因特网上的犯罪及其遏制

屈学武*

内容提要:本文首先探究了刑法学和犯罪学意义的因特网上犯罪的不同定义及犯罪种类。其次分析了因特网上犯罪的特点和趋势;反映了若干亟待解决的法律问题,如因特网上犯罪的特殊性、对第五空间的刑事管辖等。最后,本文分别从犯罪学和刑事法角度阐释了作者对网上犯罪的法律思考,包括犯罪预警网站的设立、网上犯罪的司法运作及立法构想等。

关键词:因特网上犯罪　虚拟毒品　第五空间

因特网,又称国际互联网,本是人类文明与智慧的结晶、是人类步入高科技信息时代的表征。然而,它在为人类带来便捷的同时,也为因特网上的犯罪开辟了新的犯罪平台和站点——号称第五空间。〔1〕犯罪分子、虞犯分子人人"机会均等"、个个有望在此平台一展自己的在线"天才"。看来,在人们纷纷驶上信息高速公路冲浪的同时,犯罪分子也开始撷取人类高科技文明之果并藉其利刃反刺人民了。

因特网上的多重犯罪,令犯罪学家、刑法学家们无不面临下述崭新课题:如何审视、界定因特网上的犯罪?如何探析、测定其犯罪特点及趋势?国家、政府与社会当如何协作与运作才能最大限度地遏制此类犯罪?

鉴于因特网上犯罪的跨国性、全球性及各国刑法对因特网上犯罪的定义、种类规定的不同,对此类犯罪的研究视角,也宜放诸国内与国外相结合、犯罪学与刑法学相结合的大框架内,本文正是在此语境意义上研讨因特网上的犯罪。

一、因特网上犯罪的概念及其种类

与其他犯罪概念一样,因特网上犯罪概念也有广狭义之分。狭义概念为刑法学概念,即因特网上犯罪仅限于刑法明文规定为犯罪的、严重危害社会的行为;广义概念为犯罪学概念,即

* 中国社会科学院法学研究所研究员。

〔1〕网络空间被认为是领陆、领水、领空、浮动领土以外的第五领域,故称第五空间;也有一说认为,网络空间是领陆、领水、领空、太空以外的第五空间。由于太空不属各国刑事法所界定的"领域",因而我们比较赞成前一观点。

其除了已由刑法规定为犯罪的严重危害社会行为外,还包括犯罪学家所探究的宜视作犯罪来研讨其生发过程及其对策的严重危害社会的行为。

(一)犯罪学意义的因特网上犯罪概念及其种类

犯罪学意义的因特网上犯罪,指犯罪分子利用其编程、加密、解码技术或工具、或利用软件指令、网络系统或产品加密等技术及法律规定上的漏洞或瑕疵;抑或利用其居于互联网服务供应(ISP)、互联网信息供应商(ICP)、应用服务供应商(ASP)等特殊地位或其他方法,在因特网上实施的、严重危及人类社会安全及生存发展秩序的行为。由此可见,从大面上划分,因特网上犯罪包括利用因特网实施的犯罪和针对因特网络实施的犯罪。

如前所述,犯罪学意义的因特网上犯罪,本包括已然规范和应然规范两大类。本文为了叙述的方便和明确,拟将"已然规范"部分放诸下文即"刑法学意义的因特网上犯罪"议题中专门研讨,这里仅就犯罪学意义的应然规范角度,对应当"视作犯罪"的因特网上犯罪行为加以比较分析。〔2〕

1. 网上侵犯他人隐私权利。指未经他人许可,擅自通过因特网站上他人或自己的主页,将特定的"他人"隐私公之于众;或未经他人许可,擅自通过向第三人、第四人或众多其他人等发送 Email 的方式张扬特定"他人"的隐私,情节恶劣、后果严重的行为。

2. 网上侵犯言论自由权利。主要指互联网接入服务供应商为阻断不同意见的网上通道而蓄意关闭与自己用户相连的特定网站、情节严重的行为。例如 1999 年 5 月,在北约轰炸南联盟期间,设立在美国的服务器主机就曾单方面关闭了南联盟网站,为的是不让访问这些网站的美国网民阅读到饱受战争之难的南斯拉夫人民的网上抗议、呻吟之网页。显然,这种作法,违背了互联网上的资源共享、存取自由的信息使用原则;同时也背离了服务供应商与用户之间的服务合约,即互联网服务供应商提供给用户的应是完整的全球网,不得擅自割断某网站与服务器主机的联系。除对用户的违约以外,服务供应商擅自关闭他人网站,也是对他人言论自由的侵犯,情节严重者,应视作网上侵犯言论自由的犯罪行为。

3. 网上恐吓。指通过直接投向特定他人的、含致命暴力威胁内容的 Email 信件,来恐吓"他人"的非法行径。实践中,时见在因特网上敲诈勒索他人者,此类行为人往往以"行将使用暴力"来勒索他人。与此不同的是,网上恐吓他人者,仅以暴力威胁他人而不勒索财产,这是二罪的重大区别之一。

4. 网上扰乱市场。指一些居心叵测者,采用涂改他人主页、往他人邮箱中散发虚假信息邮件、或利用自己的主页或网站上的电子公告故意在网上散布虚假的金融、股市、经济及其他天灾人祸信息,严重扰乱正常的市场经济秩序、造成严重损害后果的行为。

目前,在网上炒股、交易者日渐增加。在国内,随着统一支付网关的建成,网上顾客正在形成。例如于 1999 年 11 月建成的上海电子商务支付网点的投入运行,就意味着几百万上海持卡人已能在片刻之间完成网上商店购物。发达国家中,网上炒股、交易者相对更加普遍。据美国商务部 1999 年 6 月发布的一份研究报告表明,1998 年后期,美国网上零售交易额已达 70 亿美元。基于此,采取散布虚假经济信息手段扰乱证券市场、金融市场、电子商务市场、造成严

〔2〕 所谓"应当",在此并不必然等同或代表通说观点,而是就一些学者包括笔者自己的视角而言。

重后果者,宜予刑事惩治。[3]

当然,按照中国现行刑法的规定,上述四种"犯罪"行为在中国原则上不为罪。[4] 因而此类行为纯属犯罪学意义的因特网上犯罪。但这只是从中国刑事法域看,实际上,上述某些行为已为一些国外刑法明确规定为犯罪。例如加拿大刑法规定了"电信恐吓罪";韩国、格陵兰刑法规定了侵犯个人秘密罪等。故此,在该国范围内,这些犯罪应属刑法意义的犯罪。

(二)刑法意义的因特网上犯罪概念及其类型

刑法意义的因特网犯罪,指犯罪分子利用其编程、加密、解码技术或工具、或利用软件指令、网络系统或产品加密等技术及法律规定上的漏洞或瑕疵;抑或利用其居于互联网接入服务供应商、信息供应、应用服务供应商等特定地位或其他方法,在因特网上实施的、触犯特定刑法规范的严重危害社会的行为。

美国学者曾将计算机犯罪分类为计算机犯罪和计算机关联罪(Computer - Related Crime)。[5]借此分类法,我们不妨将刑法意义的因特网上犯罪也分类为因特网上犯罪和因特网关联罪两大类。前者为狭义的刑法意义的因特网上犯罪,指按照刑法的规定,只能通过计算机在因特网上实施的犯罪行为;后者为广义的刑法意义的因特网上犯罪,指按照刑法的规定,行为不仅可在因特网内实施,而且可以利用互联网上得到的信息或技术,在因特网内外交互实施的网上犯罪。中国现行刑法对因特网上的犯罪规定正好可以划分为如此两大类。

第一,只能在计算机网络上实施的犯罪。中国现行刑法第285、第286条分别规定的非法侵入计算机信息系统罪和破坏计算机信息系统罪即属之。

(1)非法侵入计算机信息系统罪,指"违反国家规定,侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的"犯罪行为。

所谓违反国家规定,在此主要指违反国家有关对计算机信息系统的管理规定及其有关国家事务、国防建设、尖端科学技术领域的准出准入及安全管理规定。例如违反《中华人民共和国计算机信息系统安全保护条例》第7条、第8条的有关规定,违反国务院《计算机信息网络国际联网安全保护管理办法》第4条、第5条、第6条的有关规定等。

所谓"侵入",指任何单位或个人,利用网络系统或产品加密等技术上的漏洞或瑕疵,抑或利用解密、对身份认证的破坏等手段,未经允许,擅自进入计算机信息系统的行为。

所谓"计算机信息系统",指"由计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统"。

值得注意的是,"与国际互联网相连",并不是上述法规对计算机信息系统的必备要求。因而,按照本罪的犯罪构成要件规定,行为人只要侵入了已经联网的特定局域网系统即可,无论其是否与因特网相连。但是,考虑到侵入局域网的犯罪分子,往往先行进入因特网并通过其通道非法侵入计算机局域网系统,因而该罪本质上仍属狭义的因特网上犯罪。

本罪是行为犯,行为人只要实施了上述"侵入"行为,就构成犯罪既遂。不问其是否实施了其他删除、修改、增加、干扰计算机信息或存储数据、程序的行为;更不论其行为有无特定危害

〔3〕 这当中,编造并传播影响证券交易的虚假信息,扰乱证券交易市场,造成严重后果者,已为中国现行刑法第181条规定为犯罪行为。

〔4〕 在网上侵犯他人隐私行为过程中,有公然侮辱或诽谤他人、情节严重者,可按中国刑法所规定的侮辱罪或诽谤罪定罪量刑。否则仅属民事侵权行为。

〔5〕 See Bruce T. Fraaser J. D. Candidate, M. S, Library and Information Studies.

