网络犯罪防控对策

李双其 主编

群众出版社

网络犯罪防控对策

李双其　主编

撰稿人：李双其　曹文安
郑　荔　黄云峰

群众出版社
2001·北京

图书在版编目（CIP）数据

网络犯罪防范对策 / 李双其主编 . - 北京：群众出版社，2001.9

ISBN 7-5014-2531-0

Ⅰ. 网… Ⅱ. 李… Ⅲ. 计算机网络 - 计算机犯罪 - 犯罪侦察 Ⅳ. D 918

中国版本图书馆 CIP 数据核字（2001）第 052689 号

网络犯罪防控对策 李双其 主编

责任编辑 / 张忠华
封面设计 / 书 学
技术设计 / 祝燕君

出版发行 / 群众出版社 电话：（010）67633344 转
社 址 / 北京市丰台区方庄芳星园三区 15 号楼
邮政编码 / 100078
印 刷 / 北京京安印刷厂
经 销 / 新华书店

850×1168 毫米 32 开 14.25 印张 337 千字
2001 年 9 月第 1 版 2001 年 9 月第 1 次印刷
印数：7000 册

ISBN 7-5014-2531-0 / D·1192 定价：24.50 元

前言

在漫游赛博空间的过程中，常常能捕捉到有关网络犯罪的信息，偶尔也能切身感受到这一虚拟空间里犯罪现象的存在。随着赛博空间人口的急剧膨胀，在此虚拟社会里的犯罪现象已是一个必须高度正视的问题。同时，在阅读国内外有关网络犯罪的书籍时，也觉察到系统论述网络犯罪的书还极为鲜见，由此，便产生了研究网络犯罪的动机。

2000年初，国际许多著名网站遭到骇客的疯狂攻击，进入新千年后，中国内地也频频发生网络犯罪事件，在一种山雨欲来的感觉里，更坚定了将动机付诸实践的信念。

2001年初，笔者召集若干具有扎实的法学、犯罪学、侦查学基础并在网络空间驰骋多年，对网络技术颇有研究的学者，共同讨论网络犯罪问题。讨论的结果是：普遍认为有研究网络犯罪的必要，对此课题的研究很有意义，很有价值。

于是，立刻行动起来：拟定提纲，展开调查，广泛搜集资料，深入虚拟空间继续实践，讨论分析，分头撰写。在研究的过程中，人们普遍感到在这一领域里确实有许多值得研究的问题，而且有很多问题仅凭笔者的能力是诠释不清的。在撰写过程中，我们吸收了《法制日报》、《人民公安报》、《光明日报》、《中国青年报》、《科技日报》、《电脑报》、《北京青年报》、《生活时报》、《海峡都市报》、美国《时代》周刊、美国《未来学家》、《南洋商

报》、《羊城晚报》、《澳洲日报》等报刊以及新浪、cnnic、中新社、eNet 硅谷动力、ChinaByte、互联网周刊、yabuy、人民网、Ask100 等大量网站上刊载的有关网络犯罪的案例，参阅了各种媒体上登载的有关网络犯罪的文章和近期出版的有关网络犯罪的书籍，同时吸收了同行的一些观点，在此，向有关的作者表示诚挚的谢意。

本书介绍了当前网络犯罪的基本情况，探讨了网络警察组建的有关问题，阐明了控御网络犯罪的法律对策，论述了网络犯罪的侦查途径、措施、方法，同时对控御网络犯罪的技术手段与措施进行了深入的研究。本书既是网络犯罪研究者较好的参考书，又是目前已涉足网络及未来将涉足网络的个人、企业、事业、政府等预防自身的利益遭受侵犯及防范自身侵犯他人利益的好教材。

本书分工情况如下：

李双其　第一章　第四章　第七章　附录

郑　荔　第二章　第六章

曹文安　第三章

黄云峰　第五章

由于水平所限，书中缺点错误在所难免，尚祈读者批评指正。

编　者

2001 年 6 月

试读结束：需要全本请在线购买：　www.ertongbook.com

目录

·第一章·

认识网络犯罪

一、网络与网络犯罪

本书提到的网络是计算机技术与通信技术发展的融合物。网络虽然由各种各样的物理设备构成，但这些物理设备本身并非网络。网络是由这些物理设备按照某种特定的方式互联而形成的一个信息空间，这是一个“虚拟世界”，里面充满了以脉冲信号形式存在的“比特”，我们可以从中得到各种各样的信息和资料。

