河南省哲学社会科学
“十五”规划项目

项目类别	资助项目
资助项目号	2003CFX006

信息时代网络犯罪问题研究

项目负责人：魏 月 霞

项目参加人：姚 健 刘会霞 赵永柯 刘 强
张国琦 林黄鹂 姚天民 李伟强

项目完成单位：河南公安高等专科学校

项目协作单位：河南省公安厅

项目完成时间：二000年四月

目　　录

目　　录

信息时代网络犯罪问题研究

党的十六大在科学总结信息化对社会经济发展巨大作用的基础上提出：信息化是我国加快实现工业化和现代化的必然选择。目前，我国各地区、各部门基本上都建立了各自的信息网络系统。电子商务、电子政务、网络教育成为信息化浪潮中的热门话题。信息化的快速发展对提高本地区、本部门的工作效率、增强政府监管能力、开展公共服务发挥了积极的作用，但与此同时，网络信息安全问题成为关系到信息化健康发展、关系到国家经济安全、国防安全和社会稳定的大问题，信息化发展越快、水平越高，保障信息网络安全，惩治与防范利用信息网络进行违法犯罪活动的工作也就更重要。本课题在调查我国信息网络犯罪的基础上，探讨新形势下我国信息网络犯罪的原因、特点，尝试提出防范对策。

网络犯罪的概念、种类及特点

一、网络犯罪的概念

最初的观点认为，网络犯罪是基于网络的出现而产生的一种新型犯罪现象。在刑法学界，存在着网络犯罪是以网络为犯罪对象的犯罪，还是以网络为犯罪工具的犯罪之争。而实质上，网络犯罪并不是严格的刑法学上的概念。按照 97 刑法的规定，涉及计算机犯罪的共有三条五款。第 287 条规定的是利用计算机进行传统犯罪的内容，对于此类行为，97 刑法仍规定按传统罪名定罪量刑。因而实际用来惩治计算机犯罪的条款只有第 285 条第一款和 286 条三款，即非法侵入、破坏计算机信息系统的应受处罚的行为。这一范围显然太窄，与当前涉及计算机信息系统的形式多样的违法犯罪的实际情况不相适应，并且由于网络技术的发展，仅仅涉及单机的计算机犯罪已不多见，计算机网络犯罪已成为主流，因此我们试图从犯罪学角度界定网络犯罪，探讨有关网络犯罪的问题。本课题所研究的网络犯罪是指：以信息网络服务为目标或以信息网络为实施犯罪工具的犯罪行为。

二、网络犯罪的种类

既然网络犯罪是指以信息网络为实施犯罪工具或以信息网络服务为目标的犯罪行为，网络犯罪的种类也就包括两大类型：一类是以信息服务为目标实施的犯罪，一类是利用信息网络技术实施的犯罪。

（一）以信息网络服务为目标实施的犯罪种类

1、非法侵入计算机信息系统。国际互联网是个开放的信息系统，只要具备相应的软、硬资源便可登录上网。因此对国际互联网络而言并不存在侵入问题。但由于整个网络体系当中的部分站点的特殊功能和用途涉及到专业情报和信息的保密，它们是不能被轻易进入的。因此对这些网络站点的非法登录便是侵入行为。在我国被侵入的通常是行业区域网和某些企业局域网。但由于我国刑法第285条规定了非法侵入计算机信息系统罪，是指违反国家规定，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行为。对于侵入的对象做出了严格的限制，因此真正构成非法侵入计算机信息系统罪的案件并不多。

2、破坏计算机信息系统。破坏计算机信息系统罪是指利用各种手段，通过对计算机信息系统功能既存储、传输的数据和应用程序进行删除、修改、增加、干扰的操作或故意作制并传播计算机病毒等破坏性程序，从而导致计算机信息系统的被破坏的行为。其表现形式主要为：袭击网站；在线传播计算机病毒等。

