第一章
网络恐怖主义的基本概念

20世纪40年代问世的通信与信号处理学科的采样定理，又称香农采样定理、奈奎斯特采样定理，“为数字化技术奠定了重要基础”。采样定理说明了采样频率与信号频谱之间的关系，是连续信号离散化的基本依据。就其实质而言，这一定理“在数字式遥测系统、时分制遥测系统、信息处理、数字通信和采样控制理论等领域得到广泛的应用”，为数字化技术的发展提供了重要理论依据。《数字化生存》(*Being Digital*)[①]一书是中国内地普遍认可的论述“数字化”的经典作品。数字化技术的发展为计算机、多媒体、信息、软件技术以及网络技术等的发展提供了基础的技术支持，也为其他技术的发展指明实现数字化的便捷路径。

数字化进程在信息传播方式的演变过程中充当了非常重要的角色，特别是对媒介技术的发展产生了重要的影响，也为网络恐怖主义通过网络媒介的发展提供了技术可能。同时，网络的现状与未来发展趋势，为网络时代恐怖主义通过网络手段实现其传播观念、策划行动、实施攻击等提供了便捷，更对各国防范网络恐怖主义提出了挑战。各国在认识和防范网络恐怖主义的实践中不断探索新途径，而在学界，交叉学科研究在这个历史时期的盛行，为网络恐怖主义研究带来了新的思路和方法，也为网络恐怖主义研究的历史呈现提供了现代性的可能。

---

① 尼葛洛庞帝．数字化生存[M]．胡泳，范海燕，译．海口：海南出版社，1996.

第一节　网络恐怖主义的定义

“网络恐怖主义”作为术语最早出现于20世纪80年代后期，但是，直到90年代初期才随着相关研究的深入而广为人知。[①] 2008年11月，印度孟买发生了恐怖袭击，这次恐怖袭击与因特网有着密切的联系，恐怖分子在策划袭击时通过谷歌地球查看目标位置并进行模拟演练，国外的袭击策划者还通过网络指挥具体行动。[②] 这一事件引起世界各国的广泛关注，对网络恐怖主义的研究开始进入更多国家政府的关注视野。网络恐怖主义是一个具有很大模糊性且有很大争议的概念，人们的认识目前还不统一，因此，对其的解释也存在不同版本。而且，随着网络恐怖主义的演化与变革，在不同历史时期和不同国家，就算是既有的定义，其内涵和外延也会产生变化。总之，网络恐怖主义的定义，包括内涵和外延，在逐渐得到补充和完善。

一、国外对网络恐怖主义的定义

“网络恐怖活动”这一名词最早是由美国信息战专家斯瓦特在其所著《信息战争》一书中提出的，该书稿交付出版社的时间正是美国启动“信息高速公路”的1993年。[③] 这表明，美国在迈出信息化进程的第一步时就已经意识到新的威胁，有预见性地确立了信息安全观念。

美国专家学者对网络恐怖主义研究的时间相对较早，文献数量相对丰富。在1996年美国伊利诺伊大学召开的第11次犯罪公正国际学术年会上，有学者讨论了网络中的恐怖主义，这一主题在后来的年会中得以延伸。

中国学者相关研究的文献显示，美国加州安全与情报研究所的资深研究员巴里·科林(Barry C. Collin)在1986年提出了“网络恐怖主义”(cyber-terrorism)这

① 朱永彪，任彦．国际网络恐怖主义研究[M]．北京：中国社会科学出版社，2014：4-5.

② 千省利，邵梦．网络恐怖主义法律问题研究[J]．信息网络安全，2008(2).

③ 何方明，侯晓娜．美国反网络恐怖活动的情报工作及对我国的启示[J]．江西公安专科学校学报，2009(1)：56-59.