后果。

(2) 破坏计算机信息系统罪,包括下述三种行为:其一,“违反国家规定,对计算机信息系统功能进行删除、修改、增加,干扰,造成计算机信息系统不能正常运行,后果严重的”;其二,“违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的”;其三,“故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重”者。

上述第一种行为与第二种行为的主要区别在于:第一种行为破坏的是整个计算机信息系统的功能,包括对已经联网的计算机本身及其相关的、配套的设备、设施(含网络)的破坏;第二种行为所破坏者仅仅是计算机信息系统内含的某一传输数据或应用程序。因而前者所影响的是整个信息系统功能的运行;后者对整个信息系统的运行没有影响,所影响者仅仅是系统所传输数据的真实可靠性和系统所含应用程序的正常运行;此外,前者的破坏对象含硬件和软件两类;后者的破坏标的一般表现为软件。例如后文例举的袭击网站的行为即属严重干扰计算机信息系统功能、使之不能正常运行的犯罪行为;而黑客对计算机信息系统内容及其应用程序功能进行涂改(如将政府主页涂改得面目全非),后果严重者,构成本罪的第二种行为。

本罪第三种行为与第一、二种行为的主要区别在于:前二种行为的破坏对象仅限于计算机“信息系统”本身或存储、处理、传输于该“信息系统之内”的数据或应用程序,而第三种行为的破坏面更大,包括已经联网和未曾联网的整个计算机网络和非网络系统。

综上分析可见,中国现行刑法第 285 条所规定的“侵入”行为,仅是其“破坏”信息系统的手段;“破坏”才是其“侵入”目的。因而从刑事法理角度看,二者有牵连关系。实践中,对此既侵入又破坏者,宜按牵连犯的原则,定一罪并“从一重处断”。由于“破坏”比“侵入”计算机信息系统罪的法定刑更重,因而在既侵入又破坏的场合,原则上宜按“破坏计算机信息系统罪”定罪量刑。

综上可见,中国刑法上的只能在网内实施的犯罪,如以“行为”作为划分依据,其实可分解为四罪:①非法侵入计算机信息系统罪;②非法删除、修改、增加、干扰计算机信息系统功能罪;③非法删除、修改、增加计算机信息系统中存储、处理或用作传输的数据和应用程序罪;④故意制作、传播计算机病毒等破坏性程序罪。实践中,此类只能在计算机信息系统网内实施的犯罪多表现为:

(1) 袭击网站。指秘密侵入他人大型服务器主机或电脑,在多部主机或电脑中安装“袭击程序”,并籍此程序在预定时间以无计其数的邮包炸弹袭击目标网站(路由器)、使其因无法存取而致全面瘫痪的犯罪行为。

新千年伊始的 2 月 7 日到 9 日三天,黑客们就采用此类名为 DDOS(拒绝服务)的入侵方式,成功地袭击了美国 Yahoo(雅虎公司)、eBay(电子海湾公司)、CNN(美国有线新闻网)等因特网上的著名网站。在铺天盖地的邮包炸弹攻势下,被袭击者不得不关闭网站入口,致其瘫痪数小时,造成重大损失。

(2) 在线传播计算机病毒。指通过在线邮局、在线下载软件的方式故意传播到他人计算机上的种种特制病毒。所谓病毒,指“编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码”。

电脑问世初期,计算机病毒主要用作反盗版的工具。也不排斥一些编程人员出于炫耀、展示自己才华的动机故意为之。而今,随着计算机技术的日益商用化、家庭化,随着国际互联网

在线网民的日趋增多,计算机病毒的制作者、传播者的行为动机、目的也发生了很大变化,除"炫耀"心理外,现今更多的人是出于商业"讹诈"、"故意破坏"目的故意为之。加之,当今某些计算机病毒在破坏软件的同时还破坏硬件,转瞬之间即可导致他人、社会乃至整个国家蒙受无可弥补的巨额损失。因而现今各国刑法几乎均将故意制作、传播计算机病毒的行为设定为犯罪,且不问其行为目的如何,只要是故意为之,即便构成本罪。在线传播计算机病毒更不例外。例如骇人听闻的梅丽沙病毒即属典型的在线传毒——它一旦运行,即自动搜集被侵机主邮件箱中的前 50 个 Email 地址,而后,假该机主名义自动向这 50 个地址发送带毒邮件;到各下一收信人那里,它又以同样的方式运行并以几何级数继续传播其病毒。而被侵入机主对自己的电脑如何染上病毒、如何被用作传毒工具的整个过程全然不知。由此可见,与一般性传播病毒方式相比,网上传播计算机病毒更快,危害性相对更大。

第二,计算机网络内外均可实施并成立的犯罪　中国现行刑法第 287 条规定:"利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的,依照本法有关规定定罪处罚"。中国现行刑法的这一规定,含"口袋"罪状,即其用"其他犯罪"这一"口袋",将现行刑法中一切可能在计算机系统网上实施的犯罪都囊括到了"计算机关联犯罪"之中。然而,计算机关联犯罪本身并不必然地等同于因特网上犯罪,还必须利用因特网络才构成本文所谓的网上犯罪,下文述及的种种利用因特网络系统实施的犯罪即属之。

(1)电子讹诈。该类犯罪包括:其一,通过因特网侵入他人系统,并通过自己的解码、编程技术在被侵入计算机系统内植入病毒或修改指令或盗获到重要商业信息后,通过勒令他人"交款才不涂改或公布你的重要客户的商业信息"、"交款才不炸掉你们银行的全部数据网"等方式,敲诈他人;其二,通过行将在线发布张扬他人隐私或毁损他人名誉的主页或电子公告、电子邮件的方式,敲诈他人在线或以传统方式付款。例如 2000 年 1 月 18 日,VISA 国际信用卡集团就宣布,有一黑客声称自己已从该信用卡集团的电子银行中窃取到有关数据信息,并以此向他们提出了 1000 万美元的勒索要求。

早期,黑客(hacker)即电脑迷们多为显示自己的高超实力而闯入他人十分保密的系统,并时常在他人电脑上打出"Hacker Tips"(黑客小费)的字样来,这期间,黑客们的种种作法多是恶作剧而已。而今则不然,入侵者不一定是电脑迷,却可能是财迷或有其他政治、经济动机者。网上敲诈者为勒索他人,甚而可能干出毁灭整个系统的犯罪勾当来。假如这个系统刚好是医院,则可能导致病历被改变或丢失,病人手术被耽误,生命不保等后果;假如系统刚好是机场指挥台,则可能导致系统紊乱、着陆的飞机相互碰撞坠毁等恶性事故发生。

(2)网上走私。指利用因特网上的电子交易或电子支付手段跨境买卖枪支、弹药、毒品等违禁品的犯罪行为。枪支、弹药、毒品、金银等为当今许多国家明令禁止私下买卖。然而,为了"安全"走私,一些犯罪分子竟然利用电子交易管理上的瑕疵,公然通过种种合法的、非法的电子销售站点成交大宗军火、毒品、金银等交易,并通过电子打包、密文传输、破译密码、修改指令等多种方式,欺蒙本国海关,将其违禁品非法偷渡、出入国境。据英国一名对有组织犯罪行为从事专门研究的官员分析,2000 年时,"在线上进行的枪械交易,甚至可能发展到核子武器,将会对国家安全造成威胁"。〔6〕

