面追求，是“一带一路”倡议能否获得持久动力的根源。作为倡议发起国，中国应综合考虑“一带一路”倡议推进中的机遇与风险，主动提供公共产品以争取应对各种安全威胁的主导权。同时，中国既是网络攻击的主要对象，也是恐怖主义的受害者，因此也负有应对网络恐怖主义的双重责任。例如，以“东伊运”为代表的东突恐怖主义势力将互联网作为组织、联络和训练的重要平台，不仅威胁中国国家安全，也威胁地区安全与稳定。网络恐怖主义的跨国性和虚拟特性意味着中国的应对也必须获得相关国家的支持。从国际层面来看，网络恐怖主义已经是全球性威胁，“打击网络恐怖主义是国际反恐斗争的新课题、新任务、新挑战，国际社会既需延续应对传统恐怖主义的策略和方法，又要针对网络空间特征和网络恐怖主义活动特点，找准突破口和发力点，拿出新思路和新举措。”[①] “一带一路”倡议下的反恐和网络安全合作，理应成为探索应对网络恐怖主义新思路和新举措的先行者。

[收稿日期：2016-03-18]
[修回日期：2016-04-11]
[责任编辑：樊文光]

[①] 中国外交部副部长张业遂2014年11月17日在北京“全球反恐论坛”打击网络恐怖主义研讨会上的发言，见《“全球反恐论坛”打击网络恐怖主义研讨会在京举行》，人民网，2014年11月18日，http://world.people.com.cn/n/2014/1118/c157278-26048316.html。

confronted with challenges. China should improve its imbedded agenda-setting capability, foster its international discourse power, and build a dynamic coalition, so that the Western-dominated global governance can be transformed into a co-governance by all parties concerned.

KEY WORDS: International Organization, International Regime, Chinese Diplomacy, Regime Reshaping, Regional Organization.

Cyberterrorism and Cybersecurity Cooperation under the One Belt and One Road Initiative

WANG Xiaofeng

ABSTRACT: Cyberterrorism originates from the interaction of two major trends: the integration of cyberspace and the running of economy and society, and the evolution of international terrorism. Current cyberterrorism mainly takes the form of cyber-enabled activities to spread terrorist ideology, to recruit members, to share terror information, and to teach terror attack skills. Cyberterrorism poses serious challenges to the One Belt and One Road Initiative in that it could hinder the interconnection of information infrastructure and undermine the social basis of the Belt and Road cooperation. Encouraging the cooperation on counterterrorism and cybersecurity can promote the appeal of the Belt and Road initiative by ensuring common security, securing the successful establishment of the Belt and Road cooperation projects, and preventing the rise of terrorism in cyberspace. As the initiator, China is better positioned to build broad-based consensus and facilitate policy coordination and institutional cooperation in countering cyberterrorism, through regional counterterrorism and cybersecurity cooperation.

KEY WORDS: One Belt and One Road Initiative, Cyberterrorism, Counterterrorism, Cybersecurity Cooperation.