个术语，并对它做了初步界定。但是，当时这一术语并没有引起人们的注意。直到1996年，科林对网络恐怖分子将会发动袭击的方式做了较为生动详细的描绘之后，“网络恐怖主义”一词才开始见诸学者文章与媒体报道。伴随着世界范围黑客行为的增加，美国学者、媒体对“电子珍珠港”的渲染，以及关于网络战研究的深入，“网络恐怖主义”一词开始引起更多人的注意。特别是美国“9·11”事件后，“网络恐怖主义”一词频繁出现于东西方话语体系。

虽然如此，东西方学界和业界都未能就“网络恐怖主义”的定义形成共识。资料显示，界定网络恐怖主义的有三类主体：第一类是政府部门和相关机构，如美国联邦调查局（FBI）、美国战略与国际研究中心（CSIS）等，对网络恐怖主义给出官方定义和解释。第二类是法律法规等文件，包括2001年10月26日由美国总统乔治·沃克·布什签署颁布的国会法案（Act of Congress）《美国爱国者法案》（*USA PATRIOT Act*），其正式的名称为《使用适当之手段来阻止或避免恐怖主义以团结并强化美国的法律》（*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*），将网络恐怖主义列为正式的法律术语。第三类是学术界、业界的专家学者和相关研究人员，如美国反恐专家巴里·科林、多罗西·邓宁等。

（一）组织机构对网络恐怖主义的定义

从1963年起，在联合国的支持下，16个国际公约将特定的恐怖主义行为规定为刑事犯罪。此后，在各国参与下相继制定和颁布了一系列国际公约和联合国决议，共同建立了全球反恐准则。而且，随着新媒体形态包括社交媒体等的发展，联合国致力于铲除恐怖主义思想根源，抑制恐怖主义、宗教极端主义等在网络空间的传播。国际社会已经注意到恐怖活动组织越来越多地利用互联网招募成员，进行煽动、筹资和筹划等恐怖活动，如联合国安理会第1963号决议、第2129号决议、第2133号决议等，要求成员国采取措施防止网络恐怖活动。

2013年12月，联合国安理会通过第2129号决议，强调国际社会应继续将打击恐怖主义作为工作重点。安理会成员一致同意在第2129号决议中写入中国常驻联合国代表刘结一提出的关于“当前恐怖组织和恐怖分子利用互联网发布音频、视频等煽动、策划或实施恐怖活动”等内容。这是安理会决议首次明确要求各国就加强打击网络恐怖主义采取具体措施，对国际社会进一步打击恐怖组织和恐怖分子利用互联网从事恐怖活动具有重要意义。

2013年9月，第68届联合国大会进行《联合国全球反恐战略》第四次评审并通

过决议，要求各国关注恐怖分子利用互联网等信息技术从事煽动、招募、资助或策划恐怖活动，各国、国际组织及私营部门等应合作应对，并根据中国提出的修改意见，首次在全球反恐战略的框架内写入打击网络恐怖主义的内容。

2016 年 1 月，联合国秘书长潘基文向联合国大会提交《防止暴力极端主义行动计划》。该行动计划呼吁国际社会采取一致行动防止暴力极端主义，并向各国和地区提出建立各自的行动计划建议。潘基文在联合国大会上介绍这一行动计划时说，暴力极端主义是对《联合国宪章》的直接攻击，对国际和平与安全构成严重威胁，“伊斯兰国”(ISIS)、“博科圣地”等团体的罪行惨无人道，令人震惊。潘基文说，暴力极端主义并不局限于某一特定宗教、国籍或种族，应对这一挑战是联合国的核心工作。这一行动计划通过实际和综合性手段应对暴力极端主义的驱动因素，为各国在国家层面应对这一问题提出了 70 多项具体建议。这些都为在联合国框架下开展国际反恐合作提供了依据。同年 5 月，联合国安理会就“反击恐怖主义言论和意识形态”举行公开辩论。

联合国反恐任务实施力量工作组(CTITF)以列举的形式将网络恐怖主义行为界定为四类：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；为了恐怖活动的目的将互联网作为其信息资源进行使用；将使用互联网作为散布与恐怖活动目的有关信息的手段；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。[①]

美国联邦调查局和国防部(DOD)是美国的反恐前锋，对网络恐怖主义做了更详细的定义。[②] 美国联邦调查局给网络恐怖主义的定义是：为实现特定的宗教、政治或意识形态的目的，一些非政府组织或秘密组织对信息、计算机系统、计算机程序和数据所进行的有预谋、含有政治动机的攻击，以造成严重的暴力侵害。美国国防部给网络恐怖主义的定义是：利用计算机和电信能力实施的犯罪行为，以造成暴力和对公共设施的毁灭或破坏来制造恐慌和社会不稳定，旨在影响政府或社会实现其特定的政治、宗教或意识形态目标。此外，一些研究机构也尝试界定网络恐怖主义。美国战略与国际研究中心认为：网络恐怖主义是应用计算机网络工具关闭一国基础设施(能源、交通、政府运营等)或者胁迫、恐吓政府或普通民众。

---

① 皮勇．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[J]．政法论丛，2015(1)：68-79.