袭击网站，指秘密的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”，袭击目标网站，使其因无法存取而致全面瘫痪的犯罪行为。例如：２００３年１２月１日早上，“新疆黄页网”的工作人员发现页面不能正常打开，并且数据库报错，页面提示为联接脚本错误。工作人员通过网络程序检查，发现网站近１３０Ｍ的数据被清除，仅有３Ｍ数据剩余。新疆企业的商务平台“新疆黄页网”，是目前全疆最大的企业、事业单位网络数字化信息的专业网站。“新疆黄页网”除传统模式的单一黄页外（查找电话号码），里面还罗列了各个企业的企业简介与业务范围等等，极大地突出了其实用性强的特点。其遭受突然袭击，影响极大。国家计算机网络应急技术处理协调中心接到了“新疆黄页网”工作人员的报告后，迅速做出反应，仅用３０分钟就恢复了网站的所有数据。同时该中心监视所有访问过“新疆黄页网”的ＩＰ地址。１２月１日到３日期间，国家计算机网络应急技术处理协调中心的人员，帮助“新疆黄页网”完成了所有的漏洞修复工作，使网络的安全系统恢复了正常使用。又如计算机专业的大学生张某为筹学费竟“侵入”到济宁一所高校的教学平台，并将大量资料删除，致使该教学平台一度瘫痪，后又实施敲诈。此案经济宁市中区检察院起诉后，2004年2月18日，济宁市中区法院一审以破坏计算机系统罪和敲诈勒索罪判处张某

有期徒刑2年缓刑3年。[1]

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。其中最为典型的是制造并传播计算机病毒行为。

计算机病毒是一种人工编成的破坏性很大的计算机程序，往往具有很强的自我复制能力，一旦感染，轻则扰乱屏幕上的信息，重则破坏计算机的一切数据资料。例如，1999年肆虐全球的病毒“美丽莎”和CIH.据有关部门估计，除中国外，全球共约有6000万台电脑受到CIH病毒的影响，受害的电脑用户分布于亚洲、欧美和中东等地区的国家，连美国、日本等电脑先进的国家也未能幸免。而中国，虽然媒体已经提醒包括中国在内的广大计算机用户要提防1999年4月26日的CIH病毒，但CIH依然如期在中国登场，仅这一天，至少造成数十家政府机关、企事业单位、个人用户，甚至一些著名的高科技企业、银行等的计算机系统死机、电脑硬盘遭毁，损失惨重。1997年，江苏省公安机关查处的一起传播计算机病毒案件，该案件被及时侦破，病毒很快被发现并被控制；但丹阳市供电局一台储存1989年以来该市电力负荷的统计资料和某电厂的工资、人事管理应用软件因受感染而遭到破坏；该市某局两台电脑因感染病毒致使一套业务管理系统软件遭到破坏。

（二）利用信息网络技术实施的犯罪种类：

1、利用信息网络实施金融诈骗罪。如：伪造、空存存款数额，诈骗银行或储户资金；在电子商务交易中实施空头支付或截取电子钱款。盗卖他人股票或操纵股票交易，侵占证券交易所或股民资金。主要表现为：

（1）网上诈骗行为

2002年美国联邦调查局逮捕了一位名叫马克•雅各布的男子。据报道，雅各布供职于一家网站，他于星期五在这家网站上发布一条消息说，生产网络设备的伊姆莱克斯公司总裁已经辞职，该公司以前还曾经作过假帐虚报了它的赢利数额。许多网站纷纷转载了这条消息，结果导致伊姆莱克斯公司的股票狂跌60%，该公司的市值一下子减少了25亿美元。[2]

网上诈骗方法不同，形势各异：

商业多层传销：在电子邮件中宣称，不必花太多时间和金钱，就能获得优厚

---

[1] 参见乌鲁木齐信息港 http://it.xjsohu.com/show.asp?ArticleID=1665.2003-12-17。

[2] 参见新快报>>国际新闻,2000年9月2日星期六。

报酬，以此进行非法的多层次传销。

出售电子邮件：出售数以百万计的电子邮件地址名单，或者提供收信人的代理服务器号码。这是违反当地网络服务商规定的，有的地址是失效或错误的。

连锁电子邮件：以“幸运邮件”为名，在信中要求收信人寄出小额金钱给邮件名单里的人，然后等着其他人寄钱给你，否则就会惨遭不幸。而事实上，收别人钱的可能性几乎为零！

高价回收骗局：利用登启示要求应征者花巨资买回原材料，进行加工生产，他们负责回收；但同时又以“质量未达标准”为由拒绝回收，使许多人损失惨重。

瘦身减肥骗局：在网络中“名医”侃侃而谈，声称有秘方可以让消费者减肥，结果网民花钱又伤身。

免费赠品的诱惑：“恭喜你中大奖，可以免费获得电脑、手机等高价商品”，但总是通知你先支付一笔不菲的“邮资”。结果是付钱后，奖品就遥遥无期了。

信用卡信用不保：在电子邮件中保证能免担保获得信用卡，但消费者提供个人资料后，可能会因“信用”被冒用而背负巨债。

（2）网络金融犯罪行为

网络金融犯罪行为是指以非法占有为目的，利用互联网攻击金融系统窃取公私钱财的行为。包括利用信息网络实施网上窃密，如利用远距离望远镜窥视信用卡、证等盗窃犯罪；利用信息网络修改各类账目，贪污、挪用公款等实施贪污、挪用公款罪等。