(3)网上非法交易。指行为人实施了经当事国法律或国际公法明令禁止交易或不得无证

〔6〕 参见蔡京伟:《犯罪分子拥抱信息高速路》,《华声报》1999 年 9 月 7 日。

交易的非法行为。例如中国现行刑法第 225 条就规定:“未经许可经营法律、行政法规规定的专营、专卖物品或者其他限制买卖的物品”,“扰乱市场秩序,情节严重的”,构成非法经营罪。此外,国际公法上也将出售某些禁止买卖的野生动物器官的行为规定为犯罪行为。

网上非法交易与网上走私的最大区别在于:本罪之交易性质虽然有严重违反某当事国国内法或国际刑法之处,却不涉及当事国一方的海关法规和外贸管制,即其行为仅仅触犯了该国境内或由国际法文件确认的市场交易管理法规,因而不涉及走私问题。例如网上兜售婴儿、介绍卖淫、售卖内国法或国际公法明令保护的野生动物器官(如老虎器官、犀牛角)等。又如美国著名的网上拍卖商 eBay(电子海湾)公司,为了扩大其成交份额,曾允许利用其网站销售军火、股票、酒类和烟草等。但因美国各州法律规定的不同,在一些州属于合法交易的行为,另一些州可能非法。一些犯罪分子正好利用此机非法交易。同时“管理州际酒类和烟草交易的相关法律也有可能对 eBay 公司的用户带来麻烦”,因而 eBay 公司在 1999 年 9 月 15 日业已宣布禁止通过自己的网站销售军火和股票;并声明从 1999 年 10 月 13 日起,无论是个人还是企业用户,均禁止在其网站销售酒类和烟草。“以防这些货物穿越州界可能带来的法律纠纷”。〔7〕

(4)电子色情服务及色情、虚假广告。主要表现为互联网接入服务供应商、信息供应商、应用服务供应商等出于牟利目的,不加选择地在网上提供色情信息、网上淫媒业服务或色情、虚假广告,危害网民身心健康及整个网络世界的精神文化良性发展的行为。

近年来,中国国内网络信息业发展很快。据中国互联网信息中心的统计,1998 年底至 1999 年 6 月,国内仅后缀为“.com”的网站就从 13913 个激增至 22220 个。特别是 1999 年 12 月以来,几乎每天都有新的商业网站诞生。一般而言,商业网站都会在其首页或其他网页上展示弹出式电子广告,这样做本无可非议,但一些站点为了“炒网”出名牟利,竟然藉此大干违法行径。例如近来国内网站不断发出的“竞拍”广告,就时有虚假炒作者。据报载,国内有网站以极为诱人的价格“竞拍”笔记本电脑,吸引了数以千计的消费者从头到尾泡在该站点竞拍,结果拍卖商品根本不存在。〔8〕原来商家如此广告的目的仅在增加该网站的点击率,企图以扩大知名度的方法来推促其公司股值上扬;抑或转卖其已经“出名”的网站,以卖得更高价格等。

在网上发布色情广告的案件,目前国内外均有发生。在国内,河南警方已于 1999 年底破获了一起网上传播黄毒案件。作案人系郑州无业青年何 ××、杨 ×。两人为赚取网上广告赞助费,合伙制作了隐藏在商丘信息港个人空间免费主页下的淫秽网站——“酷美女网际乐园”。自 1999 年 8 月以来,两人通过从国际互联网上下载的大量淫秽图片、色情小说,在其淫秽网页上先后发布淫秽图片万余张、色情小说百余部。

国外网络空间中,通过网络服务器公然刊出大幅色情广告、传播色情画像的案件相对更多。1999 年 9 月,英国法官已作出了关于网络色情案件的首例判决,本文将在后文对该案详加述论。

(5)网上洗钱。指犯罪分子在互联网上以密码或加密传输信息的方式,在网上销售或存储钱款,从而达到洗钱目的的犯罪活动。

常规状态下,犯罪分子通常通过银行或其他金融机构的中介转换、兑现等,使其非法资金在形式上“合法化”。信息时代,随着网络商务、虚拟钱包、电子银行、在线商店、网络租赁等业

〔7〕 见昊天编译:《eBay 禁止在自己网站上销售酒类和烟草》,《华声报》1999 年 9 月 15 日。

〔8〕 参见刘书:《小心虚假网络炒作》,《北京晨报》1999 年 12 月 5 日。

务的发展,洗钱活动也日趋电子化。犯罪分子愈来愈注意通过网上的"合法"交易,将自己的黑钱洗"白"。例如以出售毒品获得大笔黑钱的贩毒犯某A,先将其"货款"用于网上购房、进而将其转售给某网上购房户B,当B将其购房款打入A的电子帐户后,A的黑钱就堂而皇之地成为"合法"售房收入,并就此获得银行方面的、所有合法存款户一体享有的待遇和保护,如银行针对储户的保密制度、定期支付存款利息制度等。

(6)网上诈骗。包括利用网络信息服务、网络商务、虚拟钱包、电子银行、线上信用卡、在线商店、网络租赁、网上拍卖等业务的发展,所从事的种种假服务或假支付、真诈骗活动。

如今已发现有网上骗子"克隆"著名网上拍卖站点,并以该网站名义欺骗登录这些网站的用户,使得在这些网站竞拍购物者,在付款到该网站指定地点后,才发现这家网站原来是冒名顶替者。待警察得知时,该假网站早已撤出并逃之夭夭。

又如,国外一些恶意网站会在其主页或其镜像链接点上介绍一些游戏或其他颇有利用价值的新软件,诱惑网民们去游玩或下载该软件,人们一旦上当去运行该程序或下载该软件,该程序即能搜集到你计算机上保存的密码,并通过Modem指令挂断你设定的拨号连接,改拨国际长话到国外某个号码,由国外的Modem应答并建立连接。从这时起你不再是用市话或国内长话拨号上网,而是用国际长途在远程拨号上网了。因此,除了网络信息费外,你得另付高额国际长话费。难怪2000年2月以来,我国厦门地区163一些用户不断向当地电信部门投诉其未打国际长途而出现巨额国际长话费的怪现象。〔9〕

网上诈骗也包括利用网络来实施相对传统方式的诈骗行为。例如犯罪分子利用虚拟钱包制度的漏洞及其解码技术的高超,以其事实上空白(或几近空白、或不足以支付)的、真正虚拟的钱包,实现其实实在在的虚拟支付,以达到假支付、真诈骗的网上购物目的。

(7)电子盗窃。主要指以解码、修改指令或其他方式,擅自破译他人接受某项网络服务密码或侵入他人系统终端,从而达到复制他人电信号码、盗获网络接入服务的犯罪行为。例如某B以破译密码的方式,以A用户名义及其保密口令,令自己非法登录并获得China Net的网络使用权,而无论初装服务费还是继B盗获网络服务后的每一次网络使用费、在线电话费支付者仍是A而非B。因而就其实质看,B正是以盗窃的方式,来实现其"免费"接入网络服务的。

(8)网上毁损商誉。指通过电信终端,以自己设计制作的网页发布虚假信息或向众多特定、不特定的他人发送电子邮件的方式,在网上"捏造并散布虚伪事实,损害他人的商业信誉、商品声誉,给他人造成重大损失或者有其他严重情节的"犯罪行为。如今,在第五空间,一方起诉他方利用网络侵犯他人商誉的案件不少,有的还声称给自己"造成了重大损失",但尚未有构成刑事案件者。因为迄今为止,此类案件的行为人多事出有因,而非蓄意毁损他人商誉。例如北京海淀区法院审理的、北京恒升电脑公司起诉网民王某通过其个人主页损害其商誉一案即是。本案中,恒升电脑公司要求人民法院判决王某赔偿其商业损失数千万元之巨,损失看来不可谓不大。结果是,本案被告虽被判决赔偿损失50万元,学界、业界对王某是否侵犯恒升商誉的争论仍很大。不过本案被告不构成刑事犯罪,这一点倒非常明确。因为王某确曾在恒升公司购买了有一定质量问题的电脑,只因在与恒升联系解决办法时,没有达成一致,气愤之余,转而在网上公开张贴自己的意见,并号召众多网民参与"探讨"。显然,此类行为不存在故意毁损他人商誉的刑事犯罪目的,因而不能构成刑事案件。