② 黎雪琳．网络恐怖主义探析[J]．广西警官高等专科学校学报，2008(1)：17-20.

（二）各国法律法规等文件对网络恐怖主义的定义

2000年2月，英国在《反恐怖主义法案2000》（*Terrorism Act* 2000）中第一次从法律上正式明确提出“网络恐怖主义”的概念，将“影响政府或者社会的黑客行为”归入恐怖主义的范围，首次以立法的方式确认网络恐怖主义的存在。该法案认为，网络恐怖主义可以定义为：由特定组织或个人发起的，以网络为主要手段和活动空间的，旨在破坏国家或者国际政治稳定、经济安全和社会秩序的，有预谋、以制造轰动效应为目的的恐怖活动，是恐怖主义向信息技术领域扩张的产物。英国率先把任何干预公共电脑系统操作而危害他人性命的黑客，赋予“电脑恐怖分子”称号，他们将与其他恐怖分子一样，受到反恐怖主义法律条例的制裁。英国内政部发言人表示，当局并无专责部门处理计算机犯罪，它们通常由多个部门共同处理；但是任何严重干扰或妨碍电子系统运作的人士，将根据反恐怖主义法律条例惩办。此后，英国相继颁布了《2001年反恐怖主义、犯罪和安全法》（*Anti-Terrorism, Crime And Security Act* 2001）、《2005年预防恐怖主义法》（*Prevention of Terrorism Act* 2005）、《2006年反恐怖主义法》（*Terrorism Act* 2006）、《2008年反恐怖主义法》（*Counter-Terrorism Act* 2008）等。2010年，英国在国家安全战略报告中，把网络攻击与恐怖主义、国家间军事危机、重大事故和自然灾害一并定为国家安全面临的四大主要威胁。2015年，英国实施《反恐怖主义法》，针对新情况，推出应对举措，包括强制航空公司向英国政府提供乘客信息以及存储数据等，这是因为英国政府担心网络对英国人的意识形态具有蛊惑作用，所以，加强了应对网络时代恐怖主义的措施。

美国21世纪国家安全委员会在1999年发布的《新世纪国家安全报告》中，首次将网络攻击武器定义为大规模破坏性武器，并将其与专指核、生、化武器的大规模毁灭性武器相提并论。2000年，美国《国家安全报告》又首次把保卫能源、银行与财政、电信、交通、供水系统等重要的信息基础设施的安全，列为国家的关键利益。“9·11”事件发生以后，美国在加强现实空间反恐怖行动的同时，也大力加强网络空间反恐措施的制定。2001年，美国颁布了《爱国者法》，即“反恐2001法案”，将网络恐怖主义列为正式的法律术语。美国司法部通过的《反对恐怖主义法案》，把“危及美国经济稳定和政府政党活动的黑客行为”列入“恐怖主义罪行”的黑名单。此后，美国众议院司法常设委员会的一份报告中指出：“网络恐怖主义指利用电脑系统进行由特定的法律所界定的恐怖活动。真正的网络恐怖主义的特点在于大规模地破坏或是威胁要进行大规模破坏，其目的是损害或强迫平民或政府。”

布什政府在2003年和2006年发布了两份《抗击恐怖主义国家战略》，而2003年布什签发的《保护网络空间国家安全战略》中，重申维护网络安全是一项艰巨的战略挑战，需要包括各级政府、私营部门和全体公民在内的整个美国社会的协作和共同努力。2011年6月和12月，奥巴马政府相继公布《国家反恐战略》和《反恐战略执行计划》，旨在应对本土滋生的恐怖主义。

2016年12月5日，俄罗斯联邦总统普京颁布646号总统令，批准俄罗斯联邦新版《信息安全学说》即日生效，并同时宣布，2000年10月9日颁布的俄罗斯《信息安全学说》(1895号总统令)失效。俄罗斯历来十分重视信息安全问题，此前受西方“信息战”理论和实践冲击，俄罗斯在2000年颁布的《信息安全学说》中，正式把信息安全作为战略问题来考虑，从理论和实践上加紧准备与建设，认真探讨进行信息战的各种措施。2016年发布的新版学说是对2000年版《信息安全学说》的更新升级，内容更加丰富，任务更加明确。《信息安全学说》认为，“信息恐怖主义(网络恐怖主义)是为实现恐怖主义目的在国际信息领域使用电信和信息系统及资源，以及影响这些系统或资源”。①

