计算机安全

王锡林　郭庆平　程胜利　编著

人民邮电出版社

计 算 机 安 全

王锡林 郭庆平 程胜利 编著

人 民 邮 电 出 版 社

登记证号(京)143号

内 容 提 要

本书详细论述了计算机管理及计算机系统方面的安全问题，提供了密码技术和素性检测的有关资料，分析了现存多种计算机病毒的定义、分类和机理，介绍了检测与清除计算机病毒的方法。本书融理论分析、实用技术、技术资料为一体。书中还介绍了一些最新科研成果。

本书适宜计算机应用开发人员、管理人员、操作人员阅读，也可作为大专院校计算机专业师生参考教材。

计算机安全

Jisuanji Anquan

王锡林 郭庆平 程胜利 编著

责任编辑 吕晓春

*

人民邮电出版社出版发行

北京市朝阳门内南竹杆胡同 141 号

北京朝阳隆昌印刷厂印刷

新华书店总店科技发行所经销

*

开本：787×1092 1/16 1995 年 1 月 第 一 版

印张：21 1995 年 1 月 北京第 1 次印刷

字数：528 千字 印数：1— 4 000 册

ISBN7-115-05382-0/TP・136

定价：21.00 元

序　言

在计算机应用日益广泛的今天，计算机的安全运行是当前信息社会极为关注的问题。计算机病毒蔓延之广、危害之大，已引起计算机安全学术、技术工作者及各有关部门领导的重视。

为了治理计算机病毒，维护计算机公共安全，湖北省在全国率先成立了省计算机安全学会，推动了近百个行业系统成立了计算机安全工作领导小组。心诚所至，无不支持，从而使全省各界都提高了计算机安全意识，壮大了安全工作者队伍，积累了一些经验，遏制了计算机病毒的恶性蔓延。

因为计算机安全工作除了防治病毒以外，还有许多涉及到其他方面的工作。例如信息系统是计算机应用的核心，也是外界侵入与危害的主要目标。它的安全与计算机实体、机房环境和社会环境密切相关，故有必要编写一本系统论述计算机安全的书籍，供所有从事计算机技术和管理的人员参考。王锡林同志曾主持编写了一本《计算机病毒与治理》内部资料，作为治理计算机病毒实际工作的参考书，满足了一部分计算机工作人员的需要，得到社会各界的欢迎和好评。1994 年 2 月 18 日国务院第 147 号令颁发了《中华人民共和国计算机信息系统安全保护条例》。计算机信息系统的安全问题更进一步引起全国各地有关部门的重视。为了更好地贯彻这一条例，湖北省公安厅、中国计算机学会计算机安全专业委员会湖北组、湖北省暨武汉市计算机学会安全专业委员会，组织有关专家学者，在《计算机病毒与治理》的基础上，增加了大量新内容，编写了《计算机安全》一书。书中介绍了许多目前最新的安全技术和科研成果。这本书视野开阔，既着眼于计算机整个安全体系，又突出了计算机安全的工程应用；既有理论分析，又切合实际；对提高读者技术水平，解决计算机安全实际问题，会很有帮助。

希望这本书的出版，能在促进计算机安全学的研究发展中起到抛砖引玉的作用；为贯彻《中华人民共和国计算机信息系统安全保护条例》，使我国各行各业计算机的安全运行尽一份力量。

邓凡全

1994 年 10 月

前　言

随着计算机科学技术的飞速发展，计算机系统安全技术正在形成独自的学科。由于计算机系统的安全问题已变得越来越重要，有组织、有计划地搞好全社会与大、中专院校的计算机安全普及教育已提上日程。这也是贯彻落实《中华人民共和国计算机信息系统安全保护条例》重要措施之一。为此湖北省公安厅、中国计算机学会安全专业委员会湖北组、湖北省暨武汉市计算机学会计算机安全专业委员会组织有关院校专家教授共同编写了此书。

本书着眼于从计算机整个体系安全来叙述，力求深入浅出地讲清概念，并注意运用典型，提出分析问题的思路和方法。使读者能举一反三，学以致用。书中收集了许多翔实的资料，以利读者查阅参考。

本书第一、四、五、六章由王锡林编写，第二章由程胜利编写，第三章由郭庆平编写。全书由王锡林主编。本书署名以姓氏笔画为序。在本书编写过程中，孙俊逸、胡金柱协助收集了很多资料，魏修建、刘宗萍、杨超、田少波等同志做了许多工作，邓凡全同志自始至终给予了极大的关心和支持。此外我们还参考了一些专家学者的论著，并得到有关院校的大力支持，全书最后由吴庆保同志审阅。在此向这些单位和同志一并致以由衷的感谢。