在人类生存的空间里，存在着各种各样的网络。本书谈及的网络主要是指因特网，同时也触及其他的一些专用网络。

因特网是由分布于全世界的无数个大小不一的路由器连接起来的。最初，因特网仅用在美国致力于防御研究的院校和机构的少数工作人员，主要用于文书传送。而随着因特网内容的不断丰富和功能的不断增多使它的用途变得越来越广泛。而因其广泛的用途和许多有趣且有价值的方面，因特网便吸引了众多、各种各样的用户。个人、家庭、企事业、政府、军队、各种社会团体等纷纷入网。在网络这个虚拟空间里，人口急剧增多，充斥着从事

各种行当，来自于各个阶层的人，一个虚拟的社会也因此而生。计算机网络化的最大特质，是创造了一个虚拟社会，创造了新型的社会交流方式与崭新的人与人的关系。这种新的社会交流方式的滥用、新的人与人的关系的冲突，就形成了一种严重危害社会的应受制裁的行为犯罪。

在网络空间里进行的犯罪总是与信息紧密联系在一起。信息滥用和误用是网络犯罪的最基本形式，信息性是网络犯罪的最基本特征。一方面，网络犯罪必须依赖于信息才能实现。犯罪分子要想实施网络犯罪活动，必须进入到网络空间中去，即借助于特定的物理设备如计算机、调制解调器等与网络连接。许多人认为计算机、调制解调器等物理设备是犯罪分子进行网络犯罪活动的工具，这种认识实际上是不全面的。物理设备固然是实施网络犯罪必不可少的物质基础，但真正决定起作用的并不是这些物理设备，而是利用它们发送或接收的各种信息，诸如用户名称口令、程序等，物理设备不过是各种信息的载体而已。不论物理设备如何先进，如果没有必要的信息资源，犯罪分子要实施网络犯罪是根本不可能的。另一方面，网络犯罪侵害的对象也是信息。网络犯罪的形态多种多样，网络犯罪分子的目的也各不相同的，有的是为了获得某些有价值的信息，也有的是为了骗取钱财，但直接的受害对象都是信息。

在网络空间中，信息已不再仅仅是信息，而是网络中的一切。网络所能容纳的只有信息，网络中的所有东西都是信息，犯罪分子从网络空间中得到的或损害的都只能是信息。

根据上述分析，在此，我们试图对网络犯罪的概念进行界定。

网络犯罪是指行为人利用网络专门知识，以计算机为工具对存在于网络空间里的信息进行侵犯的严重危害社会的行为。进行

试读结束：需要全本请在线购买： www.ertongbook.com

网络犯罪的行为人必须利用网络专门知识并使用计算机作为作案工具（这里提到的计算机指的是广义上的计算机，当用手机、信息家电上网时，手机、信息家电就成了计算机），行为人不论实施何种网络犯罪行为，其侵犯的只能是信息。而且，这种信息仅限于存在于网络空间里的信息，它可能是存储于系统中的，也可能是正在被传送的。在此，我们排斥单机行为于研究对象之外，而以建立在局域网、广域网、互联网上的网络行为作为研究对象；这里指的犯罪为犯罪学上的概念，不以刑事法典规定的犯罪为限。以一定的社会危害性和应受惩罚性为充分条件，刑事违法性为非必要条件。

二、网络犯罪的现状与特点

如前所述，随着因特网功能的增多和其价值的增大，“涌进”因特网的人是越来越多。美国至2000年止，上网的PC用户已达近亿人；而韩国同期上网的达到2000万。中国的网络事业也发展得十分迅速。据CNNIC 2001年1月17日发布的最新《中国互联网络发展状况统计报告》显示：截止到2000年12月31日止，我国内地上网计算机数有约892万台，其中专线上网计算机141万台，拨号上网计算机751万台。我国上网用户人数约2250万人，其中专线上网的用户人数约为364万，拨号上网的用户人数约为1543万，同时使用专线与拨号的用户人数为343万，除计算机外同时使用其它设备（移动终端、信息家电等）上网的用户人数为92万。CN下注册的域名总数为122099个，WWW站点数（包括.CN、.COM、.NET、.ORG下的网站）约265405个，我国国际线路的总容量为2799M。而1999年底我国内地上网计算机数只有350万台，上网用户人数只有890万。因特网使用人群在

中国每年增长比例都超过100%。按照《数字化生存》的作者尼葛洛庞帝的推测,2000年以后,全球使用因特网的人数将以更加惊人的速度发展,预计至2005年全球因特网用户将达7.65亿。

在这个十分庞大而且将变得更加庞大的虚拟空间里,存在着各种反社会的力量,这股力量随时准备实施侵犯存在于虚拟空间的信息的行为。这股力量来自不同的角落,怀着不同的动机,出于不同的目的,采用各种手法,在不同的时间方位挖空心思、十分疯狂地对虚拟空间里的信息进行侵犯。正如国外有位犯罪学家所言,比起现实世界,人们似乎更倾向于在网上犯罪。