2001年，日本公布的“e-Japan计划”将“确保信息安全”作为五大主要方针之一，主张建立“对付网络恐怖数据库”，收集网络恐怖活动的信息，着手开发信息安全评估等基础技术。2015年9月4日，日本内阁决议正式通过了新版《网络安全战略》。与2013年版《网络安全战略》相比，新战略将网络攻击的防范监管范围扩大到“独立行政法人”和部分“特殊法人”，并规定“日本政府机关处理重要信息的系统要与网络分离开来”。同时，新战略还提出积极参与构建网络空间国际规则的方针，并强调确保2020年东京奥运会与残奥会免受网络恐怖主义攻击的相关举措。

(三)专家学者对网络恐怖主义的定义

1. 美国

美国加州安全与情报研究所的资深研究员巴里·科林发现网络与恐怖主义相结合(converge)的现象，讨论恐怖主义从现实世界到虚拟世界超越的问题。他首次正式地提出网络恐怖主义概念，并认为网络恐怖主义是“网络”与“恐怖主义”相结合的产物，是一种由国家或非国家主使的，针对信息、计算机程序和数据以及网络系统，带有明确政治目的的攻击行动。②

---

① 朱永彪，任彦．国际网络恐怖主义研究[M]．北京：中国社会科学出版社，2014：8.

② 张琼，刘璐．试论网络恐怖主义的特征及对策[J]．科技信息，2009(10)：209-210.

美国乔治敦大学(Georgetown University)计算机科学教授、密码学家、网络反恐学者多罗西·邓宁在2000年5月的一次发言中认为,“网络恐怖主义是恐怖主义和网络空间的结合(convergence)”,“它是基于对电脑、网络(networks)以及储存在电脑和网络中的数据进行非法攻击或威胁进行攻击,以便胁迫或强制一国政府或国民,从而达到一定的政治或社会目的。”[①] 邓宁还进一步对如何界定网络恐怖主义作出说明:“如果被称为网络恐怖主义,一次攻击应该在结果上表现为对民众或财产的暴力对待,或者至少是造成了爆炸或巨大经济损失的袭击,都是网络恐怖主义的例子。对关键基础设施发起的严重袭击,如果其引起的后果比较严重,可以界定为网络恐怖主义。那些造成了不重要的服务中断的攻击,或者主要是造成了重大损失的骚扰性攻击,不能称为网络恐怖主义。”此外,邓宁还给出另外一个定义:“有意要引起严重伤害(如人员死亡或严重的经济损害)的有政治动机的黑客行为。”[①]

美国联邦调查局反恐/反间谍部执行副总卡鲁索(J. T. Caruso)这样定义网络恐怖主义:“恐怖组织越来越多地利用包括互联网在内的通信技术策划恐怖活动、募集资金、进行宣传等活动。网络恐怖主义则是指利用网络破坏重要基础设施,包括电力、交通以及其他政府运营系统等,以达成其政治目的。这显然是恐怖分子一种新手段。”[②]卡鲁索认为,最有可能遭受网络恐怖袭击的基础设施有电力系统、交通系统、水利设施、通信系统等。

西南密苏里州立大学的洛德·斯塔克(Rod Stark)指出:“网络恐怖主义是由非国家或国家主使的集团进行的、有目的的或威胁使用政治、社会、经济或宗教目的的网络战或以网络为目标的暴力活动,目的是引起目标人群的恐慌、焦虑和痛苦以毁坏军事和民用设施。”[③]

在1997年10月第20届全国信息系统安全会议(National Information Systems Security Conference)上,美国联邦调查局特派员马克·波利特(Mark Pollitt)提交的论文《网络恐怖主义——现实还是想象?》将网络恐怖主义定义为“由亚国家组织(sub-national groups)或秘密行动者(clandestine agents),对信息、计算机程序,以及对数据发动有预谋的、有政治动机的攻击,其结果导致对非战斗目标实施暴力行为”[④]。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

① 朱永彪,任彦. 国际网络恐怖主义研究[M]. 北京:中国社会科学出版社,2014:6.