由于本书编写时间仓促，误漏之处在所难免，诚望读者指正。

编者

1994 年 10 月

目　　录

第一章 绪 论

自从世界上第一台计算机诞生以来，经过40多年，现在计算机已得到广泛应用，并得到迅速发展。它已经成为世界各国有关部门的要害部位。计算机对社会的作用越大，人们对计算机的依赖性越强。由于对计算机的种种危害直接威胁了各行各业的发展和国家的机密、财产的安全。所以计算机安全已经成为评估计算机系统的必不可少的重要指标。计算机安全学正在形成为独自的学科体系。

1.1 计算机安全

1.1.1 计算机安全定义

多年来，国内外对此众说纷纭，包括国际信息处理联合会(IFIP)计算机安全技术委员会(TC11)在内的不少具有一定权威的学术技术组织机构，一直未能就此表明看法。我国公安部在国内外众多说法的基础上，提出了计算机安全的概念如下：

计算机系统的硬件、软件、数据受到保护，不因偶然的或恶意的原因而遭到破坏、更改、显露，系统连续正常运行。

反过来，计算机的不安全称为计算机危害。对照计算机安全的概念，计算机危害的概念就是：计算机系统的硬件、软件、数据未受到保护，因偶然的或恶意的原因而遭到破坏、更改、显露，系统不能连续正常运行。

上述定义，既说清了计算机安全的本质和核心，又顾及到了安全所涉及到的方面。

安全对抗的核心对象是计算机信息系统。

定义中所提的计算机系统，指的是信息系统赖以存在的实体和依赖于计算机实体所生成及运行的信息系统。

所谓计算机系统实体，应包括计算机本身的硬件、软件、数据和各种接口，也应包含各种相应的外部设备，还应包括形成计算机网络时应有的通信设备和线路、信道。计算机系统之有用，是在形成了计算机信息系统之后。计算机系统实体本身再昂贵也是有价的；而信息系统则是无价的，它的损害往往是无法弥补、难以挽回的。

“系统连续正常运行”，进一步阐明信息系统的动态安全，保证信息系统正常运转，为我所用，发挥应有效益。

“保护”的终极目标是信息系统的安全。为此，必须保护计算机系统实体及其所在的环境。所谓环境，不仅是指机房等物理环境，更重要的是系统所处的社会人文环境。

安全对抗的核心因素是人。

不言而喻，计算机系统、物理环境和社会人文环境，皆为人控制，各种计算机危害，除了难以预知和抗拒的天灾，亦为人所致。人是最为活跃、能动的核心因素。唯有依靠人，采取技术的、管理的和法律的得力措施，才能把计算机危害抑制到最低限度。从这个意义上讲，计算

机安全治理的核心问题是人的技术和职业道德教育。

1.1.2 计算机危害的来源

从计算机安全治理的角度看，造成危害的来源有：自然灾害；故障；失误；违纪；违法；犯罪。

欲使计算机系统正常运行，必须努力避免各种非人为的灾害，最大限度地抑制和杜绝形形色色的人为危害。计算机安全所讨论的对象始终是人、计算机系统（各类硬件和软件）和环境（物理环境和社会的各层次管理环境）。

1.1.3 计算机危害与其他危害的区别

计算机危害是一种崭新的危害形式，与其他危害相比，突出的区别是技术性和专业性，且易造成严重的危害，而被界定为犯罪。计算机犯罪有如下特点：

（1）高技术智能犯罪。计算机犯罪的直接目标，除了有形的计算机及其运行环境，更多的是无形的电子数据或计算机信息系统，作案手段往往是运用计算机技术，作案人不少都是掌握计算机技术、从事计算机工作的。

（2）作案时间短，犯罪指令的执行，有的只要几十微秒。

（3）地域广大。在大区域范围计算机联网的情况下，作案的地点、时间难以受到限制，可在甲地作案，使乙地或广大联网地受害。

（4）隐蔽性强。作案时可以不留痕迹，极难被人发现。

（5）变化多端。

（6）破坏性大。

（7）蔓延迅速。

（8）涉及面广。

（9）攻击的主动性。

1.2 计算机危害概况

科技的进步推动了社会的进步，造福了人类；但也提供了新的危害人类和社会的有力手段。造福与危害，总是形影相随。惨痛的教训，往往更能使人警醒。前车之辙，后车之鉴。形形色色的危害，已引起人们对计算机安全的方方面面的认真思索和探讨。