1998 年 10 月 13 日，江苏警方侦破我国首例计算机侵入银行计算机网络，盗窃 26 万元巨款案。1998 年 9 月 22 日下午 4 时 30 分左右，扬州某工商银行储蓄所会计像往常一样，通过电脑进行当日进出账目预结帐，结果电脑显示存储结果大大超出流水账单，经工商银行扬州分行电脑中心核查，在当日中午 12 时 32 分 34 秒至 42 分 54 秒的 10 分零 20 秒的时间里，该储蓄所被人用计算机输入虚假存款信息 16 次，总计 72 万元。然后，从当日中午 12 时 50 分至 16 时 6 分，全市工商行系统的 9 个储蓄所被人用假存折连续取款 30 万元。据公安部权威人士介绍，类似该案件的案件，全国已发生多起。

伴随当前金融电子化的进程而出现的计算机网络盗窃和贪污银行资金的犯罪活动日益猖獗，银行、证券等金融部门的计算机犯罪占整个计算机犯罪的 61%。

大部分作案人员是金融部门内部接触计算机的人员，犯罪嫌疑人的文化程度较高。全国首例利用互联网非法集资诈骗案即东方神龙数码卡非法集资诈骗案，涉及20多万网民，诈骗金额高达2.3亿多元。作案人林杰雄是广东省阳江市人，在认识他的同伙之前，林杰雄在郑州从事“阳江刀具”批发生意。2000年12月，林与4名河南人合谋组建郑州神龙数码网站(“广州东方神龙数码科技有限公司”前身)，并于2001年1月在郑州市顺河路27号天弘大厦602房建立网站办公室，同时起草了建立网站的方案、设计了神龙卡，一伙人很快在互联网上设立了神龙数码网(SHENLONGSHUMA.COM)和神龙互联网(SHENLONGNET.COM)等4个网址。他们对外宣称：网民购买“神龙卡”后方可登陆这4个网站，进入网站后每点击网站的广告一次就可获利0.3元，但每张卡每天只限点击广告33次，一张卡的有效期为3个月，每10天兑现一次点击费。3个月网民可获点击费891元，扣除380元购卡费，可获纯利511元。网民获利由神龙公司从被点击企业所付广告费中支出。到了5月底，该网站没有继续付给网民广告费，各地网民因此向公安、工商部门报案。广东警方于7月5日彻底清查了神龙数码网的开办者——东方神龙科技有限公司。据查，犯罪嫌疑人通过代销商共售80多万张，总金额达2.3亿多元。[①]

2、利用信息网络实施侵权行为，例如网上侵犯姓名权、名誉权和个人隐私权等等

利用网络侵犯他人姓名权、名誉权和个人隐私权是指在互联网上对其他人的姓名、名誉进行攻击、诋毁，或公开他人的隐私的行为。

由于互联网没有审查机构，人们在网上活动可以随心所欲，想说什么就说什么，没有任何人去阻拦，也不可能加以阻止。他们的言论通过网络可以传到世界各地。因而，既有可能造成涉及人身权利的民事纠纷，又有可能引起涉及财产权利的民事纠纷。例如，1994年，澳大利亚一法院判决了一起利用网络进行诽谤的案件：西澳大利亚大学考古系讲师Kindos指控一用户利用网络的新闻组发表贬低他学术能力的言论。结果法院判决Kindos胜诉，责令被告赔付4万澳元的损害赔偿。1996年，我国北京大学发生了一起利用互联网侵害姓名权的民事案件。北京大学93级研究生薛某状告同寝室同学张某用电子邮件冒名拒绝美国密

[①] 新华网 http://www.sina.com.cn 2001年08月24日16:45。

执安大学教育学院为原告赴该大学攻读博士学位提供的1.8万美元奖学金，侵害了她的姓名权。1999年2月5日，《北京青年报》刊载了一篇文章，叙述了美国姑娘兰迪遭网络性侵犯的经过。1999年11月，警方逮捕了冒充兰迪的犯罪分子加里•德拉蓬特。其犯罪经过非常简单：加里冒充自己是兰迪，然后借免费电子邮件四处做广告，最后再向有反应的人发送电子邮件。据《南方日报》2000年10月6日报道，一名休假在家的市民阿江（化名）受到全国各地打来的黄色电话骚扰，而导致她被骚扰的原因是有人恶意冒充阿江的名字，在网上的成人聊天室里大谈其心情寂寞空虚，并公布了她的电话。2000年初，台湾“高等法院”审理了一起学生在网络上诽谤教授的案件。结果该学生一审被判拘役55天。这是台湾首宗因网络诽谤而被判刑的案件。[①]