② 最有可能遭受网络恐怖袭击的基础设施[N]. 青年时讯,2004-07-22. http://news.sina.com.cn/o/2004-07-22/02213189596s.shtml.

③ 朱永彪,任彦. 国际网络恐怖主义研究[M]. 北京:中国社会科学出版社,2014:7.

④ 张琼,刘璐. 试论网络恐怖主义的特征及对策[J]. 科技信息,2009(10):209-210.

暴力型恐怖活动直接联系。

原美国联邦调查局高级研究员、纽黑文大学教授威廉姆·塔夫亚(William L. Tafoya)认为,网络恐怖主义是通过应用高科技实现政治、宗教、意识形态目的,使重要基础设施数据瘫痪或者被删除而引发严重后果等行动,来恐吓普通民众。这个定义将网络恐怖行为的目的、手段和后果等因素都考虑其中。

Desouza 和 Hensgen 对网络恐怖主义的定义是:"出于个人或组织的犯罪动机,以破坏或搞垮政治稳定或国家利益为目的,通过使用电子设备及其技术手段,直接对信息系统、计算机程序或其他如通信、传输和存储等电子目标进行袭击的有目的的攻击行为。"总之,网络恐怖主义是基于政治、宗教或社会目的,通过针对关键的 ICT(信息通信技术)基础设施实施威胁攻击或破坏,以造成损失的网络攻击行为来达到其制造恐惧、惊慌和威慑目的的犯罪行为。①

美国国会研究服务部(Congressional Research Service,CSR)外交、国防以及贸易部门的技术与国家安全专家克莱·威尔逊(Clay Wilson)的定义是:"由有政治动机的国际性、亚国家群体,或秘密行动者利用计算机作为武器,或者是目标,来威胁制造或制造暴行及恐惧,意图影响民众,或使一国政府改变策略。"②2008 年,美国国会研究服务部发布了一份报告警示说,美国军队应用这项基于网络的合作技术来训练士兵和收集情报,但是同样的方法也可能被恐怖分子加以利用,来训练和组织袭击。克莱·威尔逊在报告中说:"用(虚拟现实技术)来训练,将允许相距很远的两支部队通过因特网或者是保密网际协议邮件路由网络(siprnet),在仿真的环境中进行面对面的对抗,还将允许快速反应机构、公民甚至是医疗机构通过仿真网络与部队进行配合联系。"

Janszewski 和 Colarik 指出:"网络恐怖主义的出现便意味着传统的'罪犯'又多了一种通过计算机和电信技术进行潜在攻击的新的犯罪。"在某些情况下,网络攻击往往被视为网络恐怖主义。然而,不是所有的网络犯罪都是网络恐怖主义行为。网络恐怖分子和网络犯罪分子可能会使用相同的底层安全和黑客技术入侵系统,但其根本动机、目标和破坏效果是有所区别的。③

《黑冰:无形的网络恐怖主义威胁》一书的作者丹·韦尔顿(Dan Verton)给出的定义是:"网络恐怖主义是由国内外的亚国家组织或个人发动的带有政治目的的

---

① 安尼瓦尔·加马力,木尼拉·塔里甫,张昆. 基于生命周期循环模型的网络恐怖主义犯罪治理控制研究[J]. 新疆警察学院学报,2014(3):15-21.

② 朱永彪,任彦. 国际网络恐怖主义研究[M]. 北京:中国社会科学出版社,2014:6-7.

③ 安尼瓦尔·加马力,木尼拉·塔里甫,张昆. 基于生命周期循环模型的网络恐怖主义犯罪治理控制研究[J]. 新疆警察学院学报,2014(3):15-21.

突然袭击——使用计算机技术和因特网来削弱或破坏一国的电子和物理设施，由此导致关键服务的中断，如电力、911 报警系统、电话业务、银行系统、因特网，以及其他一系列的服务。”①

2. 德国

德国马克斯普朗克刑法研究所所长乌尔里希·齐白（Ulrich Sieber）教授认为，对网络恐怖主义的界定可以采取两种方式：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。因此，德国学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，这些行为包括：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。② 这一定义将网络恐怖主义扩展到将网络作为恐怖主义手段和犯罪空间的范畴。