人为地利用计算机实施危害及犯罪活动，始于六十年代末，七十年代迅速增长，八十年代形成威胁，成为发达国家和发展中国家不得不予以关注的社会公共安全问题。尤其是泛滥的计算机病毒，已是无所不在，成了危害社会的一大公害。可以预料，计算机危害将成为强大的威胁手段，或用于恐怖活动，或用于政治、军事对抗，或用于经济、科技骚扰破坏等等。

1.2.1 日益严重的计算机危害和犯罪

一、事故

计算机系统及所在的机房，事故极为普遍，有人为的，也有自然因素造成的。

（1）1978 年 10 月 18 日，苏联驻美大使多勃雷宁乘坐的客机，飞至纽约拥挤的长岛上空时，突然从肯尼迪机场雷达望远镜上消失，飞机在无导航的情况下飞错了高度，险些发生空中

撞机或降落失败事故。事后查明，其原因是非直接担任管制的官员输入了不正确的数据。

（2）1980 年，美防空司令部指挥中心，因计算机输入数据错误，引起防空报警，控制系统上显示苏联向美国本土发射导弹，美国最高指挥部命令一千枚导弹待发，一百架飞机起飞迎击，并命令部队进入实战状态，核战争一触即发。

（3）东京电信局一工人，在维修电缆时不慎引起火灾，火灾持续 16 小时，程控电话交换机损毁，致使几家大银行和邮局的计算机系统通信中断，近 50 个邮局业务受到严重影响，有关银行分布在全国的自动付款机被迫停机，客户取不到钱用。

（4）沈阳铁路局某计算机控制系统，连续 3 次遭雷击，损坏主机和终端设备，使机车编组作业中断，严重地影响了铁路运输秩序。

（5）1978 年 8 月，山东济南某银行办事处计算机仓库失火，烧毁库内所有设备，直接损失 55 万元之多。

（6）1987 年，武汉某大学计算中心因空调系统保温材料选用不当引起火灾，只是抢救及时，才未酿成大祸。

据有关方面调查，由于受人力、物力、财力、使用水平等因素的限制，我国不少计算机房没有防震、防火、防水、避雷、防电磁泄漏或防干扰等措施，抵御自然灾害和意外事故的能力较差，事故不断，因断电而设备损坏、数据丢失的现象也屡见不鲜。

二、窃用计算机系统

（1）1978 年，纽约港丢失了一张提货单，被一伙熟悉计算机技术和货物处理业务的人拾到后，潜入机房操作计算机，改变到货地点，并通知将这批货转运到黑市场出售，事后抹除作案时留下的数据记录，获利一亿美元之多。

（2）有些工作人员利用计算机，把个人打长途电话的费用记到公家帐号上，以此“揩油”。

（3）我国某研究院，有人更换计算机口令，取消了对一些系统数据的保护；后又发现修改了记帐收费程序参数，造成计算机运行混乱，日记账表不能打印输出，系统管理员无法工作。

其实，大多数恶性计算机危害案件，其基本的作案形式就是窃用计算机系统，只是因为危害的引人注目而归为其他类型罢了。在我国，由于对知识、资源等观念上的差异，或因这些危害造成的有形的损失似乎不大，未能引起应有的关注和认定。

三、非法获取数据和信息，窃取机密，倒卖获利

（1）美国某软件公司一职员在其女友鼓动下，乘夜间无人值班之机，只用了 20 多分钟，就打印并转移了该公司耗资 7 万美元研制的软件；直到其女友以该软件敲诈该公司时，才发现软件产品被窃。

（2）日本某杂志社发行代理公司，将耗资 5 亿日元收集到的订户名单等公司商业绝密信息委托给太平洋计算机中心处理，在转手处理过程中，其信息磁带被人转录，并以 82 万日元出手获利。

（3）我国家机关某助理工程师借工作之便非法复制单位属有的软件 37 个、100 多片软盘，并以某技术开发公司的名义倒售给该国家机关和其他单位，售价 7100 元，本人获款 5150 元。