3、利用信息网络进行电子色情服务。

利用网络进行电子色情服务的行为是指在互联网上进行生产和传播色情资料的行为。色情总是在不遗余力地追赶着现代通信的快车。互联网是最新兴起的通信方式之一，寄生其上的色情网站正以每日万计的速度发展着。例如sex.com被认为是全球域名中最有升值潜力的网络名称之一，该网址每天浏览的人次超过2500万人次。

2000年，在纽约发生一起重大的网上恋童犯罪案件，一个名为罗伯特的37岁男子，在网上引诱少女外出与他发生性关系，奸污了12名未成年少女，并将其中一名12岁的女童奸污后杀害，罪犯被捕后对所犯罪行供认不讳。[②]

1999年9月,河南省郑州市何肃黄、杨柯，在商丘信息港上建立了一个个人主页，用五十多天的时间建立的网站上存了一万多幅淫秽照片、100多部色情小说和小电影。不到54天的时间，访问量达到30万次。

美国卡内基•梅隆大学曾对国际互联网中的色情服务做了一次较为详细的跟踪调查，统计出网上共有儿童色情图像450620个。在短短半年时间内，仅美国就有6432297人次浏览。[③]2001年台湾破获一家庞大的色情网站，它的主要成员是在台北市某技术学院上学的一年级学生周某。他们利用针孔摄像机专门在公共场所偷拍女子裙底风光、女子入浴、入厕情形，还拍有女子护肤的裸体镜头，并

[①] 参见蒋平：《计算机犯罪问题研究》，商务印书馆，2000年版，第74—75页。

[②] 参见李玉华：《网络世界与精神家园》，西安交通大学出版社，2002年版，第165页。

[③] 参见《焦点》深圳商报社主办，1999/2/23。

把偷拍下来的影片放置到色情网站上。

4、利用信息网络刺探、盗窃秘密行为

利用信息网络刺探、盗窃秘密行为是指在互联网上窃取他人重要信息的行为。网络窃秘行为主要有：盗窃商业机密、技术机密、国家机密、个人隐私等。

2000年2月24日，江苏省工商银行何某来到南京市公安局梅园派出所报案，称其于去年7月在南京电信局办理了互联网上网手续，由于密码原因一直未上网操作，但近日发现电信局给他的帐单上竟有5900元的上网费。警方经过侦查证实，先后共有14人盗用了何某的账号和密码“免费”上网。2000年4月，《电脑报》报道，上海警方日前抓获2名侵入一家证券公司电脑系统偷盗该公司上万名股民的地址、资金额度、证券种类、帐号和买卖记录信息的黑客。19岁的涉案人章某及其同学田某被刑事拘留。最令人震惊的当属英国1994年11月破获的一起重大的计算机网络泄密事件。这位“骑士”是英国电信公司一位短期合同计算机操作员，他借助其他公司职员为其提供的密码“闯入”公司内部数据库，获得英国政府防务机构和反间谍机构，包括英国情报机构军情五处、军情六处的地下掩体、英国导弹基地和军事指挥控制中心的电话号码，甚至还有当时首相梅杰的住址和在白金汉宫的私人电话号码。

5、网络恐怖行为

网络恐怖行为是指通过互联网而使对方受到恐怖威胁与侵害的行为。一些国际恐怖组织、邪教组织和种族主义分子，利用互联网络进行国际恐怖活动，肆意散播他们的反动言论等。1994年，互联网上出现了恐怖分子为谋杀美国好莱坞女影星朱迪•福斯特征集杀手的电子广告。2002年7月，美联邦调查局负责打击网络恐怖主义的负责人迪克说，美国能源公司计算机系统过去半年来共遭受18万次攻击，远远超过了其它行业遭受的网络攻击，有迹象表明，恐怖分子已将美国能源系统当作其发动网络恐怖袭击的首要目标。总部设在弗吉尼亚州的私营计算机安全公司在其发表的半年一度的网络安全报告中说，这家公司的20家大型能源客户的计算机系统在2002年上半年以来遭受的网络攻击比去年同期增加了77%，其中14家所遭受的攻击是致命的，如果没有得到及时修复，公司计算机系统将处于瘫痪。石油、水和电力输送涉及国家的经济命脉，如果这些系统计