〔9〕 参见支德林:《警惕Internet陷井》,《人民邮电报》2000年3月1日。

(9) 在线侮辱、诽谤。指利用因特网散布严重毁损公民个人名誉或声誉的犯罪行径,主要表现为在因特网上指名道姓地侮辱或诽谤特定的他人、情节严重、致法定后果者。当然,要达至犯罪程度而非民事上的侮辱、诽谤,起码应具有广泛的"扩散"行为。因而但凡通过因特网侮辱、诽谤他人者,仅往特定的他人的 Email 邮箱中散发中伤他人的电子邮件,还不足以构成侮辱或诽谤犯罪。要构成网上侮辱、诽谤犯罪,除特定结果外,行为方式可为以下任意一种:

其一,除被中伤之"他人"外,还向其他特定、不特定的人的电子邮箱中散发了此类侮辱、诽谤特定"他人"的电子邮件;

其二,直接通过行为人自设的网站或个人主页公然侮辱、诽谤特定的他人;

其三,兼采上述两种方式恶意侮辱、诽谤特定的他人。例如,据报载,一位女士曾投诉公安机关,称其前男友竟然利用 BBS(网站)作为"大字报",在网上辱骂她,其语言污秽,不堪入目。[10] 此类行为如达到刑法要求的"情节严重"的程度,可直接适用现行刑法第 246 条按侮辱罪定罪量刑。

(10) 网上侵犯商业秘密。"商业秘密",指不为公众所知悉、能为权利人带来经济利益、具有实用性并已经为权利人采取保密措施的技术或经营信息。网上侵犯他人商业秘密的行为主要表现为:

其一,以网上解码、修改指令等手段,通过因特网非法侵入他人计算机信息系统,盗获他人商业秘密;其二,通过网站或电子邮箱在线披露、使用其以盗窃、利诱、胁迫或其他手段非法获取的权利人的商业秘密;其三,违反约定或者权利人有关保守商业秘密的要求,在网上披露、使用其所掌握的商业秘密。实践中,此类犯罪以第一种网上作案方式更加常见。例如上海就有两个黑客成功地接通了上海证交所的计算机控制系统,并阅读到上海证交所的有关商业档案,从而构成对上海证交所商业秘密的侵犯。

(11) 网上组织邪教组织。当今世界各国之邪教组织,无不以宣传在世教主为"神"、世界末日行将来临之类妖言邪说,作为其吸纳信众、发展组织的理论基础。据此,纵贯全球的因特网无疑是邪教组织建立宣传站点、扩充信众的最佳空间。因而尽管邪教头头们一方面竭力宣扬自己是法力无边的"神身";另方面又不靠自己的"神力"、偏要靠其百般诋毁的现代科技力量将自己送上"神天",于是网上扩充邪教组织,成为邪教头头们扩充实力的称手工具。他们往往以向因特网中的个人电子邮箱发送种种密文,作为该组织内外联系、活动包括发展信徒的重要手段。

(12) 在线间谍。主要指采用破译密文密钥及准入口令、修改身份证认定指令等方法,侵入事关国家机密的计算机信息系统,并利用因特网实施领受间谍任务、传递间谍信息或为敌人指示轰击目标等间谍犯罪行为者。

众所周知,与现实世界相比,因特网上的比特(byte)数字世界虽号称"虚拟空间",却有着现实世界无以伦比的优缺点,首先,从理论上讲,比特数字世界都是以光速传递数字信息的;其次,它还有资源共享、存取资源自由、侵入系统快捷而隐蔽等特点。正是这些特点,为在线间谍提供了作案空间和手段。

例如美国五角大楼的计算机曾显示过"Air Force Home Page ,Altered"(空军主页被涂改)

〔10〕 参见孔屏:《混战的网络如何纳入法网》,《法制日报》2000 年 1 月 10 日。

的信息,[11]表明系统已遭到入侵。幸而该入侵者未曾盗窃五角大楼的机密文件,否则,假如此类黑客是为执行间谍任务而闯入军事机密系统,还神不知、鬼不觉地窃走了军事机密并将其提供给外国谍报机关,该案则属典型的网上间谍案。

(13)网上刺探、提供国家机密的犯罪。指间谍以外的其他行为人等,通过因特网络,为境外机构、组织或人员窃取、刺探、收买或者非法提供国家秘密或者情报的犯罪行径。

二、因特网上犯罪特点及趋势

(一)因特网上犯罪特点

1. 自然犯与法定犯并存。自然犯指刑事古典学派所主张的悖德的犯罪,可划属于罗马法上的"自体恶"(malainse)的犯罪,即其恶与生俱来、不待法律规定。法定犯又称行政犯,可划属于罗马法中的"禁止恶"(mala prohibita)的犯罪,指行为的恶性不是与生俱来,而源于法律的禁止性规定。上文例举的多类因特网上犯罪中,网上盗窃、网上诈骗可谓典型的"自体恶"的自然犯;而网上知识产权犯罪、网上侵犯商业秘密罪则可谓典型的"禁止恶"的法定犯。

2. 普通犯与国事犯并存。普通犯是相对于国事犯而言,指"危害国家安全"罪类以外的其他一般刑事犯罪。除犯罪学意义的"犯罪"外,网上绝大多数犯罪为普通刑事犯罪,但间谋罪、网上刺探、提供国家机密的犯罪等涉及国家安全,属国事犯罪。

3. 刑法学与犯罪学意义的犯罪并存。网上侵犯他人隐私、破坏言论、新闻出版自由及其网上恐吓他人的行为,虽为一些国家刑法典明定其为刑事犯罪行为,但在我国刑法中并未规定,因而,至少就我国刑法角度看,此行为在我国仅属犯罪学意义的犯罪。

4. 行为的跨国性。因特网上犯罪往往跨涉多国、多地区乃至全球。因而在犯罪管辖上,往往涉及多国;在犯罪国别形式上,往往表现为国内犯罪与跨国犯罪相交织、国内犯罪与国际犯罪相交织的形式。

5. 故意犯罪的普遍性。在犯罪主观要件上,网上犯罪一般表现为故意犯罪,但在有罪过的场合,不排斥过失犯罪。例如,在有注意义务的场合,因疏于网上注意或防范义务而致国家机密出网总部时被"嗅探"截获致泄密于境外者,仍应构成过失泄密。[12]

6. 公然犯与隐秘犯的两相交织性。在犯罪实行方式上,因特网上犯罪表现出犯罪活动的公然性与隐秘性两相交织的特征。一般而言,犯罪之恶,具有面孔的背向性、手法的狡黠性和活动的阴谋性的特征。[13] 然而因特网上的多数犯罪至少具有犯罪学意义的公然犯罪特征。[14] 即不论其刑法的规定怎样(刑法恐来不及对因特网上的犯罪作出特别规定),至少从事实角度看,此类犯罪中的多数犯罪,已经表现出"必须或必然为不特定的人或特定的多数人所共见"(非此该犯罪不能进行)的公然犯罪特征。如:网上泄露商业秘密、网上毁损商誉、网上毁

---

〔11〕 参见光盘信息:《未来战争》,湖北音像艺术出版社,ISRC CN - F06 - 96 - 407 - 00/ V. Z.

〔12〕 网上泄密,并不必然地致负有保密义务者构成犯罪。因为众所周知,网络系统的保护往往防不胜防。但在保密者有疏于注意义务或过于自信的场合,由于保密者有过失,仍应依法构成相关刑事犯罪。

〔13〕 见李建华:《罪恶论》,辽宁人民出版社 1994 年版,(序)第 3 页。

〔14〕 刑法意义的公然犯罪,指按照刑法特定犯罪构成要件及其刑罚规范的预设,某种犯罪行为必须或必然地表现为故意在不特定的人或者多数人能够认识其犯罪行为的场合、仍然实施该犯罪的罪态方式。犯罪学意义的公然犯,则不以刑法的规定为限。见屈学武:《公然犯罪研究》,中国政法大学出版社 1998 年版,第 29 页。

损名誉、网上假冒注册商标、网上假冒专利、网络色情服务、网络色情广告、网上虚假广告、网上非法交易、网上扰乱市场、网上扩充邪教组织等。

另一方面,网上犯罪的场合,行为人破译密钥密码及编程技术手法上的隐秘性,又使其具有隐秘特征。因而公然性与隐秘性两相交织,是因特网上不少犯罪共有的特征。

7. 无犯罪现场性。刑事法上的所谓犯罪"现场",一般是指目击者、扭送者、追捕者目睹、擒拿人犯视力所及的场域。因特网上犯罪既实施于虚拟空间,即没有这种"现场"可言。因而,某种意义上可以说,因特网上犯罪,具有犯罪人永不在现场的特点。而且这种"不在现场",不仅不在有关人士目力所及现场,还有可能根本不在受害人或受害国所在的刑事司法管辖领域。

