第 57 卷 第 5 期
2004 年 9 月

武汉大学学报(人文科学版)
Wuhan University Journal (Humanity Sciences)

Vol. 57. No. 5
Sept. 2004. 582~586

● 刑 法

论网络恐怖活动犯罪及对策

皮 勇
(武汉大学 法学院, 湖北 武汉 430072)

[作者简介] 皮 勇(1974-), 男, 湖北通城人, 武汉大学法学院法律系副教授, 法学博士, 中国人民大学法学院博士后, 主要从事刑法学、犯罪学研究。

[摘 要] 网络恐怖主义是在信息技术革命和新的国际形势下恐怖活动犯罪发展的新形式, 主要表现为网络恐怖攻击、网上散布恐怖信息和利用互联网组织恐怖活动 3 种形式。为打击网络恐怖活动犯罪, 许多国家采取了一系列防范行动, 并加强了国际合作, 制定了相关国际公约。我国也面临网络恐怖活动犯罪的威胁, 应未雨绸缪, 及早制定遏制网络恐怖活动犯罪的防范对策。

[关 键 词] 网络恐怖主义; 国际合作; 对策
[中图分类号] DF611 [文献标识码] A [文章编号] 1671-881X(2004)05-0582-05

一、网络恐怖活动犯罪的主要特征

网络恐怖主义(Cyber-Terrorism)是近年来出现的新名词, 指的是在信息技术革命和新的国际形势下恐怖活动犯罪发展的新形式。关于网络恐怖主义, 国际上有不同定义。美国 Georgetown 大学的学者 Dorothy E. DENNING 把网络恐怖主义界定为:"恐怖主义和网络空间的结合, 是指非法攻击或者威胁攻击计算机、网络以及存储在其中的信息, 以威胁或者强迫某国政府及其人民满足一定的政治或者社会目的。"[1](P.29) 2000 年英国通过《2000 年反恐怖主义法案》, 该法案第一条规定, 恐怖主义包括"故意严重干扰或者瓦解一个电子系统"的恐怖活动性质行为, 该法案因此被认为是国际上第一部规定网络恐怖主义的法律。以上定义都把网络恐怖主义限制在以一国或数国的计算机、网络系统为攻击目标的恐怖活动范围内。

实际上, 网络恐怖主义是恐怖主义在信息技术高度应用环境下的一种新形式, 它带有恐怖主义的共性, 即通过攻击、威胁攻击一国或数国的人民、民用或军事设施, 制造人员生命财产损失和心理恐慌, 以达到某种政治、宗教和意识形态的目的。因此, 它不限于攻击计算机、网络系统, 网上散布恐怖信息和利用互联网组织恐怖活动, 也是网络恐怖主义的重要内容, 它们所造成的社会危害有时并不亚于前者。网络恐怖主义是一种严重犯罪, 它能利用计算机、网络、多媒体等多种信息技术跨国跨地区造成危害, 并能直接或者间接地危及其他国家, 甚至造成全球性的灾难。因此, 网络恐怖主义绝不仅仅是恐怖主义的一种新手段, 而是"一个非传统安全领域的新的全球性问题"[2](第 37 页)。

目前, 网络恐怖活动犯罪主要表现为 3 种形式, 即网络恐怖攻击、网上散布恐怖信息和网上组织恐怖活动。其中网络恐怖攻击是目前影响最大的一种, 后两种较少为公众了解, 但它们对社会的危害却丝毫不逊色于第一种形式。

收稿日期: 2004-01-28

(一)网络恐怖攻击

所谓网络恐怖攻击,指的是出于政治、宗教和意识形态的目的,非法攻击或者威胁攻击某国的计算机、网络系统及其中的信息的行为。网络恐怖攻击和黑客骚扰有相似之处,如都表现为利用信息技术进行网络攻击,但二者的区别是明显的:黑客骚扰也会攻击大量的计算机、网络系统,但往往是出于制造混乱、恶作剧和捣乱的目的,而网络恐怖攻击则是出于政治、社会目的,往往制造重大人员伤亡、财产损失的暴力事件,虽然有些网络恐怖攻击不立即导致暴力破坏的后果,但会持久发生作用,造成比一般恐怖活动更大的危害。

在当今复杂的国际形势下,网络恐怖攻击将会继续增加,网络恐怖主义正在成为关系国家安全、国际政治与国际关系的突出问题。目前,网络恐怖攻击的主要特征表现在以下几方面:

1.这些恐怖活动有明显的政治、宗教或意识形态目的。如美国"9·11 事件"后不久,"穆斯林游击战士"等一些伊斯兰黑客组织攻击了美国国家海洋及大气局等网站,并在其网页上留下恐吓字句。

2.网络恐怖攻击的形式多种多样,但利用"混合性病毒"(Mixed Virus)攻击成为危害最大的一种。据反病毒软件生产企业英国 Sophos 公司称,2001 年一年内共发现有 1.116 万种电脑新病毒,其中"尼姆达"病毒和"Cam 先生"病毒所侵害的电脑数量约占全球受病毒感染电脑总数的一半,造成的经济损失约 18 亿美元。更令人担忧的是,计算机病毒发展进入所谓"后病毒时代"。据《科技日报》消息,法国通过监视互联网上对网络发起的攻击行为和分析攻击行为的变化及结果后认为,在网络攻击中最具"毒"性的是"混合性攻击",即利用结合计算机病毒、黑客技术、网络蠕虫和拒绝服务等技术于一体的"混合性病毒"。新的网络攻击方式使网络恐怖攻击的破坏力和破坏范围成倍增加,在互联网和无线通讯普及的情况下,将会在信息网络产生连锁反应,对信息社会的正常运行构成致命威胁。

3.网络恐怖攻击的主要目标转向关系国计民生领域的计算机、网络系统。传统恐怖袭击的目标多数是某国政府、军事机构的设施,随着恐怖主义发展,防护相对薄弱却关系国计民生的重要领域日益成为恐怖袭击的主要目标。以遭受网络恐怖袭击最多的美国为例,美国虽然拥有世界上最先进的信息技术、最强的经济实力来对付网络恐怖攻击,但 2000 年至"9·11 事件"发生,美国遭受的网络袭击达到 4 万次,其中不乏恐怖攻击。目前,美国除了继续加强军事、政府部门的计算机、网络系统的安全防护外,又特别把电信、金融财政、电力供应、燃油燃气的分发和储存、供水、交通、紧急服务等领域列入防范网络恐怖攻击的范围。美国政府认为,这些领域的计算机、网络系统更加脆弱,而一旦遭到恐怖攻击,将导致更大的人员伤亡和财产损失。

(二)网上散布恐怖袭击信息,制造社会恐慌

人们对恐怖袭击有着深重的恐惧,这种恐惧心理能够破坏人们正常的工作生活秩序,因此,散布恐怖袭击信息和恐怖袭击一样,能扰乱社会秩序,影响经济发展和社会稳定。如 2002 年美国民众经常接到政府发布的各种恐怖袭击警报:恐怖分子要袭击自由女神像!恐怖分子要攻击布鲁克林大桥!恐怖分子要在独立日袭击拉斯维加斯!一时间国家处于战争戒备状况,人心惶惶,不可终日,国民经济遭受重创,美国股市一再下挫。恐怖袭击信息散布的范围越广,制造的社会恐慌越大,对社会的危害越严重。

互联网覆盖范围广,方便恐怖分子在任何地方隐蔽地登入互联网,广泛发送恐怖袭击信息,因此日益成为恐怖分子发动心理战的最佳途径。网上散布恐怖袭击信息的一个重要特点是虚虚实实、弄假成真。恐怖分子可以在网络聊天室中伴作密谋恐怖袭击计划,吸引情报部门的关注,借助官方之口将恐怖袭击信息传播出来,或者利用黑客技术侵入民航、火车站、地铁等领域的计算机、网络系统,在公告系统如大型显示屏公布恐怖袭击的信息,还可能利用计算机病毒技术,将恐怖袭击信息直接发送给广泛的网络用户,威胁进行恐怖袭击等。网上散布恐怖袭击信息,一方面能制造社会恐慌,给对方造成经济损失和社会混乱,另一方面能为真实的恐怖袭击打掩护,真假恐怖袭击构成一体,能使对方国家长时间笼罩在恐怖袭击的阴云之下。