算机网络瘫痪，将导致灾难性后果。[1]

6、网上组织邪教组织

这类案件目前比较多，如创立法轮功邪教组织的李洪志就充分利用互联网的便利，在全球建立了几十个网站，蒙骗群众，通过互联网大肆传播经文，发表各式各样的“最新指示”，操纵遥控国内“法轮功”骨干分子继续开展反社会、反科学、反人类的破坏活动。

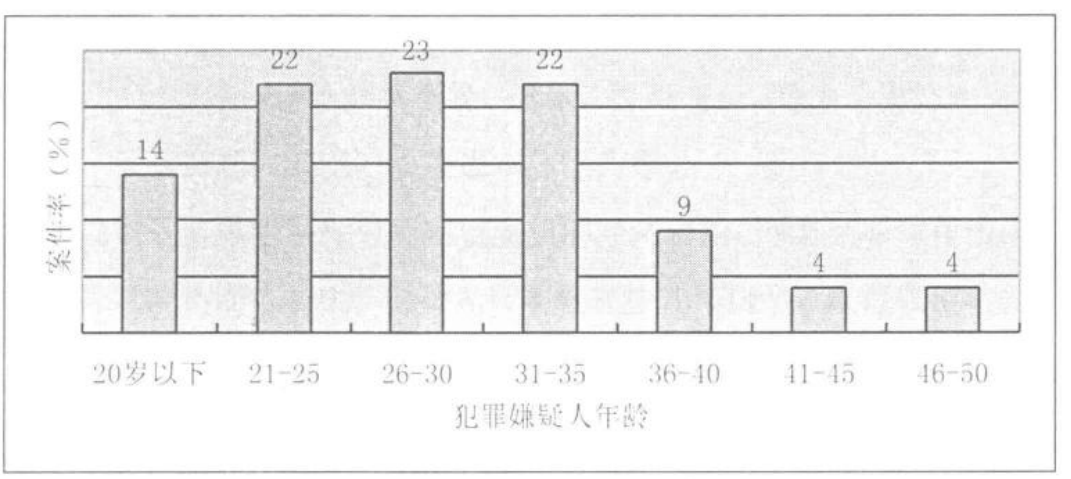
四、网络犯罪的特点

（一）犯罪主体具有高智能、高学历、低龄化、内部人员多的特点

现代网络系统都比较注重网络安全问题，都为网络提供了一些安全防范措施。要破解安全系统和侵入计算机系统，行为人必须具有较高的专业水平。因此，网络犯罪者主要是一些掌握了电脑技术，特别是网络技术的专业人员。他们洞悉网络的缺陷和漏洞，运用丰富的电脑及网络技术，借助四通八达的网络对网络系统及各种电子数据资料等信息发动攻击，进行破坏。如：现已开始出现具有推理技能，能够自动进行目标搜索，并可改变自身形态，具有自行修复能力的智能型计算机病毒，可对抗一般的反病毒措施。

据中国互联网信息中心（CNNIC）2000 年 7 月统计结果显示，我国上网人数 1998 年为 117.5 万人，2000 年 7 月则达到 1690 万人，用户年龄 18－24 岁站 46.77%，具有本科学历的占 46%，大专学历为 46%，硕士及以上学历 6%。[2]

从美国 20 世纪 80 年代前的网络犯罪嫌疑人的年龄情况看，81%的犯罪嫌疑人年龄在 35 岁以下，见下图：[3]



[1] 参见新华网洛杉矶 2002 年 7 月 8 日。

[2] 中国互联网信息中心 http://www.cnnic.net.cn，2000 年 7 月。

[3] 参见李玉华：《网络世界精神家园》，西安交通大学出版社，2002 年 1 月，第 198 页。

（二）侵犯客体多样化

网络犯罪侵犯客体多样化是指网络侵犯的客体既有国家安全、社会秩序、经济秩序，也有财产所有权、人身权利、民主权利等。

1994 年，美国国防部五角大楼网站被黑客侵犯，黑客窃取了美军作战模拟计划、美军空军作战计划等机密军事档案，并企图侵入朝鲜半岛某处核设施的电脑主机，差点引发了第三次世界大战。