3. 以色列

以色列海法大学传播学教授加布里埃尔·韦曼（Gabriel Weimann）指出，网络恐怖主义是网络空间与恐怖主义的结合，指的是对于计算机、网络及其上存储的信息的非法攻击和威胁攻击，以恐吓或强迫政府或其人民来达到政治或社会目的。2004 年已经处于 Web 2.0 时期，但是，韦曼教授的观点仍然停留在 Web 1.0 时代，也就是说，他认为网络恐怖主义只限于网络恐怖攻击行为即对于网络本身的攻击。到 2014 年的 Web 3.0 阶段，韦曼对网络恐怖主义的认识及时跟进，认为新媒体带来了新恐怖主义。他详细分析了电子“圣战”、脸谱恐怖主义、推特恐怖主义、优图恐怖主义等新恐怖主义，认为恐怖分子已经长久使用网络，以招募人员、进行宣传、蛊惑、恐吓和募集资金。③

4. 俄罗斯

俄罗斯政治研究中心的学者给出的定义是：“网络恐怖主义（计算机恐怖主义，或电子恐怖主义）是指通过计算机网络传播数据的方法对计算中心、军事网络和医疗机构管理中心、银行及其他金融网络展开的攻击。其结果可能造成（政府机关等）瘫痪，造成（大型生产集团）经济损失，甚至可能由于紊乱的工作秩序造成人员伤亡（如攻击机场调度与控制系统）。”据俄罗斯卫星新闻通讯社报道，2016 年 5 月，俄罗斯总统信息安全领域国际合作事务特别代表安德烈·克鲁茨基赫在接受

---

① 朱永彪，任彦．国际网络恐怖主义研究[M]．北京：中国社会科学出版社，2014：7.

② 皮勇．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[J]．政法论丛，2015(1)：68-79.

③ 于志刚，郭旨龙．网络恐怖活动犯罪与中国法律应对——基于 100 个随机案例的分析和思考[J]．河南大学学报（社会科学版），2015，55(1)：11-20.

《生意人报》采访时表示:“网络恐怖主义是最为可怕的现象之一,但又是全新的。然而,举例来说,‘伊斯兰国’就已经进入了信息空间,在从事网络恐怖主义。”

5. 英国

英国爱丁堡大学的瓦尔瓦拉·密特里阿加(Varvara Mitliaga)虽然没有直接给出网络恐怖主义的定义,但是他指出网络恐怖主义必须具备以下特征:“……袭击必须造成针对人或财产的暴力,或者至少是造成能引起恐怖的损害。那些造成了不重要的服务中断的攻击,或者主要造成了重大损失的骚扰性攻击,不能称为网络恐怖主义。”他举例说:“远程访问一个飞机或者道路交通控制系统并制造一起使人丧命的事故,或者至少是严重的破坏以及恐慌的蔓延,这将构成网络恐怖主义。然而,目的是转移信息而未经授权就渗进一个计算机系统,或者仅仅是为了骚扰系统用户的渗透,并不构成网络恐怖。”①

二、国内对网络恐怖主义的定义

“9·11”事件后,更多的中国学者开始关注网络恐怖主义,尝试给网络恐怖主义作比较系统、明确的界定,且从不同角度研究网络恐怖主义相关课题。

1. 法律和文件的定义

中国颁布的《计算机软件保护条例》《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》等行政法律、法规都规定,单位能够成为计算机违法行为的主体,对单位犯罪的,应当依法追究刑事责任。立法将单位纳入计算机犯罪的主体,实现了“刑法与非刑事法律之间的对接”。

2008 年,中国公安部反恐局在其编印的《公民防范恐怖袭击手册》和《公民安全防范手册》中对“网络恐怖袭击”作出说明,即“利用网络散布恐怖信息、组织恐怖活动、攻击电脑程序和信息系统等”。

2015 年通过的《中华人民共和国刑法修正案(九)》和《中华人民共和国反恐怖主义法》并没有专门就网络恐怖主义犯罪设置单独的条款,但是,对具有恐怖主义目的攻击或利用网络的行为提供了相应的行政或刑罚处罚指引。因此,在打击网络恐怖主义犯罪方面,我国已“有法可依”。

2. 专家学者的定义

随着研究人数和研究成果数量的增加,中国学者对网络恐怖主义的研究越来

① 朱永彪,任彦. 国际网络恐怖主义研究[M]. 北京:中国社会科学出版社,2014:8.