(三)利用互联网联络恐怖活动犯罪

互联网除了能成为网络恐怖袭击、网络心理战的空间外,还能成为联络恐怖活动分子、建立恐怖活动组织、协调恐怖袭击行动的黑色空间。由于各国政府加强了对恐怖活动犯罪的打击,公开的恐怖活动联络几乎无藏身之处,大批恐怖活动分子潜伏下来。而互联网成为他们联系、协调的关键途径,互联网上巨量的信息流和多种多样的反侦察技术给反恐当局造成难以克服的障碍,而恐怖分子却能借助互联网,在全球各地大肆发展恐怖活动组织,策划恐怖袭击。例如,本·拉登和其他穆斯林极端分子曾利用互联网和数据加密技术,策划针对美国及其盟国的恐怖主义活动,互联网上的许多体育交谈室、色情标贴板和其他著名网址都成为他们发布恐怖活动的指示的隐蔽场所。

由于互联网本身的特性、信息保密技术的发展和管理的失控,以及互联网上信息管理的混乱,在目前情况下,任何国家的政府都无法有效监控互联网上传输的信息,网络恐怖活动犯罪分子总能利用互联网上数量众多的网站、网络匿名交谈室,使用各种加密技术进行网络通讯和传递加密文件。如果不能控制利用互联网发展和联络恐怖活动,就不能阻止恐怖活动力量的集聚和消除恐慌袭击的威胁。因此,恐怖活动分子和反恐当局对于互联网控制权的争夺,将成为网络反恐斗争能否胜利的关键。

二、世界主要国家打击网络恐怖活动犯罪的行动及相关国际立法

美国是社会信息化程度最高的国家,拥有世界上最大规模的信息基础设施,对信息基础设施的依赖性最深,同时,也是遭受网络恐怖活动犯罪危害最严重的国家。美国国防大学托马斯·彻尔温斯基教授指出:"我们的信息系统比任何国家都多,因而也比任何国家更容易受到信息武器的攻击。""9·11 事件"发生后,美国政府、企业非常担心国际恐怖分子采取网络袭击的办法攻击和破坏美国庞大的信息基础设施,美国联邦调查局在"9·11 事件"发生的第 2 天就发出恐怖分子可能发动网络袭击的警告,将亚特兰大基础因特网安全系统(它控制和管理美国国家信息共享和分析中心)的运作设置在次最高级上,以保护全美信息资源与系统。美国政府还成立了"国土安全办公室",将打击网络恐怖作为其主要职责之一;召集由副总统、司法部长和美国 10 大网络供应商高官参加的"网络恐怖袭击对策"会议;在美国联邦调查局内新设反网络犯罪局,专司打击网络犯罪之责;指令美军加强网络战准备,防范网络恐怖袭击以及打击网络恐怖活动。为使反网络恐怖袭击有法可依,美国国会于 2002 年 10 月通过了《反恐怖主义法》,法案将黑客攻击视为恐怖主义行为之一,并把打击网络恐怖列为其中的一项重要内容,为反恐怖主义设立了特殊的法律措施,如允许执法机构窃听恐怖嫌疑分子的电话并跟踪其联网和电子邮件的使用;允许司法部门在提出犯罪指控和驱逐之前对有犯罪嫌疑的外国人拘留 7 天;把庇护恐怖分子的行为定为犯罪;加大对恐怖犯罪的打击与惩罚力度等。

在欧洲,英国 2000 年通过的"2000 年反恐怖主义法"把黑客入侵列为恐怖行为,2001 年 12 月英国议会通过了新的紧急反恐法案,又把网络恐怖活动列入打击目标。德国外交部和国防部在 2001 年底发布报告称,城市基础设施和全国通讯网络系统可能成为恐怖袭击的目标,提出要尽快采取措施加以防范。德国政府正筹划建立一个特别安全机构和制定相关防御计划,研制更多独立的、全国性的软件和密码程序,以应对网络恐怖攻击。

在亚洲,日本"IT 战略本部"提出将过于集中在东京的因特网转换枢纽分散到地方,建立全国网络系统备用中心,日本防卫厅还举办了对付网络入侵的模拟演习,以增强网络防御的有效性。韩国信息通讯部将每月 15 号定为"预防网络恐怖袭击日",以使政府、企业、民众定时对计算机和网络系统进行自我检查,提高预防网络袭击的能力。

长期以来国际社会一直关注恐怖主义犯罪,先后通过了联合国《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》两个国际公约。网络恐怖活动犯罪具有跨国性、高技术性等特征,使各国运用国内力量打击犯罪时,遇到了诸多困难,这促使国际社会加深合作,携手共同对付网

