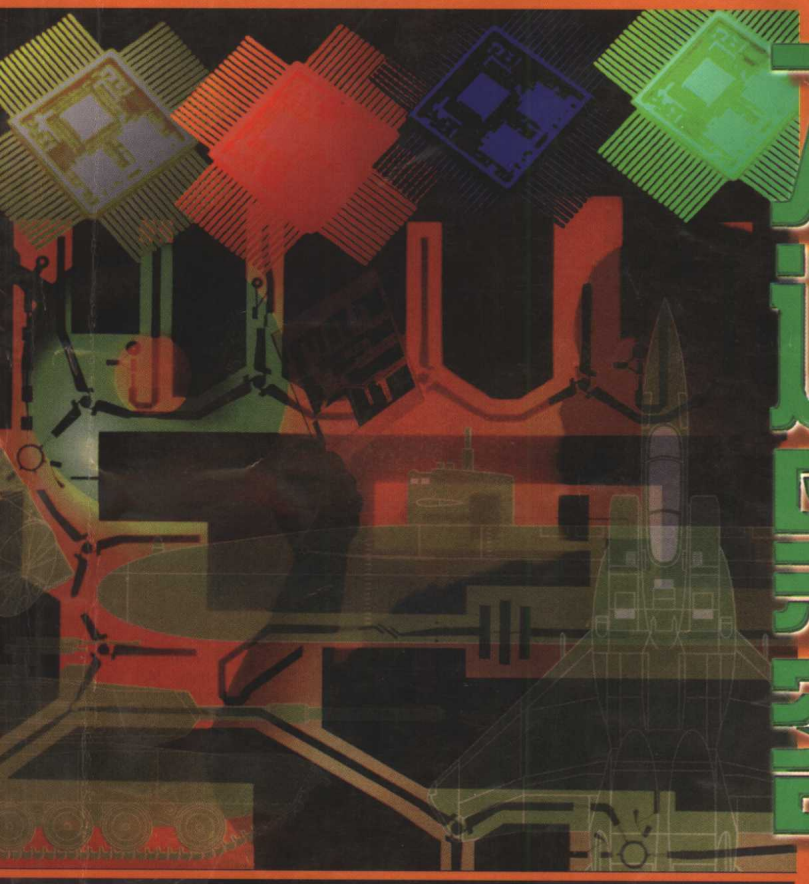
新概念武器丛书

不速黑客

计算机病毒武器



魏 平 编著

国防大学出版社

新概念武器丛书

不速黑客

——计算机病毒武器

魏 平 编著

国防大学出版社

图书在版编目（CIP）数据

不速黑客—计算机病毒武器/魏　平编著．—北京：
国防大学出版社，1998.8
ISBN7—5626—0872—5

Ⅰ．不…　Ⅱ．魏…　Ⅲ．计算机病毒—武器—军事技术　Ⅳ．E92

中国版本图书馆 CIP 数据核字（98）第 14664 号

国防大学出版社出版发行
（北京海淀区红山口甲 3 号）
邮编：100091　电话：（010）66769235

颐航印刷厂印刷　新华书店经销
1998 年 8 月第 1 版　1998 年 8 月第 1 次印刷
开本：850×1168 毫米　1/32　印张：4.25
字数：79 千字　印数：8000 册
定价：6.20 元

编者的话

人类社会的历史，经历了农业革命、工业革命，正在进行着一场新的技术革命。

在今后的20年，人们将会看到，信息技术、生物技术、新材料技术、新能源技术、航天技术、海洋开发技术、纳米技术以及氢能技术等将飞速发展，并对社会各个领域产生重大影响。

同历史上的每一次技术革命一样，当代正在进行的高新技术革命，也把它长长的触角伸向了军事领域。

科学技术发展对军事领域的影响，往往最先表现在武器装备的更新换代上。高新技术革命的浪潮，正有力地推动着“新概念武器”的诞生。

那么，什么是新概念武器呢？从广义上讲，新概念武器是代表着一代武器发展及其技术进步趋势的一个新的武器技术群体，其特点是原理概念新，高技术含量大，具有鲜明的时代特征。例如，火器在冷兵器时代后期曾是当时的新概念武器，今天却变成了常规兵器，而今天的新概念武器，则处于当今时代兵器技术发展的前沿，成为牵引未来武器技术进步的“火车头”。从目前情况看，已经崭露头角的新概念武器主要有智能武器、太空武器、隐形武器、计