（4）我国公安部门，当初为社会各界免费拷贝清除病毒软件，但个别公司却转手高价倒卖给暂不知情的用户。

四、破坏计算机系统

（1）东亚反日武装战线会员 6 人，于 1975 年 2 月，用爆炸手段袭击建设公司大楼六层的

营业部和九层的计算机房，造成损失约 20 亿日元。

（2）西德一研制导弹的公司遭炸弹袭击，使计算机设备和大量数据被毁，只因存有备份数据，公司业务工作才得以恢复。

（3）美国一爱滋病研究人员，向世界两万多机构邮寄了带有破坏性程序的爱滋病咨询信息磁盘 200 万个，被国际刑警抓获。

（4）我国某市电信局某工作人员对其工作调动不满，破坏了该局计算机长途电话查询系统，致使长途电话查询瘫痪。

五、计算机病毒

研制、传播计算机病毒的客观效果是危害或破坏计算机系统的资源，中断或干扰计算机系统的正常运行。计算机病毒是危害计算机的最新手段，防不胜防。许多国家的官员和经理们整日提心吊胆，坐立不安，不知什么时候，哪些计算机会有哪些病毒发作，造成什么样的严重恶果；技术人员也弄不准自己手中的软件里，有没有传染上病毒，人心惶惶，造成极大的心理负担。工作越是认真的，心理压力就越大。

1. 计算机病毒的出现

（1）计算机病毒概念的提出

有人说，早在计算机诞生不久，就有人预言了今日谓之计算机病毒的功能的存在。在 1984 年以前，有人声称，计算机病毒已实际存在。弗瑞德. 科亨(Fred. B. Cohen)博士经过一段摸索，作为他的博士论文的一部分，建立了一种演示病毒。其初衷在于试图找到一种防止计算机系统程序自我复制的方法。

1984 年 9 月，在加拿大多伦多，国际信息处理联合会(IFIP)计算机安全技术委员会(TC11) 举行年会(IFIP/SEC'84)，他首次正式发表论文《计算机病毒：原理和实验》，公开提出了计算机病毒的概念；其后，又发表了论文《计算机和安全》。

1986 年 3 月，儒迪吉. 戴尔斯吞(Rudiger. Dierstein) 在巴黎举行的 SECRICOM 会议期间，发表了《计算机病毒：一种隐藏的威胁》。

1987 年夏，艾恩. 威吞(Ian. H. Witten) 在 Abacus 杂志上发表了《计算机和安全：渗透开放系统》。

（2）计算机病毒侵入社会

① 首例计算机病毒——BRAIN

1987 年 10 月，美国得拉华大学(Delaware)受到了巴基斯坦病毒(Pakistan 或称 Brain 病毒) 的攻击。它是攻击测试实验室以外的计算机的首例。接着，又在美国匹兹堡、华盛顿、宾夕法尼亚等大学陆续出现。随后，又传到澳大利亚、新西兰、英、法、德、荷等国和香港等地。该病毒是一种引导型病毒，以 Brain 为卷标，系巴基斯坦拉合尔(Lahore)的巴西特(Basit) 和阿姆杰得(Amjed) 所为。受感染的文件运行时，显示屏上出现如下内容：

Welcome to the Dungeon
(c) 1986 Basit & Amjed (pvt) Ltd.
BRAIN COMPUTER SERVICES
730 Nizam Block Allama Igbal Town
Lahore, Pakistan
Phone: 430791, 443248, 2800530

Beware of this VIRUS

Contact us for vaccination

由显示内容可知，该病毒的编制和出台是在1986年。

② 早期的计算机病毒

根据 Aziz. East 的报告，1987年9月，阿拉梅达(Alameda)病毒（国内称林荫道病毒）出现在美国加利福尼亚的阿拉梅达学院，攻击了梅里特学院的计算机系统。

1987年11月，(COMMAND.COM)病毒（又称利哈依病毒）出现在宾夕法尼亚的利哈依大学。

1987年12月，以色列耶路撒冷的希伯莱大学受到了计算机病毒的攻击，发现了黑色星期五病毒和四月一日病毒（或称愚人节病毒）。

此后，又出现了乒乓、大麻、维也纳、批处理、Macro 等病毒。

2. 计算机病毒泛滥世界

自1987年秋，计算机病毒开始受到世界范围新闻机构的关注和报道。不断产生的计算机病毒及在世界范围内的泛滥和危害，加上新闻媒介的报道，一时成为世界计算机界的热点，公认1988年为世界计算机病毒年，几乎到了风声鹤唳，谈毒色变的地步。