8. 犯罪危险及结果的广域性、变异性、快速性。网上数字世界,本来就是以光速传递数字信息(byte)的高速世界,因而因特网上的犯罪结果往往瞬间即成、稍纵即逝并能很快蔓延,危及世界各地。例如网上发射电子邮件炸弹,即能在很短时间内以数以几十亿计的邮包堵塞多个目标主机的路由器,致其很快瘫痪。

9. 犯罪证据的可修改性。对某些高明的黑客而言,其作案证据可通过预先安装好的、作案完毕便自动运行的、抹平证据的程序来抹去。如此一来,即便是具有高超计算机技术知识的行家,要想捕获此类作案人都十分困难。例如 2000 年 2 月 7 日至 9 日,通过邮包炸弹瘫痪了著名网站的作案者,就在短时间内抹平了该作案痕迹,逃之夭夭,以致美国官方至今也未曾捕获到操作该案的全部黑客。

10. 犯罪成本的低投入性。从社会经济学、制度经济学角度讲,网上犯罪可谓典型的低投入、"高产出"犯罪。且其不仅仅是经济成本上的低投入,还包括风险程度上的低投入、高产出。反之,遏制、打击之,却须消耗相对大得多的反犯罪成本。

(二)因特网上犯罪趋势

1. 网上犯罪平民化趋势。所谓"平民"是相对于科技人才而言。因特网刚由军事目的转入民用时,人们须有相当程度的电脑编程、应用能力,才能实施破坏活动。而今却不然,侵入并破坏计算机的安全系统几乎成了一般网民均能办到的事。因为在今天,打通或穿透整个系统的工具均能在国际互联网上轻易获得,黑客们在国际互联网上开设的教习"如何入侵计算机信息系统"的网站更是比比皆是,任何一名"上心"的一般网民均能在短时间内自我"培养"成为一名黑客。难怪国际刑警们惊呼:到 1999 年底,因特网上已有 3 万多个黑客网站,全球有近 1700 万人具备"黑客"电脑的技术。由此可见,如不加以有力遏制,网络犯罪的平民化,势将在新的千年愈演愈烈,导致网络犯罪总量的更大幅度攀升。

2. 在线寻找作案目标的趋势。随着电子银行、电子商务的发达,犯罪分子也开始将作案目标瞄准网上搜寻:如设法进入银行计算机系统,阅读到银行内部掌握的储户存款资料后,即可通过修改指令,将他人虚拟钱包中的钱"转入"自己钱袋中;抑或,也可通过对"存款大户"的掌握,预先排定作案目标,以便实施传统的抢劫、敲诈勒索乃至盗窃等犯罪。

3."虚拟毒品"趋势。据报载,"随着互联网的不断发展,各种形式的高科技犯罪行为,将会渗透到社会的每一角落。有专家预测说,网上将会出现一种'虚拟毒品',这是一种可以通过互联网传输的数码'兴奋剂'或者'迷幻剂',可以使人上瘾"。[15] 然而,这种可以使人"上瘾"的数码兴奋剂或迷幻剂既然被称作毒品,可以想见,它势将同真实的毒品——可卡因、海洛因等一

[15] 见前引[6],蔡京伟文。

样 ——几乎无可摆脱地终身残害“瘾君子”的身心健康,直至死亡。

4.“禁止恶”大于“自体恶”、普通犯大于国事犯罪比例的趋势。如网上操纵证券交易价格、毁损商誉、虚假广告、假冒专利、假冒注册商标等犯罪都是法定犯而非自然犯。由于网上尚不能直接实施必须与被害人或被破坏物面对面的接触方能完成的“亲手犯”,如不能实施杀人、抢劫、强奸、抢夺、伤害、放火等杀人越货的悖德犯罪,加之现代社会,整个法定犯的比例日趋扩大,因而网上犯罪也呈现出法定犯多于自然犯的趋势。

5. 网络使用者比网络提供者所实施的犯罪种类更多、总量更大的趋势。网络提供者,指互联网接入服务供应商,无论是一级网还是二级子网服务供应商;网络使用者包括互联网信息供应商和互联网用户。虽然从理论上看,网络提供者具有实施上述几乎所有网上犯罪的能力,但就基本情理看,实施上述多类犯罪一般不符合其作为互联网服务供应商的设立宗旨。从数量上看,大量的网上犯罪,主要为网络使用者所实施。然而,毋庸讳言,网络提供者一旦实施网上犯罪行为,就可能具有较之网络使用者大得多的破坏力。例如网络提供者可关闭某一方甚至某一国的局部乃至全部网站;破坏某一方甚至某一国的局部甚至全部网络通道。

6. 网上犯罪数量剧增且总量居先的趋势。根据中国互联网信息中心(CNNIC)的统计显示,截止 1999 年 6 月,国内共有互联网用户 400 万,是香港的 4 倍,1999 年底达 700 万;2000 年初达 900 万。到 2002 年我国上网人数将紧随美国、德国之后,位居全球第三,达 3200 多万,而美国在 1999 年已达 9400 万。随之而来的是互联网所带来的无限的商机和隐伏在商机之后的犯罪的增多。例如仅以我国香港特区的网上犯罪举例便可见一斑。1998 年,香港的网上犯罪仅 38 起;1999 年猛地扩大了 7 倍多,达 296 起。其中,非法侵入他人电脑的犯罪由 1998 年的 13 起增至 218 起;发送淫秽物品的犯罪由 13 起增至 32 起;互联网购物诈骗由 1 起增至 17 起。可见,从比例关系看,网上犯罪的增幅远比网民的增幅比例高得多。

就我国总体情况看,由于计算机网络化程度在我国尚不高,因而眼下,计算机网络犯罪在我国尚低于线外犯罪总量。但从趋势上看,随着国家科技的日益发展,随着现代社会生活的进一步智能化、网络化,网上犯罪的总量最终将超过线外犯罪总量。美国印第安那州韦恩(Wayne)大学的约瑟夫·阿尔比里(Joseph Albini)曾预言:“到 2000 年时,90 %多的有组织犯罪是由那些高水平的计算机罪犯完成的。他们利用高科技的手段,通过大众媒体进行犯罪。从而使他们从普通的犯罪分子转化成一个影响力极大的超级罪犯。”

7. 网上信息战争趋势。战争罪、侵略罪、灭种罪等,均属“严重危害国际社会根本利益,依据国际公约确定为犯罪、应予刑罚惩罚”的国际犯罪行为。[16] 国际犯罪与一般国内犯罪不同的是,其犯罪主体不仅限于一般个人或团体,还可能是整个国家。

战争罪、侵略罪本是最严重的国际犯罪之一。未来新世纪的战争虽难免荷枪实弹的面对面的武器较量,但是,鉴于新世纪中,不仅仅美国、全球均在步入由计算机网络控制国家的财政系统、经济系统、交通运输系统、能源系统、行政乃至整个国防系统的时代。因而,在此信息时代中,敌对双方仅须信息战争即可使对方国防瘫痪、能源中断、交通失序、财政紊乱、经济崩溃。基于此,假定作为侵略一方的国家,悍然进入国际互联网,通过计算机热线和卫星截断另方通讯,植入足以使计算机系统紊乱的病毒,或足以“刺杀”对方计算机系统的计算机软件“小虫”,甚至“特洛伊木马”式的计算机逻辑炸弹 ——并通过因特网或遥控装置致对方核动力工厂熔

〔16〕 见廖增昀:《国际犯罪与我国刑法完善》,《法学研究》1996 年第 6 期。

化、永久性国民防御设施毁损,全国通信、能源中断,政府指挥失灵、飞机坠毁、火车相撞……显然,这种通过因特网发动的侵略战争行径,乃是假手人类文明成果对人类文明的致命扼杀与摧毁。而这种今天听来还"耸人听闻"的信息战争,明天可能成为摧毁人类文明的现实,因而,它理当引起全世界爱好和平人民的充分警惕和防范。〔17〕

三、对网上犯罪的遏制措施

因特网作为一柄双刃剑,自其诞生到现在,其无比的强大性和极大的脆弱性随着时间的推移愈益明显。循此特征,它在犯罪与反犯罪领域也存在着既有利于搜索、查获罪犯又便于罪犯低风险、高"效益"作案的两面性。