网络犯罪带来了极坏的社会影响和破坏作用,它直接危害国家的政治、经济、文化等各个方面的正常秩序。根据美国联邦调查局1999年对《财富》杂志500大企业所做的调查,高达62%的企业网络曾遭非法侵入。美国联邦调查局局长路易斯·弗里奇更是表示,网络犯罪对美国国家及经济安全造成了严重威胁,最近几年的网络犯罪案件正以令人惊异的速度增长着。这其中很多是来自青少年的简单的黑客攻击案件,另外则是一些对雇主不满的员工发动的网络攻击和一些复杂的黑客攻击。弗里奇认为,虽然政府和企业现在已经显著地提高了对付网络入侵的能力,但这个问题依然越来越严重,一些为寻求刺激和经济好处而攻击网络的黑客、病毒制造者以及有组织的犯罪集团和恐怖组织使互联网时代的国家及经济安全受到了前所未有的威胁。

我国学者与官员持同样的看法。《计算机犯罪的定罪与量刑》的作者在该书序部分里指出:“网络犯罪是信息时代的产物。无论是国外还是国内,在信息技术突飞猛进,信息产业蓬勃发展的同时,网络空间的计算机犯罪案件每年都以几倍甚至十几倍的速度增长,其所造成的损害远远大于现实空间的犯罪……”信息产业部部长吴基传在为《国家信息安全报告》作序时指出:“计算

机互联网络涉及社会经济生活各个领域，并直接与世界相联，可以说是国家的一个政治关口，一条经济命脉。”对网络犯罪的控御直接关系到社会的安定，经济的发展，国家的安全。

故此，以计算机及网络的滥用为基本手段和特征的网络犯罪已经成为网络时代里严重的社会问题之一，在全球范围内受到各国际组织、各国政府和有关当局、各种商业和非商业机构的高度重视，如何防范网络犯罪不但是各国立法机关、司法机关及行政机关迫切要解决的问题，而且也是计算机技术领域、法学及犯罪学研究领域中最引人关注的课题。

这种在虚拟空间里实施的犯罪与在物理空间里实施的犯罪比较有如下一些特点：

（一）主体的年轻化

据统计，网络犯罪分子的平均年龄约为24岁。在网络犯罪中，特别是黑客中，青少年的比例相当大。网络犯罪主体的年轻化与使用电子计算机者特别是上网者年轻人占较大的比例及年轻人对网络的情有独钟和特有的心态有很大的关系。据CNNIC 2001年1月17日发布的最新《中国互联网络发展状况统计报告》：56%的用户年龄在24岁以下，学生为网络的主要使用者之一，约占20%以上。未婚人士仍占大多数，约为总数的2/3。这些年轻人虽然一般没有成年人网络犯罪的商业动机或者政治目的，但是同侵入国家事务、国防建设、尖端科学技术领域的计算机系统所造成的社会危害一样严重。

（二）具有跨国性

网络发展形成了一个虚拟的空间，在这个空间里，既消除了国境线，也打破了社会和阶级的界限，真正实现了“天涯若比邻”，使得双向性、多向性交流传播成为可能。在全球化的计算机网络上，信息传递的速度是以毫秒计时的，你从中国向美国传

递一条信息花时不过600毫秒，即使向地球上最远的一个点传送，也不过花时1秒之内。这就意味着，在网络空间里，国内与国外、近与远的概念已变得十分模糊，跨国成为一种十分平常的网络犯罪形式。

（三）专业化程度高

网络犯罪是一种高技术的智能犯罪，犯罪分子主要是一些掌握计算机技术的专业研究人员或对计算机有特殊兴趣并掌握网络技术的人员，他们大多具有较高的智力水平，既熟悉计算机及网络的功能与特性，又洞悉计算机及网络的缺陷与漏洞。只有他们能够借助本身技术优势对系统网络发动攻击，对网络信息进行侵犯，并达到预期的目的。