国外有人估计，现在病毒的传染范围将两月增一倍。凡用 PC 微机的，几乎没有不受到过病毒侵袭的，不同的，只是程度的差异。据不完全统计，美国在1988年里，约有9万台计算机被病毒感染；仅在11月份里，病毒感染造成的损失就超过了1亿美元。

(1) 美国一家银行的一名计算机程序员事先在计算机中放入一个病毒，该病毒发作的条件是“当我的名字在人事档案中消失，会计系统则发生紊乱”。后来他被辞退了，果然，不仅银行会计系统出了问题，而且，所有与这家银行联网的部门也都出现了紊乱。

(2) 1988年8月，苏联政府机构的计算机网络发现病毒入侵，3个月后，据专家宣称发现了3类病毒，已查明其中两种：一类是 A 型，专门阻塞存储器，迫使计算机停止工作；一类是 B 型，破坏文件目录，使计算机无法工作。

(3) 1988年9月，与日本电气公司联网的日本最大的计算机网络 PC—VAN 网，其用户计算机遭病毒侵害。

(4) 1988年春，台湾大学资讯工程研究所，一台参加国际计算机围棋赛的计算机被病毒侵扰瘫痪，无法对弈。这是在台湾发现的首例计算机病毒。

3. 计算机病毒侵入我国

随着计算机病毒世界范围的泛滥，我国也未能幸免。不少单位、各类人员出于猎奇、研究、营利、炫耀等不同初衷，对病毒知识及其防治起了普及的作用。有关病毒防治的工具产品正在形成市场，有关资料、书刊、交流、培训，势头见旺。但在看到积极效果的同时，也须注意到病毒在我国迅速泛滥的状态。据不完全统计，我国拥有计算机的单位中，大约80%为病毒所害过，几乎无一行业系统幸免；经销、维护、研究及院校等单位，微机病毒感染率达百分之百。自1989年春始，在短短不到一年的时间里，计算机病毒的泛滥、危害达到如此程度，成为我国1989年计算机界十件大事中的第五件。有人称，1989年是我国的计算机病毒年。

(1) 我国国家某部门进口了数百台微机，拟发全国有关部门使用，经检查，发现台台有计算机病毒。

(2) 有人把国外传入的计算机病毒国产化；或自行研制国产计算机病毒；在计算机病毒

检测软件出现后，修改病毒标志，使之难以发现，例如，把乒乓病毒标志“1357”改为“8024”，把以色列病毒标志“MSDOS”改为“MSVVV”。

（3）广州某大学一学生编制了一病毒，命名为“中国病毒一号”。

（4）西安某大学传出的“中国炸弹”有多种版本，它使山东某单位受害，自1949年以来辛辛苦苦积累起来的数据毁于一旦。

六、诈骗

采用各种非法手段，例如编制诈骗程序、篡改数据、输入假数据等，获取非法利益。这是到目前为止，世界范围损失惨重，计算机违法犯罪的又一突出方面。有资料报导全世界每年被计算机违法犯罪直接盗走的资金达20亿美元以上，平均每次违法犯罪造成的损失，1983年约为5万美元，到1988年，就增加到65万美元，而传统的敲诈银行案平均每起损失1.9万美元，抢劫银行案平均每起损失4900美元，相比之下，是常规犯罪的几百倍。在英国，有一个不完全的调查，约20%以上的计算机用户遭害，平均每起损失约7万美元。

（1）1978年，美国太平洋安全银行雇用的计算机技术顾问，通过银行计算机，将一千多万美元转到瑞士苏黎世某银行，构成美国当时最大的盗窃案。

（2）1986年5月，联邦德国的4名罪犯，利用计算机改变信用卡上的磁带密码，骗取了10万马克，后经发现而被捕。

（3）1986年12月，法国银行发生了一起几千万法郎的丢失案件，至今尚未破获。

（4）曾被国际刑警组织列为第六号和第七号要犯的盖里奥和奥尔托拉尼，用计算机系统把意大利亚布罗西银行的约9千万美元一扫而空，移款至瑞士，逍遥于拉美，致使银行倒闭，银行总裁自杀。

（5）美国一计算机工程师以考察为名，两次混入某银行电子转账室，骗取信任，一边询问查阅，一边记下重要口令；然后从外部打电话，自称银行行长，需向苏黎世银行转1020万美元，业务员竟然照办。之后，该犯飞抵苏黎世，用该款购得钻石，返美销售，直至事败被捕，银行毫无察觉。