据新华社 1999 年 9 月 15 日报道:我国各地"公安机关对本地 1990 年以来,负案、批捕、刑拘在逃的犯罪嫌疑人、罪犯,以及 1990 年以前的重要在逃人员进行了调查,将身份资料输入'在逃人员信息系统',并进入计算机网络。截至目前为止,警方已经在网上抓获在逃人员近 8 万名,其中公安部督捕的在逃人员 281 名"——仅此"一斑"足见互联网络的无比强大。

然而,正由于其无比强大,才为犯罪提供了更好的第五空间。在此空间,人们在遭到非法侵入时,难以象在第一、二、三空间那样,可以很快或最终面对犯罪人。第五空间的某类罪犯,你可能永远无法寻到。因为你很难知道他(或她)来自何方?什么时候来?为什么来?有鉴于此,面对因特网上的罪恶,综合法律界、科技界、计算机软硬件编制、生产部门、政府与国家乃至国际间的全方位的协同努力、共同防范,可能比单纯的破案与打击更见效。目前国内外正着手并拟议实施的措施包括:

(一)犯罪学措施

1. 计算机及互联网技术系统的完善。从犯罪学意义看,堵塞性预防是预防各类犯罪的行之有效的重要手段。从计算机信息系统看,为防止黑客穿透或打通自己的系统,确保网络安全,需从如下几方面着手堵塞漏洞:

(1)设立防火墙。防火墙是计算机内部系统与因特网接入服务商提供的外部网络系统之间的过滤屏障,以防止非法数据及非法用户的侵入。其作用虽非万能,但却是确保网络安全的充分必要条件之一。

(2)身份认证。除一般的密码口令外,身份认证还可采取系统对人体指纹、眼睛形状、声音记录的识别以及读卡机对智能卡的识别等方法,替代自己的通行词(password)以登录上网,从而防止自己的个人资料、在线信用卡密码被破译、自己的电子帐户被盗用,等等。

(3)加密与数字签名。如上所述,而今,由于有多种工具可用于截取人们在互联网上自由支配的密码,密码的效用愈来愈低下,因而对至关重要的密件进一步加密十分必要。现行加密技术实质是一种信息的重新组合,收发双方必须使用同一密钥,才能加密和解码,从而还原其本来信息。硬件方面,目前国际上一些大型计算机软硬件公司,如 Inter 公司、IBM、微软公司等在亚特兰大举行的 Network + Interop 大会上公布了"点到点"的安全网络解决方案。包括针对微机和网络服务器的"互联网协议安全"(IPSec)产品。此项产品将被康柏、IBM 等计算机

〔17〕 参见:《未来战争》,光盘资料,湖北音像艺术出版社,ISRC CN - F06 - 96 - 407 - 00/ V. Z.

厂商用于自己的计算机,以保障计算机网络的安全,防止个人监视局域网通道。[18]

数字签名实质是密上加密、组合加密。即密文和用来解码的密钥一起发送,而密钥本身又被加密,还需要另一个密钥来解码。据此,信息的密钥和密钥的密钥的有机组合构成了数字签名。

2. 公安系统科技网络的建立与完善。公安系统科技网络的完善,不仅在于将有前科者和在逃人员的姓名、性别、体貌特征、身份证号码、照片、指纹档案、声音记录、DNA 资料乃至面部毛细血管分析图等输入计算机系统,也不仅仅在引进初开发 CCIC 系统、可疑物品管理系统,或建立起"帧中继"网,等等,对于网络犯罪来说,公安科技网络的完善,还在于建立起自己的反计算机网络入侵的"网络侦探"。此类"网络侦探"乃大量与各种网络联系的计算机。其主要任务是通过因特网热线、专门跟踪监视软件及其他设施,追踪、查获黑客及网上冒名者、网上嗅探,防止其袭击特定的系统。并对已经遭到袭击的计算机提供跟踪搜索与技术援助,并尽最大努力保全遭到入侵的系统。[19]

显然,此类公安系统的建立、健全与完善,需要强大的物质经济及高精科技基础,因而,对处于发展之中、但正在起飞的我国而言,它既需要相当长的建立健全完善时间,又需要抓紧时机、大力着手并强化此类建设,以处理新世纪在线犯罪对人民公安的挑战。

3. 预防犯罪网络的建立和完善。所谓预防犯罪网络,包括:(1)职能部门的预警网站;(2)职能部门的预防犯罪网站;(3)群众性预防犯罪网站;(4)网内外相结合的预防犯罪系统。

众所周知,信息的开放性、互联性与便用的隐秘性,是因特网的重要特征,惟其如此,利用因特网络建立预防犯罪机制,对于有效遏制网上犯罪大有裨益。就当前网络犯罪的发展趋势看,既然黑客技术已经愈来愈平民化,反黑客的预防犯罪网络也当相应群众化,才能更加卓有成效地打击因特网上犯罪。因而,此类预防犯罪网络,也应采取职能系统与群众系统相结合的方法来运作。所谓职能系统,指公安机关、检察机关等设立的预警网站和预防犯罪的网站及其配套设施;所谓群众性系统,指群众自发开辟的宣传预防因特网上犯罪的网页及其他举报网上犯罪设施或在线邮箱等。

据报载,北京丰台区检察院前不久已成功建立了国内首家"预防犯罪网站"。该网站开辟了"预防网络交流"、"个案预防"、"行业预防"、"专项预防"、"普遍预防"、"案例分析"等栏目,并创办了"预防犯罪论坛"电子杂志。我国香港特区政府也开办了防范电脑犯罪的训练班等。此类预防措施均属职能性预防。而共青团、学校、计算机知识训练班、报纸、书籍等机构及传媒开设的防止电脑网页被"黑"、防范电脑病毒等课程或有关知识,则属群众性预防犯罪系统。这在我国还处于相对朦胧、自发的阶段。有关部门应当强化此类预防工作的引导和培育,以形成专门预防与全民预防网络犯罪的良好气候和环境条件。

(二)刑事法措施

1. 刑事侦查系统。即采取线内外相结合的方法,创设侦破线上犯罪的软硬件有机结合的侦查犯罪网络,以有力打击互联网上的犯罪。众所周知,在互联网上作案者,行为地与结果地往往各异,甚至远隔重洋;加之作案者不是匿名,就是将犯罪证据以数码记录,再编译成密码逃避侦查;或者在可能暴露的证据中安装涂抹、修改证据的程序:一俟其犯罪行为完成,则以其预

[18] 参见吴昊天编译:《英特尔等 PC 巨头宣布网络安全计划》,《华声报》1999 年 9 月 15 日。

[19] 参见吴昊天编译:《网上布下天罗地网》,《华声报》1999 年 9 月 15 日。

前安装的定时自动运作的涂改程序抹去全部证据。因而打击网络犯罪,显然需要计高一筹的网络定位侦查系统。基于此,我国内地公安机关已设立了计算机安全监察处。我国香港特区警方也已于 1999 年底成立了一个 18 人组成的电脑罪案组,专职侦察电脑犯罪活动。为配合办案,香港警方同时设立了一个经过专门训练的 80 人组成的电脑罪案调查支援组。香港廉政司也设立了一个 7 人组成的电脑资料监证及资讯科技研究组,等等。另据了解,香港特区廉政司还在考虑作出"互联网服务供应商需在一段时间内保存用户的往来电子邮件或其他记录,以作为警方调查重要线索"的规定。我们认为,这一规定为网上刑事侦查系统顺利破案,提供了一定便利条件,值得推广借鉴。

2. 刑事审判运作。司法运作的成功与否,直接关系到对因特网上犯罪的打击力度及其遏制程度。迄今为止,网络犯罪虽然有增无减,但由于立法滞后、取证困难、破案率低下等原因,致使迄今为止将此类罪犯诉诸公堂者寥寥。我国台湾对传播 CIH 病毒的案犯审理可谓一例;前不久英国方面又传来突破性进展。

据吴昊天编译的 1999 年 9 月 7 日的 Infonews 专稿称:英国法院关于网络色情案的判决,成为全球网上刑事犯罪首次判例。据称,"反对 Internet 色情的斗争获得巨大进展,伦敦 Southwark Crown 案的一项判决成为全球首例"。

该案中,格雷厄姆·沃迪恩(Graham Waddon)是来自萨里(Surrey)的一名 29 岁商人,因通过设在美国的服务器从事英国历史上最大规模的色情活动而被判处 18 个月的监禁,(因病)缓期执行。