1999 年 4 月 20 日，郑州交通银行发生的挤兑案则是犯罪嫌疑人在郑州商都信息港 BBS 上信口雌黄，随心所欲地发表自己的观感所直接引发的。

2001 年 3 月 20 日，美国纽约警方向媒体披露了一起让超级富翁们都心惊胆战的网络诈骗案内情。一名餐厅打杂的男子只是利用当地图书馆里的几部电脑，便成功地制造了一起互联网出现以来的数额最大的身份诈骗大案：跻身《福布斯》评选的“美国富人排行榜”前 200 名的富人，成为其首当其冲的目标。

（三）网络犯罪成本低

网络犯罪成本是指行为人因利用网络资源作为攻击工具与对象而实施的严重危害社会的行为所承受的精神性、物质性代价。其中包括心理成本、经济成本和法律成本。

心理成本是行为人实施犯罪行为时对于受社会道德谴责和可能受法律惩罚的恐惧所导致的心理压力。网络犯罪策划时间较长，犯罪人需要经过一段时间才能完成对密码的破译工作。但是，一旦犯罪人开始实施犯罪，其犯罪往往是通过一系列犯罪指令来完成，所需时间只有几秒甚至是几微秒，这种犯罪时间的短促性使犯罪人在作案时自我谴责和现场恐惧的心理大大降低。特别是一些犯罪人错误地认为，自己非法入侵计算机系统、破坏计算机安全，是为了更好地完善系统，非但无罪，反而有功，其犯罪心理成本几乎为零。

经济成本是实施犯罪行为所需要支付的经济费用。网络犯罪与传统手段的犯罪相比所冒风险小而收益大，犯罪人只需轻轻按几下键盘，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。

法律成本是指计算机网络犯罪行为可能被司法机关或其他具有同等功能的机关抓获的概率大小，具有惩罚性和不确定性。如果犯罪行为没有被发现，则该

成本为零；反之，则有一个法定惩罚成本。而网络犯罪不仅被发现的概率很低，而且由于犯罪的跨国性、跨区域性以及法律在惩罚网络犯罪方面的艰难性，致使网络犯罪的法律成本较低。据有关部门统计，在号称“网络王国”的美国，计算机网络犯罪的破案率还不到10%，其中定罪的则不到3%。据有关新闻报道，计算机犯罪只有11%被报道，其中仅1%的犯罪被侦查过，而高达85%以上的犯罪行为没有被发现。

根据美国联邦调查局的一项最新调查结果，大部分大型企业和政府机构都遭到过计算机黑客的攻击，但他们常常不向当局报告。调查发现，90%的被访者在2002年中发现了破坏计算机安全的行为，但只有34%的攻击向当局报告。许多被访者强调，他们担心计算机安全漏洞被揭露有可能破坏他们的公众形象。这次调查是由计算机安全研究所与FBI旧金山计算机犯罪小组联合实施的，该研究所主任Patrice Rapalus说：“实际发生的计算机领域内的犯罪或违规行为，远远多于企业向客户、股东及合作伙伴承认的数量或向司法当局报告的数量。” 38%的被访者说他们的网站在过去一年中曾被人入侵，有21%的人回答说不能确定，18%的人回答说有某些交易信息被窃，如信用卡号码或客户数据，或报告了金融欺诈行为。有 7%的单位报告说他们的网站被人在线涂改，这通常是最简单也是危害最轻的攻击行为。进行涂改的黑客用他们自己的文本或常常是带有攻击性的图片篡改网站的主页。[1]

在我国，遭受恶意攻击或病毒袭击的信息网络应用单位不在少数。但真正想到报警求助的却很少。我们曾做调查，2003年9月份的冲击波病毒，某市仅20家单位报警称受到袭击。大多数被病毒袭击的单位都按“惯例”，选择了沉默。如对一家建有内、外网的重点信息网络应用单位进行暗访发现，该单位在冲击波病毒来临时，病毒由外网感染到内网，可谓中毒至深。但却没引起该单位重视，也没有向网监通报情况。好不容易摆平冲击波后，该单位又被一种蠕虫病毒感染，由内网传到外网，结果网络全面崩溃。系统管理员不得不一台电脑一台电脑地杀毒、格式化。但该单位最终仍未将这一情况通报网监。沉默的主要原因也是害怕报警后，网络遭袭事件被公之于众，影响自身形象。