算机病毒武器、激光武器、粒子束武器、射频武器、基因武器、非致命武器、超高速动能武器、气象武器等。这些武器，具有超常的威力和非凡的功能。它们在战场上的广泛使用，将使战争面貌为之一新。

为了普及军事高技术武器知识，使更多的人了解新概念武器的种类、原理、性能、现状、发展趋势及战场运用特点，我们特编辑出版这套丛书。丛书共5册，包括《超级斗士——智能武器》、《神奇杀手——新机理武器》、《天庭战神——太空武器》、《战场幽灵——隐形武器》、《不速黑客——计算机病毒武器》。丛书依据新概念武器技术的现状及可能发展，对未来可能出现的新概念武器进行了预测，并对这些武器在战争中的运用进行了假想。在写法上，以故事为载体，采用了一些文学描写手法，力求把深奥的高技术知识融入有趣的故事情节之中，使之具有较强的趣味性和可读性。如果这套丛书能够得到广大读者的认可和喜爱，我们将感到莫大欣慰。

目　录

不速黑客

——计算机病毒武器

引　言

1946 年 2 月 14 日，美国宾夕法尼亚大学一间食堂大厅里挤满了要人和工程师，美国陆军的一位将军按下一个按钮，一个有 17468 个真空管的庞大的家伙开始运行起来，人们把它称为“埃尼阿克”（ENIAC），即电子数值积分和计算机。

这一天，成为人类历史上重要的一天。

1996 年，在世界上第一台电子计算机问世 50 周年之际，还是在宾夕法尼亚大学，为纪念它诞生 50 周年的纪念仪式上，美国副总统戈尔按动了这台已沉睡了几十年的庞大计算机的启动电钮，以纪念信息时代的到来。“埃尼阿克”上的两排灯以准确的节奏闪烁到 46，标志着它于 1946 年公开亮相，然后，又闪烁到 96，标志着计算机时代开始以来的 50 年。

50 年转眼而过，计算机已经不再是又笨又大的家伙了。第二代、第三代、第四代计算机相继问世，第五代智能机正在发展中。计算机变得小巧便携，操作方便，价格适宜，计算速度以亿次计，它已经深入到人类生活的每一个角落，扩展了人的大脑，延伸了人的手脚。计算机的应

用已普遍深入到企业、机关、学校等领域，并已经走进家庭，无论是传真、电话、汽车、微波炉、自动售货机、电视、录像机、金融卡、自动柜员机，还是工业管理、文档管理、交通信号系统、医疗设备、天气预报等，都必须依赖电脑。最近，美国有关部门就其国内的家庭电脑的拥有状况做了一次全面调查。其结果表明，到目前为止，在美国 6200 万个家庭中，37%的家庭拥有电脑。美国的一个调查机构估计，到本世纪末，美国每户人家平均拥有 2.2 部个人电脑。现在美国每人每周在家庭电脑前平均花费 13 个小时。电脑已确确实实地深入人们的生活之中，给人们带来了巨大的方便。

然而，科学的发展史表明，科学技术的作用具有极大的矛盾性，它即可以极大地造福人类，又可以伤害甚至毁灭人类。

法国著名作家雨果曾说过："没有什么东西比烟更柔和，也没有什么东西比烟更可怕的了。有和平的烟，也有罪恶的烟。一股烟的浓度和颜色不同，也就是战争与和平、友爱和仇恨、生和死的全部分别。树丛里升起一股烟，可能意味着世界上最可爱的东西：家庭里的灶火；也可能意味着最可怕的东西：火灾。有时一个人的全部幸福或者全部不幸就寄托在这随风吹散的东西里。"

当远古的先哲们构想了一个神话英雄普罗米修斯从天上盗取火种带到人间的故事时，他就昭示人类：火可以给人类以无穷的力量，也会带来灾难。

中国古人发明了火药，却被西洋人用来制造枪炮，于是，地球这个蓝色的星球被人类的两次世界大战的烟云所笼罩。第一次世界大战，厮杀的双方使用了机关枪、大炮、军舰，甚至坦克和飞机也开始派上用场，人类为此付出了惨重的代价。第二次世界大战，火药的功能发挥到了极点，飞机、坦克、大炮、军舰，甚至导弹统统派上了用场，从大西洋到太平洋，从欧洲到亚洲再到非洲，世界各地战火纷纭，生灵涂炭，人类再次付出了惨痛的代价。