实际上,就英国法律规定看,迄今为止,个人通过国外的服务器传播色情作品是否会遭到起诉,英国制定法并没有明确规定。但英国是判例法国家,法官根据有关判例原则可对新行为作出判决。从而可能创制出新型的法律原则乃至新罪名来。如本案中,英国的克里斯托弗·哈迪(Christopher Hardy)法官就在这项"具有里程碑意义的判决"中指出:"只要这些色情图片是从英国国内网上下载的,就应当按照英国的法律治罪"。

据此,专家们相信,这次判决等于向那些网络色情作品发行者发出了明确的警告:即使你们的服务器设在英国以外,你们的行为仍然触犯了英国法律,表明在 Internet 上也是"有法制的"。专家们还相信,哈迪法官的判决将对打击 Internet 犯罪活动产生巨大的影响,基于因特网和大型网络上的犯罪活动均将遭到沉重打击。

我们认为,英国法官的这次判决,不仅在英国法律上具有里程碑意义,而且应当及于全球的网络犯罪立法与司法。各国应当强化对此类犯罪的立法与司法,以便更加卓有成效地惩治此类犯罪。

在国内,如前所述,河南警方已于 1999 年底破获了一起网上传播黄毒案件,对在淫秽网页上先后发布了万余张淫秽图片、百余部色情小说的作案人何××、杨×的审判,将是国内互联网上此类案件的首次判例。

将英国法官与中国法官所审理的案件性质相比,两者所审理的行为及其结果地不同:前者行为地在美国,案发结果地却在英国;后者却属行为与案发结果地都在中国。因而作为判例,前者比之后者,对刑法空间效力管辖原则的突破,有着更加切实的指导意义。

3. 网上犯罪的立法完善。在此新旧世纪之交,随着第五空间犯罪比例的扩大,立法机关将面临着越来越多的难题。

第一,网络立法的建立健全。

据报载,国际互联网的发明人之一罗伯特·卡约曾提出了对所有因特网用户实行许可证管理制度的建言,主张对所有获得上网帐号者,均需先行一定阶段的入网行为规范教育,使他们充分了解自己的权利和义务,从而,令信息高速公路上的冲浪者象公路上的司机一样承担起责任来,以最大限度地避免上网伤害别人或为别人所伤害。

我们认为,这一立法建言,从长远看,有其推广、应用价值。但眼下就推广、应用于我国还缺乏可行性。原因有二:一是国内网民数量的迅速扩大及其异常庞大,令我国政府难以组织起相应庞大且愈来愈大的培训队伍,而如为此耽延了民众上网,又不利于我国科技与经济的发展,不利于民众生活质量的提高、旨趣的扩大,因而殊不可取。其次,现今网站上有许多免费上网服务,此类服务既毋需交费、也毋需办理其他任何网外登记手续,只要申请人成为其网站会员即自动取得一定时间内的上网资格。因而培训发照的事宜也难于操作。假如以立法形式简单地禁止免费上网服务,又会有碍网站的竞争和发展,不符合经济发展的规律,仍不可取。

为此,当前在我国,建立相对完善的涉及民事、刑事等实体法律规范的网络立法至关重要。目前,由于因特网络发展异常迅速,各国均未来得及规制出相对完善的法律来规则该虚拟空间的法律秩序,相比之下,美国的网络法相对"完善"并渐成体系,可在一定程度上为我国立法时参照考虑。

美国的网络法由多个单行网络法案构成,包括《网络免税法案》、《网络公平法案》、《电子隐私权法案》、《儿童网上隐私保护法案》、《电子信箱保护法案》、《电子信箱使用者保护法案》、《数字签名和电子印鉴法及互联网上禁赌法案》等。由此可见,由这些系列法案构成的美国网络立法,既含民事立法规范、经济行政立法规范,也有若干刑事立法规范。

我国现行的(广义上的)网络法规多属行政性、程序性法规,虽然其间含有个别附属刑法规范,但都没有超出我国现行刑法对计算机信息系统犯罪的规定。例如,国务院关于《中华人民共和国计算机信息系统安全保护条例》、邮电部关于《中国公用计算机互联网国际联网管理办法》、公安部关于《计算机信息网络国际联网安全保护管理办法》、《计算机信息系统安全专用产品检测和销售许可证管理办法》、《中国互联网络域名注册暂行管理办法》、《金融机构计算机信息系统安全保护暂行规定》、国家保密局关于《计算机信息系统国际联网保密管理规定》,以及省地方政府颁布的如《黑龙江省计算机信息系统安全管理规定》、《四川省计算机信息系统安全保护管理办法》等,均属此类广义的网络法规。

这些法规对计算机信息系统安全保护的责任、安全保护的监督、安全保护的义务、违法责任等都作了一一规定。但就其规范性质看,其规范内容基本限于网络内外的安全保护或准入准出问题,尚未有专门的关于民法、刑法等部门实体法的网络法规范出台。由此可见,与美国相比,而今我国面临的不是网络法完不完善的问题,而是网络法体系尚未形成的问题。因而如何建立健全我国的网络立法,在我国还是一个任重道远的问题。

第二,刑事犯罪的管辖范围应否扩及"第五空间"的问题。

对刑事犯罪的管辖,各国多采地域主义为主的原则。传统刑法的"地域"(即领域)仅含领陆、领水、领空、浮动领土,[20]不包括"第五空间",因而对发生在本国领域外、又非直接针对本国国家或特定公民的第五空间犯罪,以属地原则为主、其他属人或保护原则为辅的传统刑法的

[20] 浮动领土,又称拟制领土。指悬挂本国国旗或国徽的停泊、行驶在任何海域、(太空以外之)空域的本国船舶或者航空器。

管辖权显然难以覆盖。惟其如此 ——上文提及的英国克里斯托弗·哈迪大法官审理的网上色情服务案,才以判例的形式对英国刑法的刑事管辖权作出了"具有里程碑意义的判决"。尽管如此,英国法官认为"应当按照英国的法律治罪"的依据并不在对单纯的"第五空间"的管辖主张,而是因为该"色情图片是从英国国内网上下载的"。即:是"下载"导致了英国"领域"的接通与进入,从而构成了格雷厄姆·沃迪恩在英国"领域"的犯罪。由此逆推,假定网民们仅仅在网上收看、未曾"下载",英国刑法是否就没有了管辖权呢?类似案件,中国刑法又当如何处置、规定呢?例如 ——

无国籍人某 B 在 Z 国 X 网站实施了通过因特网传授邪教教义并发展邪教组织的行为 ——访问该网站的任何人等因此均可在该站主页上读到其教义并在线入教;假如中国公民 C、D、E、F、L 等百十人因此在网上"受洗"并在线入教。这样,某 B 的行为无疑涉嫌构成中国刑法第 300 条规定的"组织邪教组织罪"。然而对本案,中国刑法碍难管辖。因为因特网域既非领陆、领水、领空,也非浮动领土,不属于上述四大领域之任一部分,本案行为及结果不发生在中华人民共和国"领域内",加之行为人某 B 既不是中国公民、又不是针对特定的中国国家或公民的犯罪,因而根据中国现行刑法关于空间效力的规定,中国刑法无权管辖。

由此可见,传统刑法的空间管辖规定,存在不能有效管辖因特网上犯罪的立法缺口,随着时间的推移、网上犯罪比例的扩大,缺口会更大。值此新千年之际,我们认为有必要未雨绸缪:反思传统刑法对于新空间管辖规定的不足;构想超前性的刑法新"领域"。简单地说,我们认为,随着信息世纪的到来,刑法的"领域"宜于有所限制地扩大到第五空间。

有所"限制"地扩大,是因为因特网域并不当然地等同于各国刑事法域,第五空间也不当然地属于各国刑事管辖空间,否则,由于国际互联网络几乎及于世界各地,无限制的领域"扩张",无异主张因特网上犯罪等同于全球犯罪。全世界任何地域因之均享有一体管辖权?似此"领域"扩张泛化下去,国家主权原则必将受到极大影响和损害。

"限制"的内容,可设定为具下列条件之一时,刑法领域可扩至第五空间:

(1)网上作案的终端设备地、服务器设立地在本国第一、二、三、四空间范围内。如在线洗钱者、电子敲诈者的终端所在地、[21]网上色情服务器的设立地在本国领域。

(2)网上作案所侵入的系统局域网或侵入的终端设备地在本国第一、二、三、四空间范围内。如电子间谍、网上侵犯商业秘密者的系统网站或终端所在地在本国领域。

(3)行为人获取、显示网上作案结果信息的终端所在地在本国第一、二、三、四空间范围内。例如网上盗窃、网上诈骗作案信息显示终端所在地在本国领域。

需要特别说明的是,上述可扩大的刑事犯罪领域的条件,只是对"犯罪的行为或者结果有一项发生在本国领域内,就认为是对本国犯罪"的属地原则的补充,而非相排斥。因而,在承认上述"扩充"条件时,对某犯罪行为主张管辖权的地域范围理所当然地有所扩大。例如,对来自 A 国的某网上商业诈骗犯 B,在 C 国被骗的受害人可根据"结果发生地"原则在 C 国主张管辖并控告;A 国可根据"属人原则"主张 A 国管辖;D 国则可根据 B 是利用其在 D 国的终端获得诈骗结果信息、而主张 D 国对本案的管辖权 ……

——本案中,D 国根据上述第(3)种条件将其刑事管辖领域扩到了第五空间并主张管辖。

[21] 终端,在此指供行为人使用的、与因特网或局域网相连接的网络接入服务器、计算机工作站、PC 机、付款机、传真机、掌中宝小电脑等。

这种“扩大”,可能带来管理上的冲突、争讼或推倭,但长远来看,它对强化惩治因特网上犯罪的法网密度及犯罪控制,很有裨益,利大于弊,值得考虑。

第三,控制网上犯罪的立法模式。

随着新世纪的逼近,对网上犯罪的特别刑事立法、附属刑事立法,愈显必要。当前,就我国新出台的刑法典看,现行刑法典关于网络信息的犯罪仅只刑法第 285 条至 287 条三个法条、两种犯罪。即:非法侵入计算机信息系统罪和破坏计算机信息系统罪。

刑法第 287 条则属无个罪规定的重申性“筐式”罪状,根据该条规定,凡“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的,依照本法有关规定处罚”。据此,除刑法第 285 条、第 286 条规定的犯罪以外,凡在计算机网络中实施了刑法典中其他任何法定犯罪行为者,需各自适用相关法条。而因特网上犯罪的特殊性质,又决定了刑法第 287 条的“筐式”罪状,难以覆盖因特网上所有罪恶。例如前文述及的“打通或穿透整个系统的工具均能在国际互联网上轻易获得”的问题,究竟是一个软件赠与或售让的民事问题,还是帮助犯罪或传授犯罪方法问题?就是说,对提供各类非法侵入系统的 key(密钥)或其他帮助的网上软件售让人,除民事、经济法律外,各国刑法能否定罪、管辖?根据什么罪名管辖,诸此问题值得一一研讨。

中国现行刑法第 295 条所规定的传授犯罪方法罪,在罪状设定上仅是“传授犯罪方法的,处 ×××刑”的简单罪状表述。显然,传授犯罪方法与提供犯罪工具是两个既相联系又有区别的概念。而要打通或穿透整个系统,光有工具、没有高技能的方法又难行得通。因而,对诸如此类的网上不法行为的立法绳禁模式,值得刑事法理界、刑事实务界预前进行调查、总结、预测、估算并提出可行的立法思考或方案,以供立法机关完善这类法律时斟酌。我们认为:

首先,对因特网上犯罪,宜采以附属刑法与单行刑法为主、普通刑法为辅的立法模式。虽然,对整个刑事犯罪构成及其刑罚设定而言,刑法典始终是主体;但具体到对某类特殊犯罪——特别是因特网上犯罪规定时,现行刑法典的规定显然已经滞后。

这是因为,就因特网上犯罪看,信息时代的到来必然引发社会政治经济体制和各类规范的急遽变迁,作为社会“存在”能动反映的政治上层建筑——法津制度亦会发生相对快速的变革。为此,想要以一部相对稳定的刑法典将包罗万象的法律现象特别是日益变迁的网上犯罪现象尽皆规范进去,既不现实也不可能。加之,如前所述,行政犯在整个因特网上犯罪中将占据更大比例,这是未来因特网上犯罪的类型演化趋势。因而我们更赞成以单行刑法、特别是附属刑事立法的方式,将“日新月异”的因特网上犯罪规制进去。例如,上文述及的在互联网上提供“打通或穿透整个系统的工具”的问题,显然就不是一个软件赠与问题,而是一种特殊的提供犯罪工具与传授犯罪方法相结合的网络犯罪行为,宜通过单行刑事立法的方式,对其作出相应的犯罪设定。

其次,对附属刑法宜采用“一步到位”的“双轨”立法模式。我国现行的单轨刑事立法模式,导致了附属刑法往往只有简单罪状而无相应罚则规定,由于其有罪无刑,司法上也就不能操作。按照我国立法例,遇此情况,须待立法机关修改刑法典或出台单行刑事条例、作为附属刑法特设的罚则,尔后附属刑法上规制的犯罪才能成为真正的、令行禁止的刑法规范。如此操作,难免产生下述弊端:(1)从社会效益看,刑法规范久久形同虚设——令不能行、禁不能止,必然损害国法的严肃性、权威性。(2)从经济效益讲,立法不能一步到位,必然延误时日甚至旷日持久、耗资本身即更大;同时,既定的社会规则难以及时有效地运行,市场经济下的“社会产出”

也难免蒙受影响并进一步影响到"社会产出大于社会投入"的效益立法原则。因而,我们不妨借鉴国外的"一步到位"的立法模式——在条件成熟时,对因特网上的犯罪,宜在附属刑事立法的同时,径直设定法定刑。

再次,有关因特网上的国际犯罪与国内照应立法问题。因特网络的国际化、普及化,使一些国际公约设定的刑事犯罪,愈来愈涉足因特网域。如《联合国禁止非法贩运麻醉药品和精神药物公约》规定的国际毒品犯罪、洗钱犯罪,《国家责任公约草案》、《危险物品国际贸易公约》(CITES)所规定或涉及的危害国际环境的犯罪,《联合国宪章》、日内瓦四公约、《防止及惩治灭绝种族罪公约》等设定的侵略罪、战争罪、灭种罪等,都不同程度地表现出已经或可以对在线作案的防范趋势。

除传统的国际犯罪外,因特网络的全球化、一体化趋势,还决定了因特网上的若干危及全人类发展与安全的犯罪的国际化,例如侵入信息系统的犯罪、破坏信息系统的犯罪、在线提供侵入系统的工具,等等。有鉴于此,对此类发生在国际互联网络上的、危害全球发展与安全行为的"国际犯罪"的法定化,势在必行。就是说,为要遏制有关侵入系统的因特网上犯罪、为要掣肘未来信息战争罪犯们利用信息网络技术发动侵略战争等,各主权国家及其他国际法主体,通过联合国或其他多边形式,订立一个或多个专门防范或禁止各方实施上述危及国际秩序的网络犯罪的多边国际公约,十分必要并切实可行。

然而,因特网上的国际犯罪的设定还需要国内照应立法,否则难以操作。我国在照应立法方面所作不少,但迄今为止,对照我国已参加的国际公约看,《中华人民共和国刑法》作为刑事立法尚未充分照应我国参加的国际刑法规范。例如我国早在 1983 年就参加了《防止及惩治灭绝种族罪公约》,因而应当承担惩治灭种罪的国际义务。但我国现行刑法典既无此罪名规定、也无法定刑。从而根据现行刑法第 9 条的规定,我国对此犯罪虽享有普遍刑事管辖权,却因有罪无刑,仍难操作。与我国相比较,1996 年俄罗斯国家杜马新通过的俄罗斯联邦刑法典则相反——为了照应其已参加的国际公约,俄罗斯刑法专门规定了战争罪、侵略罪、种族灭绝罪、生态灭绝罪,等等。我们认为,为要有力惩治涉足因特网域的未来国际犯罪,特别是信息战争罪、侵略罪等,我们似应在此方面迈出更大一步。

Abstract : First of all the article explores definitions and categories of internet related crimes from the perspectives of criminal law and criminology in different jurisprudence. Then it analyses characteristics and trends of internet related crimes ,where the author raises some law problems which need to be solved as early as possible ,such as particularity of internet related crimes ,jurisdiction for the fifth space. Finally the author illuminates her legal insights into internet related crimes ,including initiatives for prevention of crimes 'BBS and judiciary administration and proposals of law-making for network - crimes.