犯罪黑数的不断增加，致使网络犯罪的法律成本不断降低。同样，由于惩罚

[1] 参见(http://www.sina.com.cn 2002年04月08日 11:30 赛迪网)。

网络犯罪的法律还不够完善（后面专题论述），也使网络犯罪的成本较低。

（四）犯罪行为的跨国性和明显性

网络犯罪往往是作案地与犯罪结果地相分离，地区跨度大，甚至是跨国犯罪，使侦查取证难度较大。

随着网络的日趋大众化，网络技术犯罪在网络犯罪中呈现出相对下降的趋势，针对社会普通公众的网络滥用犯罪呈上升趋势。因此，犯罪行为表露，容易被发觉。

（五）犯罪手段的隐蔽性

在互联网构成的虚拟空间中，参与者的身份虚拟化，任何人都可以带着假面具将自己推上网。其犯罪的隐蔽性主要表现在：作案范围一般不受时间和地点限制，可以在任何时间、任何地点到某省、某市甚至某国作案；犯罪人对犯罪结果发生的时间可以随心所欲的控制；作案时间短，长则几分钟，短则几秒钟；犯罪不留痕迹，没有特定的表现场所和客观表现形态，不易识别，不易被人发现，不易侦破，犯罪黑数高。有人预算，抢劫犯采用传统方式抢劫银行，平均每次获得的赃款只有 3551 美元，而且抢劫者入狱的可能性高达 82%；而利用网络盗窃，平均每次可得赃款 25 万美元，被抓获的可能性只有 2%。犯罪手段的隐蔽性给网络管理和执法带来了巨大困难。

（六）犯罪危害的严重性

传统犯罪一般只局限于一时一地，针对的是特定的犯罪对象或者一定范围内的不特定多数。网络犯罪则可能造成全世界的网络受到破坏，甚至有可能连行为人自身都无法预计或控制其破坏的后果。网络上任何有意或无意的攻击，都可能造成网络上成千上万台计算机瘫痪。尤其是在网络空间中实施的涉及经济利益的犯罪，其非法获利或在客观上造成的损害通常较大。据美国学者估测，在国际互联网上实施的侵犯著作权犯罪每年可导致数百亿美元的损失。在网上黑客们只需坐在温暖的家中敲击几下键盘，就可以使全球的电子商务大厦在几秒钟内轰然倒塌。在我国，仅 2002、2003 两年，银行系统就发生计算机犯罪案件共 200 余起，平均每起涉案金额一百多万元，造成的经济损失巨大。

（七）犯罪本身的“虚幻”性

网络犯罪不同于传统的犯罪，网络犯罪披上了一层文雅的面纱，使得人们并

不将其视为一般的、真实的犯罪。网络犯罪通常不附加暴力，犯罪者大多文质彬彬，喝着咖啡，坐在计算机前敲打几下键盘就可以实施犯罪。网络犯罪一般不直接针对公众，使得其社会危害性一定程度上被屏蔽。网络犯罪的这一特征，极易导致人们特别是青少年判断上的偏差。很多青少年对网络犯罪投以崇敬的目光。对此，日本学者西田修有一段精彩的评论："不少人觉得，利用电子计算机实施犯罪是一种智慧的表现，它既不像躲在黑暗中突然猛击行人头部，乘其休克抢走钱财的强盗那样凶狠残暴，又不像欺骗贫穷的老人，将其仅有的一点点退休金洗劫一空那样伤天害理……对于不附加任何暴力、稳稳当当实施的计算机犯罪，不少人都怀着羡慕的心情不禁赞叹道：干得真漂亮！甚至可能有人会这样想：这计算机我拼命学会还搞不懂，可他竟能用来干'坏事'，这家伙肯定非等闲之辈！倘若我也有干这一手儿的本事……"[1]网络犯罪的温柔面纱蒙蔽了许多人的眼睛，人们不仅看不清网络犯罪及其严重的危害性，自觉地同网络犯罪作坚决斗争，反而对它报以"崇敬"的心理，甚至崇拜网络犯罪分子。

网络犯罪的手段

防范网络犯罪，必须对网络犯罪的作案手段有所了解，以便对症下药。我国常见的网络犯罪手段。

一、利用网络系统实施犯罪的常用手段

1、色拉米术

以微小不易察觉的方式侵占，最后达到犯罪目的的方法。最典型的犯罪案例是计算机程序员修改程序，截留银行储户四舍五入的利息尾数零头，积少成多。在中国的深圳、济南、上海都曾发生过这种犯罪，因为只有修改计算机程序才能达到其犯罪目的，故多为直接接触程序的工作人员所为。

2、冒名顶替

利用各种手段获取别人密码后进入系统，冒充合法用户进行犯罪活动。获取他人密码的方法很多，有的从旁窥视别人操作获取密码，有的从组合猜测获取密码，有的趁合法用户暂时离开机器进入系统，还有人利用管理混乱骗取密码。典型案例是在柜台外观察管理员手形猜测管理员密码，冒充部门经理骗取密码等。