（6）日本某银行一女职员与男友共谋，事先在该银行的5个分行设户头，然后操作终端机，向这些户头汇入存款，分别从大阪、东京的三个分行提取现金及支票总额1.3亿日元。作案者当天潜逃国外，后经国际刑警组织追捕归案。

（7）日本某银行行长和一分行行长代理，与该分行贷款董事会代表共谋，事先设立假户头，然后非法操作终端机制作存折，从该行支取四十多亿日元。

（8）美证券投资公司为掩盖连年亏损，利用其计算机伪造高收益账面，以欺骗各股票交易所和州政府保险局，进行大规模弄虚作假，编制了总金额为21亿美元的人寿保险合同6400个。因一名内部人员向州政府保险局告发，受到特别检查，发现该公司进行这种欺骗活动已达10年之久。最后不得不宣布破产，成为美国历史上第二大破产事件。

（9）1988年3月，我国成都某银行微机操作员伙同借调人员，篡改计算机程序骗得人民币87万元。案发后，在有关部门调查此案的同时，又用计算机消除罪证，企图掩盖罪行。

（10）1989年12月，河北某银行营业部副主任伙同他人，利用微机开空头汇票，骗得人民币179万余元。

七、其他

形形色色的计算机危害，早已实实在在地存在着，只是未引起人们重视。

例如，信息的电磁泄漏与侦截，是无线电技术领域里的老课题；利用计算机及其外围设备

电磁泄漏，侦截各种情报资料，是驾轻就熟的情报战的新热点。

再如，利用“黑客”窃取口令等手段，渗入计算机系统，用以干扰、篡改、窃取或破坏。

又如，在磁盘信息恢复技术方面，国外达到的水平是，硬盘被格式化多遍，其残留信息仍能被恢复；在我们的磁盘“以坏换新”时，多未注意这种形式的信息外泄。

1.2.2 计算机危害的特点及发展趋势

一、危害巨大，发生率的上升势头前所未有

(1) 据有关方面统计，由于计算机犯罪而遭受的损失，目前美国每年超过百亿美元；法国约 100 亿法郎。

(2) 美国联邦调查局的一份报告指出，在硅谷，计算机犯罪正以每年 400% 的速度上升，能破获的，只有其中的 10%。

(3) 日本自动付款机的犯罪案十年间增长 90 倍；已立案的利用信用卡犯罪案高达 10108 起，损失金额高达 6.287 亿元；据警方人士估计，实际犯罪案件数要高出立案数的好几倍。

(4) 美国康奈尔州大学博士研究生莫里斯，他研制的蠕虫病毒使美国国防系统的洲际 INTERNET 和 ARPANET 计算机网络的 6000 多台计算机受害瘫痪，仅二十四小时停机一项，直接损失就达一亿美元，恢复工作则持续一月之久。有人说，这是未来战争序幕的一次演习。

(5) 世界上现在到底已出现了多少病毒，无准确的统计。在 1989 年，有说 30 多种的；1990 年初，AST 公司在推出《VIRUSCAN》抗病毒软件时声称，可测知及消除 52 种病毒。1990 年中有检测到 100 多种的；1990 年底有人说有 300 多种；1991 年，出现了列有 500 多种的计算机病毒表；1992 年二季度，美国的 McAfee 则推出能检测和清除 1000 多种病毒的治理软件。最近，美国 Trend 分公司又推出能检测 2300 种病毒的软、硬结合的 PC—cllin。

(6) 我国自 1986 年发现首例计算机犯罪以来，1986—1987 年发生 9 起案件，1988—1989 年则发生上百起。诈骗金额从数万元发展到上百万。从 1989 年初发现计算机病毒，不到两年就蔓延到全国各地的各行各业，几乎无一行业系统幸免。若将计算机病毒列入计算机犯罪中统计，我国的计算机犯罪，正以每年平均数十倍甚至上百倍的速度猛增。

二、危害领域不断扩大

当初，危害领域主要是金融系统。现在，则已发展到邮电、科研、卫生、生产等几乎所有使用计算机的领域。受害的，往往是整个地区、行业系统、社会或国家，以致被称为公害。

三、计算机违法犯罪社会化

开始阶段主要是内部计算机专业技术人员作案；现在，则是非计算机专业技术人员和熟悉部门业务及其他外部人员作案增多；作案过程中，也并非完全使用高技术手段，且多为内外勾结，共谋作案。