络恐怖威胁。继 2000 年 5 月召开的首次以打击网络犯罪为主要议题的国际性会议——“政府机构和私营部门关于网络空间安全与信任对话”八国集团会议后, 2001 年 11 月 23 日欧洲委员会国家及美国、加拿大、日本、南非正式签署《网络犯罪条约》。《网络犯罪公约》是针对网络犯罪的第一个国际公约, 其主要目标是寻求打击网络犯罪的共同的刑事政策, 特别是建立适应网络犯罪的法律体系和国际协助。除序言外, 该公约正文分为四章, 核心内容是第二章“国家层面上的措施”和第三章“国际合作”的规定, 第二章“国家层面上的措施”包括三个部分, 即“刑事实体法”、“刑事程序法”和“管辖权”, 第三章“国际合作”包括两个部分, 即“一般原则”和“特殊规定”。《网络犯罪公约》的通过具有里程碑意义, 它揭开了国际社会合作打击包括网络恐怖活动犯罪在内的网络犯罪的序幕, 对整合国际反恐怖主义力量, 有效遏制网络恐怖主义将发挥重要作用。

三、我国打击网络恐怖活动犯罪应采取的对策

网络恐怖活动犯罪的产生有社会、政治和意识形态等方面的原因, 而促使其迅速发展并给社会造成严重危害的条件, 则与互联网广泛的覆盖范围、互联网安全的脆弱、难以控制信息技术的滥用、互联网管理的薄弱、法律体系不完善等方面的原因有关。因此, 要消除网络恐怖活动犯罪的危害, 除了要逐渐化解其产生的根本原因, 使其丧失发展蔓延的条件, 也能起到有效遏制的效果。

针对网络恐怖活动犯罪发展的条件, 我国应采取以法律控制为指导, 结合法律、管理、技术、教育等多种手段的综合防治的对策。所谓以法律控制为指导, 是指建立预防控制网络恐怖活动犯罪的法律体系, 管理、技术、教育等手段服从法律控制的指导和需要, 并在各领域内充分发挥预防、控制、遏制犯罪人和犯罪发生的作用。在法制建设方面, 我国不仅应迅速完善控制犯罪的国内法, 还要及时根据国际社会控制犯罪的发展趋势, 积极参加打击网络恐怖活动犯罪的国际条约, 利用国际司法机制共同打击犯罪; 在管理方面, 应根据控制犯罪的法律要求, 完善信息基础设施安全管理和人员管理的制度, 防止因内部管理的疏漏给犯罪以可乘之机; 在技术方面, 不仅要充分发挥技术措施直接对抗犯罪的作用, 还要在法律控制的指导下, 积极为犯罪的预防、侦查, 追究法律责任和完善管理提供必要支持; 在教育方面, 既要教育公民积极维护互联网正常秩序, 配合打击网络犯罪活动, 也要对一部分社会危险分子进行法律宣传, 使之遏制、消除实施犯罪行为的动机。在目前我国防范网络恐怖活动犯罪的状况下, 以下方面应予以特别关注:

1. 参加有关国际条约, 完善我国相关法律体系, 加强国际司法合作。我国《刑法》在“危害公共安全罪”一章规定了领导、组织恐怖活动组织罪、积极参加恐怖活动组织罪、资助恐怖活动罪等犯罪, 还把为恐怖活动犯罪洗钱的行为规定为犯罪; 在“妨害社会管理秩序罪”规定了非法侵入计算机信息系统罪、破坏计算机信息系统罪; 在《维护互联网安全的决定》中规定, 利用计算机、互联网实施 21 种行为, 构成犯罪的, 应当追究刑事责任。以上立法是我国打击网络恐怖活动犯罪的法律依据, 反映了我国高度重视恐怖主义犯罪问题, 已经建立了比较完善的打击网络恐怖活动犯罪的法律体系。但是, 现有的法律体系仍然存在一些不足, 如积极参加恐怖活动组织, 并实施网络恐怖活动行为构成犯罪的, 是否实行数罪并罚, 法律没有明确规定; 为实施恐怖活动犯罪而滥用密码、黑客工具等设备的, 网上散布恐怖信息, 造成社会恐慌, 造成严重后果的, 法律没有将这种行为规定为犯罪等。此外, 由于网络恐怖活动犯罪能够借助互联网跨国跨地区造成危害, 因此, 协调世界各国法律, 加强国际司法合作, 成为打击这类犯罪所必需, 而目前我国在这方面参与的国际合作还不够, 有些重要国际公约如《网络犯罪公约》我国没有加入。总之, 我国应当积极参与国际合作, 研究并加入相关国际条约, 完善我国网络恐怖活动犯罪立法体系, 融入国际司法体系共同打击这类犯罪。