这就是科学技术的双重作用。它既给人类带来光明，又不时把人类抛进黑暗。

计算机，这个人类的新宠儿，随着它从幼年走向成熟，在社会中起的作用越来越大，也走入了科技发展的“怪圈”之中——开始对人类产生危害，计算机病毒就是它对人类社会最大的危害。

1988 年，美国一所大学里的一名研究生利用小小的病毒使美国国防部远景规划局等部门的几千台计算机瘫痪，使美国乃至全世界都为之震惊。

1990 年 1 月，美国电话电报公司的交换台电脑出现一种传染性故障，并扩散至整个庞大的电话网络，导致几百万用户不能使用长途电话长达 9 个小时。1990 年 8 月，美国陆军一位情报军官说，有理由相信这件事是软件破坏分子用计算机病毒蓄意制造的。

1992 年 3 月 13 日，尽管新闻媒体事前大量提醒人们注意这一天要防止受到“米开朗基罗”病毒的攻击，但仅

欧洲就有2000台重要部门的计算机受到该病毒的感染。

1994年初的一天，我国南方某大型国有企业的财务部门正在紧张进行年终财务结算。突然，计算机屏幕上出现了几只熊熊燃烧的火把，财务工作被中断，操作人员被惊呆了。经过专家会诊，确定为“火炬”病毒，如不及时消除，就会毁坏系统和数据，后果不堪设想。

有一次，某高校为新开发的数控精密机床开鉴定会，刚一开车，猛然一声巨响，夹具自动松开，加工件被砸在地上。后来才弄清楚，原来是微机中的“黑色星期五”病毒在作祟。

……

病毒，病毒，还是病毒！美国大陆告急，欧洲大陆告急，中国大陆也警报频传！

在当今的社会中，只有两种病毒能引起人类的极大关注，一个是艾滋病病毒，另一个就是计算机病毒，现在的人们已经是谈“毒”色变了。

科幻小说与游戏的产物

“病毒”（Virus）一词源于生物学。过去，由于计算机普及程度较低，人们对计算机病毒还没有一个正确的理解，因此，发生过许多令人啼笑皆非的故事。

一天，一位从事计算机安全工作的专家和一位出租车司机聊开了舆论界的热门话题——计算机病毒。司机问他：“到底计算机是怎样染上病毒的呢？是程序员冲着计算机打了个喷嚏吗？”计算机安全专家哑口苦笑。

还有一个令人哭笑不得的故事。一个在单位负责管理计算机的技术人员得知近期是电脑病毒集中发作期，而他又不能判断机器内是否有病毒存在，为了安全起见，他向领导申请购买杀毒软件。领导听后很不高兴，认为他太娇气，只发给他一副口罩。

今天，提起计算机病毒简直是妇孺皆知了，甚至在有些地方、有些时候，人们已经达到了谈毒色变的地步。那么计算机病毒到底是怎样产生的呢？

在美国，有一个闻名世界的大公司——美国电报电话公司。它所属的贝尔研究所里，有一群年轻有为的青年人，他们为公司创造了巨大的财富，也领取着丰厚的薪金。年

轻人毕竟是好动的。在工作之余，他们常常玩一种他们自己创造的计算机游戏，这种被称作“达尔文”的游戏很有趣，由每个人编一段小程序，输入到计算机中运行，相互展开攻击，设法毁灭别人的程序。这种程序就是一种计算机病毒的雏形，只是当时人们并没有意识到这一点，也没有向实验室外有意传播。这件事发生在本世纪的 60 年代初。

不知是受这种行为的启发，还是心有灵犀，十几年后，即 1977 年夏季，一位美国人写了一本科幻小说，名叫《THE ADOLESCENCE OF P－1》。在这本书中，作者构思出了世界上第一个计算机病毒，这种病毒能从一个计算机到另一个计算机传染流行，能控制 7000 台计算机的操作系统。虽然这本小说受到世人的瞩目，但人们仅仅把它作为一种幻想，一部文学作品。