四、计算机危害的国际化

过去作案，主要在一个国家内；现在，则通过国际联网，或计算机技术产品和媒体等，跨国作案，成功率很高，而且发案率有上升趋势。

五、危害目的多样化

计算机信息系统，已日益成为各个行业系统、各个地区国家的核心机密的集中部位。信息系统运行的干扰与反干扰信息的窃取与保护，历来是异常激烈的看不见的战线。以前作案，多以获取钱财为目的；现在，各政治经济集团、敌对势力之间，则纷纷利用各种计算机危害手段

来达到各自的目的。国外甚至有人声称，计算机战争的威胁远比核武器的大，包括计算机病毒在内的各种危害手段，正受到国外军方与日俱增的高度重视。

(1) 有消息说，美国军方已签订了价值数十万美元的武器合同，武器是带有固化病毒的微机芯片；平时，这类芯片以商品的形式进入敌对国家的计算机系统，一旦需要，随时可以激活，危害敌对的计算机指挥控制信息系统、自动化指挥系统或雷达系统等，使之失灵或瘫痪。

据英国《新科学报》报导，伊拉克从法国购买了一种用于空防系统的新型打印机，美国间谍在其中插入了一种带有计算机病毒的微机芯片，该病毒能使伊拉克军事指挥中心的主计算机失灵。据称，微机芯片是美国马里兰州米德堡国家安全局设计的，病毒名为 AF/91。美官员说，该病毒达到了预期的目的。这恐怕是把计算机病毒用于战争的首例。

(2) 1988 年，联邦德国汉诺威大学计算机系学生，把自己的计算机联入美国军方及军工承包商的有 30 台的计算机网络，在两年的时间里，收集到大量的美国国防机密，其中有"星球大战"计划，北美防空司令部、核武器和通信卫星等方面的有关情报。

另据报导，由于美国国家航空航天局在全世界的数据网的保密系统存在缺陷，被一些计算机爱好者钻了空子，用"航天飞机"、"挑战者号"和"机密"等关键字进入了该数据网，看到了"航天飞机 C 研究合同"、"系统的安全调查"和"助推火箭事故"等内容，还可接触该网用户的电子邮件，甚至可使整个数据网陷于瘫痪。

(3) 我国国内的敌对分子已开始用计算机病毒制造政治影响。国内某些单位的计算机既未和社会计算机联网，也未和社会系统交换数据，却也感染了计算机病毒，这说明，国内外敌对势力的阴谋不是不可能实现的，值得我们高度重视。

六、计算机犯罪者年轻化，转化为恶性案件的增多

根据调查统计，计算机犯罪者的年龄区段为 18—46 岁，平均年龄约为 25 岁。他们大多有知识，且聪敏好动，虚荣心强。计算机犯罪的一大特点是，正常的运行操作同危害犯罪的实施，在工作形式上甚难被发现。有些年轻人的猎奇冲动之下，易于顾后不顾前作案，这在国外已不稀奇，在国内也发生多起。

七、危害手段更趋隐蔽复杂

据美联社 1990 年初报导，三名计算机工作人员利用个人计算机和偷窃的某电话公司的设备及开关密码，取得了绝密的军事文件和联邦调查局关于菲律宾前总统马科斯密友的情报。

1991 年 1 月，我国某银行微机操作员盗取密押软件，利用计算机联行的有利条件，将 186 万美元巨款转出境外，据为己有。

八、计算机犯罪的高技术，使许多犯罪的实施，可在瞬间完成，往往不留痕迹

现有的规章制度、法规和不少人的观念难以对他们进行制约、界定和制裁。这也是计算机危害日趋严重的重要原因之一。因此，法规的制订刻不容缓，安全管理必须加强，安全技术措施应当跟上，计算机安全教育和职业道德教育势在必上，这已成为国内外专家学者、有识之士及深受其害的广大用户的共识。

1.2.3 计算机安全内容层次

形形色色对计算机的危害，其最终目的是使计算机信息系统遭到显露、更改或破坏。除了不可预知和抗拒的灾害，都与人有关。人是最活跃、最能动的因素。任何危害，都有一个过程。在这全过程的任何环节上，我们都可以采取相应的有力措施予以制约和制止，避免或减轻损失。或者说，我们应当而且可以在计算机安全的各个工作层次上制止或制约危害的产生，确保