3、越权浏览

---

[1] 李玉华：《网络世界精神家园》西安交通大学出版社，2002年1月，第79页。

利用合法的操作搜寻不允许访问的文件。浏览者有猎奇的爱好，对各种保护文件有一睹为快的感觉，掌握机密信息是诱发犯罪的因素。此种犯罪通常是能接触计算机信息者所为。

4、“窃听机密”

主要是利用信息网络系统的电磁泄漏获取信息或搭线截获信息的方法。两种方法都能准确的获得计算机信息，但由于多种信息混杂在一起或是密文信息，所以破解窃听信息，从中得到有用信息不是一般人轻易可以做到的，要专用设备或高技术支持，通常只有个别专门技术人员才能做到。

5、设置后门

程序开发者在编程中人为设置的进入系统的后门。虽然一些程序员设置后门的初衷可能不是为了犯罪，但该后门是引起犯罪的隐患。利用程序的后门从事违法犯罪活动，是和编程有关的人员或对程序非常了解的技术人员。

6、伪造文件

利用使用计算机伪造也是网络犯罪的一种形式。伪造证明、伪造合同、伪造信用卡等，计算机输出信息的规范、便捷，排除了人为痕迹，便于快捷、大量伪造各种计算机处理输出文本。

二、以信息网络系统为对象的犯罪常用手段

1、数据欺骗

非法篡改输入/输出数据获取个人利益，是最普通、最常见的网络犯罪活动。发生在金融系统的此种信息网络多为内外勾结，串谋作案。由内部人员修改数据篡改帐目，外部人员提取钱款。

2、逻辑炸弹

计算机程序中有意插入的，在特定时间或特定条件能激活起破坏作用的代码。由于破坏性代码和程序一体，所以是程序设计人员在编程中有意加入的内容。中国上海、四川、河南、北京先后多次发生技术人员在程序中放置“逻辑炸弹”危及计算机信息系统安全的事件。

3、清理垃圾

从计算机系统周围废弃物中获取信息的一种方法。由此带来损失的例子并不罕见，因此提醒计算机用户不要随便处理所谓的计算机信息系统废弃物，因为其

中可能含有不愿泄漏的信息资料。

4、木马攻击

也称“特洛伊木马术”，表示以软件程序为基础进行欺骗和破坏的方法。一些免费软件经常隐藏有一些不可告人的目的，轻者是恶作剧，重者毁坏系统，引起财产损失。由于特洛伊木马是施展诱人上当的欺骗术，程序的破坏作用较隐蔽，编制这一类程序需要丰富的编程经验，所以是程序设计人员所为。提高对来路不明软件的警惕性，是避免上当减少损失的最好办法。

5、制造病毒

计算机病毒是一种破坏性程序，是靠自我复制能力进行传播的，也是黑客攻击网络常用的方法之一。但病毒程序与特洛伊程序有明显的不同。特洛伊程序是静态的程序，被植入在一个被信任的程序之中。特洛伊程序会执行一些未经授权的功能，如把口令文件传递给攻击者，或给他提供一个后门。攻击者通过这个后门可以进入那台主机，并获得控制系统的权力。而计算机病毒是靠自身的复制能力将破坏性程序复制到其它计算机中。

网络犯罪产生的社会文化心理分析

随着社会的进步，科技的发展，网络以迅雷不及掩耳之势，渗透到人类生活的各个领域，影响着人们的生活方式、人际关系、思维方式、情绪表达等。而以计算机技术和通信技术的融合为物质基础，以发送和接收信息为核心的网络文化，作为一种环境因素，在发挥其独有的“示范作用”、“导向作用”、“创新作用”、“教育作用”等功能的同时，也为人类创造出了一种新的生存方式、活动方式和思维方式。但是，网络是一把双刃剑，网络文化在发挥其正面教育等功能的同时，也给人类带来了一些负面影响。

一、网络文化为犯罪心理的形成提供了重要氛围

（一）网络文化的无序性与人的个性的畸形发展

网络文化的无序发展，使其出现了一种无政府化的倾向。“文化的维持经验功能，使得特定文化及其包含的价值符合特定文化环境中人的需要和人的价值心理，而且随着日积月累，该文化的结构和排列顺序就会出现一种特定情形，形成该文化下的价值取向。”[2]但是，传统文化对个体发生作用往往要经过一些“关口”

[2] 参见魏月霞：《文化及其对人格的影响》，河南教育学院学报，1998年第1期，第78页。