鉴于上述情况，人们普遍认为计算机病毒发源于美国。

所谓计算机病毒，其实是人们对一种能够破坏计算机正常工作的特殊软件程序的形象称呼。计算机病毒能够篡改正常运行的计算机程序，破坏这些程序的有效功能，并能够复制和侵入其它有用程序之中。

首次正式提出计算机病毒概念的是弗瑞德·科亨博士。他于 1984 年 9 月在加拿大多伦多国际信息处理联合会计算机安全技术委员会举行的年会上，发表了题为《计算机病毒：原理和实验》的论文。其后，又发表了《计算机和安全》等论文。然而，弗瑞德·科亨博士的论文并未引

起新闻界的重视，因为，计算机病毒毕竟只是在实验室、计算机中心才出现过。

然而，计算机病毒是不甘寂寞的。

1987 年秋，计算机病毒开始受到世界范围内新闻媒体的普遍重视。因为此时计算机病毒已不再是科幻作品，也不再是无害的游戏。它开始出现在实验室外，开始对人们的计算机造成威胁。当年的年末，计算机病毒攻击了三所大学。这三所大学中两所在美国，一所在以色列。

1987 年 10 月，美国特拉华大学计算机中心报告，在校园的其它地方而不是在计算机中心发现了病毒。这种名为“巴基斯坦”的病毒，由于是第一个攻击美国计算机中心、实验室之外的计算机系统的计算机病毒，因而在世界上有了相当的“知名度”。它之所以叫作“巴基斯坦”病毒，是因为人们在一张被感染的盘上，最初分析得到了两个病毒编写者的名字，其地址在巴基斯坦。这是一种引导扇区感染型病毒。

11 月，利哈伊病毒或称 COMMAND. COM 病毒在宾夕法尼亚州的利哈伊大学被发现。在利哈伊大学，计算机工作人员用图书馆借书一样的方式借给学生们微机程序盘，这些盘用于完成布置在机器上、或在大学的微机实验室、或在学生家中甚至在宿舍中做的家庭作业。学生们在计算机中心的检验计算机上操作时，因为磁盘引导失败，许多盘被退了回来。这一现象引起了负责实验室工作的学生顾问的注意。经过和原始的被保护的版本对比，他们发现

了病毒。由于病毒发现时恰好是学校的假期，一些学生已经把被感染的磁盘带到了家里，因此，造成了计算机病毒的扩散。

12 月，耶路撒冷希伯莱大学的工作人员发现，他们受到了计算机病毒的攻击。经过搜寻，发现了黑色星期五病毒。在进一步的搜寻时，又发现了两个名为四月一日病毒或称四月愚人节病毒的病毒变种。当时，学校的工作人员发现一些他们过去经常执行的程序突然变大而使内存容量不够，使程序不能运行。经过调查分析又发现，当病毒感染了内存之后，如果计算机的系统日期是从 1988 年开始的每逢星期五为 13 日的时候，所有被执行过的程序就会从盘上被神秘地删除。

计算机病毒根据其引导方式可分为三大类。

第一类是系统引导型病毒。这类病毒在系统（主要指 DOS）引导时进入到系统中，获得对系统的控制权，在完成其自身的安装后才去引导系统。在用户看来，DOS 系统已引导计算机进入正常工作状态，但实际上此时计算机的整个系统已在病毒程序的控制之下了。这类病毒的典型代表有米开朗基罗病毒、磁盘杀手病毒、2708 病毒等。

第二类是文件型病毒。这类病毒都依附在系统可执行文件（*. EXE 或 *. COM）或覆盖文件（*. OVL）上，在文件装入系统执行时，引导病毒程序进入计算机系统中。极少数文件型病毒程序也会感染数据文件。这类病毒主要有黑色星期五病毒、维也纳病毒、扬基都德病毒等。

第三类是复合型病毒。这类病毒同时具有系统引导型和文件引导型病毒的特点，它传染硬盘的主引导扇区和所有在系统中执行的文件。这类病毒的代表有 2153 病毒和 DIR－2 病毒。

计算机病毒最初出现的时候，许多人把它作为一种恶作剧式的行为，并未当作犯罪的手段。而且早期的一些计算机病毒也确实危害不大。1988 年 3 月 2 日，是美国苹果机诞生的纪念日。这一天，潜伏在苹果型计算机中的病毒突然发作，使计算机停止工作，并在屏幕上显示“向所有苹果电脑的使用者宣布世界和平的信息”的字样，令人啼笑皆非。