2. 加强互联网信息的控制。互联网是信息交流的新空间, 在互联网上人们可以不受时间空间限制, 获取、交换极为丰富的信息, 但同时互联网也能成为网络恐怖活动犯罪散布恐怖信息、交换犯罪信息、获

取犯罪工具的隐蔽空间。因此,在保障公民通信自由、保护个人隐私的同时,必须实现对互联网上信息的有效控制。我国已经着手互联网信息控制方面立法,如《互联网信息服务管理办法》第 15、16 条规定,互联网信息服务提供者不得制作、复制、发布、传播含有法定九类内容的信息,互联网信息服务提供者发现其网站传输的信息明显属于这些内容的,应当立即停止传输,保存有关记录,并向国家有关机关报告。有类似规定的还有《互联网电子公告服务管理规定》、《高等学校计算机网络电子公告服务管理规定》等法规规章。这是我国实现依法控制互联网信息的开始,在防范网络恐怖活动犯罪利用互联网危害社会中发挥了重要作用。但是,我国目前对互联网信息的控制管理仍然非常有限,除了因为互联网连接范围广、互联网技术本身特性不便管理等原因外,缺乏系统、完整的互联网管理体系是主要原因。建议我国把互联网信息管理作为一项信息社会犯罪预防控制的系统工程,借鉴国外成功经验,广泛吸纳各信息服务提供单位参与,建立包括法律规范、制度管理、技术保障在内的一体化综合控制系统。

3. 提高侦查网络恐怖活动犯罪的技术能力。网络恐怖活动犯罪是一类技术性很强的犯罪,侦破这类犯罪需要高素质的侦查人员正确应用高技术措施,才能保障案件的及时侦破。如果我们只有对付传统犯罪的工作人员和工作手段,那么,不仅不能侦破案件,而且可能成为这类犯罪猖狂发展的诱因和条件。目前,我国公安部门成立了专司恐怖活动犯罪、计算机犯罪的机构,打击网络恐怖活动犯罪的专业人员越来越多。但是,整体而言,我国侦查网络恐怖活动犯罪的队伍建立时间还不长,有经验、有技术的专业司法工作人员还十分缺乏,专业人才问题将成为较长时间内制约提高我国侦查网络恐怖活动犯罪案件能力的"瓶颈"。另外,"兵欲擅其战,必先利其器",先进的网络犯罪侦查工具、对抗反侦查的技术能力等,也是提高侦查能力的关键。我国应当充分利用国内信息技术人才充裕的优势,与国内信息技术企业合作开发先进的侦查工具,或者积极吸纳有效的技术支持,以提高我国侦破网络恐怖活动犯罪的整体水平。

[参 考 文 献]

[1] Denning, Dorothy E. Arms Control in Cyberspace[J]. Heinrich B9 ll Foundation, 2001,(1).
[2] 俞晓秋. 全球信息网络安全动向与特点[J]. 现代国际关系, 2002,(2).
[3] 胡积康. SOPHOS 公司:2001 年危害最大 10 种电脑病毒[DB/OL]. 新华网, 2001-11-30.
[4] 李 红. 法国调查表明:网络攻击有增无减[DB/OL]. http://www.stdaily.com/gb/stdaily/, 2003-2-19.

(责任编辑 车 英)

Research on Cyber-Terrorism Crime & Its Control Method

PI Yong
(Wuhan University Law School, Wuhan 430072, Hubei, China)

Biography: PI Yong(1974-), male, Associate professor, Wuhan University Law School, majoring in criminal law.

Abstract: Cyber-Terrorism crime is the new kind of terrorism in the circumstance of information technology revolutionary and new international situation. For purpose of control Cyber-Terrorism crime, many countries have taken series of actions and strengthen the international cooperation, new international conventions were passed too. China also faces the threat of Cyber-Terrorism crime, should prepares before serious crime situation and make effective method to control Cyber-Terrorism crime.

Key words: cyber-terrorism; international cooperation; control method