（四）犯罪成本低

网络犯罪成本是指行为人因实施网络犯罪行为所承受的精神性、物质性代价。成本由直接成本（包括心理成本和经济成本）和间接成本（包含法律成本和竞争成本）组成。网络犯罪的直接成本和间接成本都比传统犯罪要低。就直接成本而言，网络犯罪的心理成本不高。网络犯罪者实施犯罪行为常常是在极短的时间内完成的，作案时间的短促性使罪犯在作案时自我谴责和“现潮心理恐惧感”大大降低，同时由于“网络犯罪伦理”的作用，相当多的网络犯罪者在实施犯罪行为时并没有认识到自己实施的是一种危害社会的行为，这样，使它们的犯罪心理成本几乎等于零。网络犯罪与传统犯罪相比所冒的风险小而获益大，作案者只要轻轻按几下键盘，就可以使被害对象遭受巨大损失，而使罪犯获得巨大利益或对计算机系统入侵的刺激和挑战给他的心理带来极大的满足。所以，网络犯罪经济成本极低。就间接成本而言，因网络犯罪的发现率低，各国对付网络犯罪的立法参差不齐，网络立法的滞后及打击不力等原因，使网络犯罪的间接成本低下，

有时甚至等于零。

（五）隐蔽性强

网络犯罪的实施主要是犯罪主体通过程序和数据等各种无形信息的操作来进行。犯罪分子可以从任何一个计算机网络终端实施犯罪行为，且不受时间的限制。犯罪行为实施终了后对机器硬件的信息载体可以不造成任何损坏，甚至不留下任何痕迹，所以，犯罪行为不易被发现、识别和侦破，犯罪隐蔽性极高。

（六）取证困难

“网络空间没有指纹”，因为网络犯罪本身经常是虚拟的，它的行为对象是计算机数据和程序，它们存储在电磁介质上。磁介质上的数据必须经特定算法转换后才能以人眼可见的形式表现出来，更因存入计算机的数据以数字或代号形成的匿名性，增加了取证的难度。同时，因数据高密度存储，体积小，携带方便，且可以不为人觉察地拷贝，故不易被发现。更何况，现场的计算机系统内所存储的有关证据方面的数据很容易被破坏。再加上受害者不愿报案及行为时与结果时的分离性，行为地与结果发生地的分离性等，使网络犯罪的取证工作十分困难。

（七）具有连续性

网络犯罪具有连续性是由网络犯罪具有很强的隐蔽性、网络犯罪具有低成本及网络犯罪主体的特点决定的。网络犯罪常常难以被发现，风险较小，所以，行为人第一次犯罪得逞后，很少立即会被 发现，其犯罪心理就会得到强化，使其犯罪欲不断升级而继续实施犯罪。另外，由于网络犯罪的主体多数是技术人员，他们在社会上代表着高科技和智慧，加上网络犯罪一般没有惨状，社会危害性不直观，行为人实施犯罪后大多没有罪恶感，犯罪目的的实现，不仅给犯罪分子带来物质利益，同时也能满足其智力上的优越感。

（八）犯罪黑数高

犯罪黑数是指所有不在犯罪统计上出现的犯罪数值，也就是未为公众所周知，或未受司法机关追究的犯罪数。据美国学者唐·派克估计，计算机犯罪的黑数约为85%，而德国有学者估计计算机犯罪的黑数约为80%。美国CSI和FBI近几年来的调查结果表明，已发生的计算机犯罪案件中，只有约17%到达侦查机关手中，即计算机犯罪的黑数约83%。这就是说，实际发生的100件计算机犯罪中，约有83件未被发现或未受到法律制裁。至于单纯网络犯罪的黑数目前尚无一个较权威的统计数据，据估计，单纯网络犯罪的黑数比计算机犯罪的黑数还要高。网络犯罪黑数高，其原因主要有以下几个方面：一是由于网络犯罪极强的隐蔽性特点使网络犯罪很难被发现。二是网络犯罪被害人为了自身的信誉和保守秘密，或是由于反复受到侵害而钝化，或是对公力和自力救济有效性的质疑，或是出于其他动机不愿举报。

（九）具有严重的社会危害性

随着网络信息技术的不断发展，不但人们的工作生活与网络连在了一起，而且一个国家的电力、银行、电话系统乃至国防和国家的安全都与网络息息相关。网络犯罪造成的经济损失，网络犯罪对社会管理秩序和国家安全造成的危害都是其他类型犯罪无法比拟的。我们仅以黑客攻击为例来说明网络犯罪对经济的影响。当今世界上，平均每20秒钟就有一起黑客事件发生，仅在美国每年造成的经济损失就超过100亿美元。2000年2月eBay、E－Trade、Amazon等电子商务网站相继挂彩，其商务受到严重影响；YAHOO，全球第二大搜索引擎站点，注册用户一亿，平均日浏览页次4.85亿，也无可奈何地瘫痪了三个多小时。2月9日，全美因特网运行性能下降26.8%，三日内，受害公司损失超十亿。网络犯罪对社会管理秩序和国家安全造成的危害更是一

试读结束：需要全本请在线购买： www.ertongbook.com