类似这样的病毒还有许多，如 1991 年出现的“讲故事者病毒”，该病毒进入计算机后，每 40 分钟有一次发作机会，屏幕上将出现一个窗口，病毒会在窗口逐行填入一段约为 1600 个字符的英文小故事。当故事全部显示完以后，病毒程序要求计算机用户入键一个字符，窗口便隐去，屏幕恢复正常。

然而，计算机病毒并不都是开玩笑、搞恶作剧的，还有许多病毒具有极大的破坏性。最后，甚至还要让你来个“苦恼人的笑”。这类病毒主要有以下几种：

“两只老虎”病毒。该病毒最早在台湾发现，当其发作时，不仅破坏数据，而且反复演奏儿歌《两只老虎》：“两只老虎，跑得快，一只没有尾巴，一只没有耳朵，真奇怪！”

“杨基都德”病毒。《杨基都德》是美国独立战争时期

的著名民歌，被计算机病毒程序编制者套用。在毁坏数据之后，该病毒便会得意洋洋地高歌此曲。这种病毒最早在美国出现，通常于每日下午5时发作。

“赌棍”病毒。这种病毒发作时，常把计算机中文件的长度加长，使之运行速度减慢，而且病毒还会向计算机用户挑战：“我是赌棍病毒。来吧，咱们赌一把吧！如果你赢了，我就把数据还给你。如果你输了，那你就含泪向你的数据说拜拜吧！想不想试一下你的运气？保证够刺激。”

“磁盘杀手”病毒。这种病毒发作时，会提醒你：“不要碰键盘，我来帮你清盘。”病毒将会删掉你所有有用的文件，待删尽计算机内的文件后，它还会彬彬有礼地向你告辞：“磁盘已删尽，再见！”

“快乐星期天”病毒。这种病毒会在星期天发作，感染了该病毒的计算机若在星期天被打开，病毒会在屏幕上告诉用户：“今天是快乐的星期天，忘掉你的工作吧！”然后便开始破坏计算机上的文件，使用户无法工作。

随着病毒在世界范围内的泛滥，还有些人开始别有用心地编造病毒程序，来达到自己的目的。

在美国，一所医院存储在计算机里的病历莫名其妙地全部消失了，计算机里留下了电话号码和这样一句话：“当心病毒，请和我们联系接种疫苗。”很显然，这是在进行敲诈，制造病毒的人把医院病历控制在手，就等于以病人的健康甚至生命为筹码向医院进行勒索。

自1987年10月计算机病毒首次公开露面以来，它已

经在世界范围内造成了极大的危害。可以毫不夸张地说，计算机病毒就在你身边。由于不断有计算机病毒破坏的新闻报道，使世人已经到了风声鹤唳、谈“毒”色变的地步。凡使用过微机的人，几乎没有不被计算机病毒侵袭过的，只不过有的因发现及时没有造成损失而已。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，病毒感染造成的损失就超过了1亿美元。于是，世人公认1988年为世界计算机病毒年。

有些人还把计算机病毒作为报复他人的手段。美国纽约州曾发生一起这样的案件，预测公司的经理哈伯曼向MJL公司订购了3600美元的软件。后来，哈伯曼以其性能不理想为由只付了1200美元，其余欠款拒付。为此，MJL的经理洛法罗恼羞成怒，开始实施报复。他让本公司的计算机软件技术员在预测公司的计算机系统中安装了能够销毁所有数据而造成惨重损失的“病毒”程序，但被警方发现，将洛法罗和技术员逮捕法办。

在日益激烈的商业竞争中，一些人发现计算机病毒还是打击竞争对手的有力武器。因此，想方设法把计算机病毒输入到对手的计算机系统内，使其公司的重要商务信息一夜之间面目全非。有许多软件公司耗费大量人力、时间和资金推出新的软件，指望借此发一笔横财。没想到，新软件刚一上市，专门针对它的病毒早已“守株待兔”地等在那里了。结果导致软件销量大降，经济遭受严重损失。

我国在这场世界性的计算机病毒灾难中也未能幸免，