当代

滔天大罪恶

刘喜峰 曲铁夫等／编著

哈尔滨出版社

当代弥天大罪恶

刘喜峰　曲铁夫　李英荔　张东梅　周志兰　编著

哈尔滨出版社

图书在版编目(CIP)数据

当代弥天大罪恶/刘喜峰等编著. -哈尔滨:哈尔滨出版社,2000

ISBN 7-80639-267-X

Ⅰ.当… Ⅱ.刘… Ⅲ.纪实文学-作品集-中国-当代 Ⅳ.I25

中国版本图书馆 CIP 数据核字(1999)第 74164 号

当代弥天大罪恶

作者 / 刘喜峰 曲铁夫 李英荔 张东梅 周志兰
责编 / 戴淮明
封面 / 杨群
版式 / 张吉
出版 / 哈尔滨出版社
地址 / 哈尔滨市南岗区贵新街 170 号
制版 / 黑龙江省教委印刷厂
印刷 / 黑龙江省教委印刷厂
发行 / 全国新华书店经销
开本 / 850×1168 毫米 1/32
印张 / 12
字数 / 290 千字
插页 / 2
版次 / 1999 年 12 月第 1 版
印次 / 2000 年 2 月第 1 次印刷
印数 / 1～6000 册
书号 / ISBN 7-80639-267-X/I·61
定价 / 18.00 元

如发现印、装质量问题,请与本厂质量科联系调换。

地址:哈尔滨市南岗区和兴路 147 号 邮编:150080

- 冷血杀手档案
- 海匪 空难 大爆炸
- 绑架与劫持
- 色情犯罪狂潮
- 高科技高智能犯罪
- 毒品——白色瘟疫在蔓延
- 人类肌体的癌细胞——黑社会
- 国际大走私
- 超级诈骗大要案
- 邪恶教派覆灭记

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

1. 高科技智能犯罪

高科技的发展，极大地促进了社会发展的进程，但是人们在享用高科技成果的同时，又不能不在感叹中精心设立另一道防线。因为高科技的发展，也为高智能犯罪的滋生提供了温床。

一、本世纪最大的一场计算机“瘟疫”的制造者

1988年11月2日傍晚，美国纽约州康奈尔大学的计算机屏幕上忽闪忽闪地出现一个来历不明的小程序，该计算机管理中心的值班人员发现这是一个从未见过的现象，计算机在它的作用下减速、停顿、乃至瘫痪。几小时后，全美各地的计算机纷纷遭到这个小“蠕虫”病毒的威胁，它在全美国网络内纵横出入，一时间，使数千台计算机变成废物。制造这场本世纪最大的计算机“瘟疫”的竟是莽撞不懂事的青少年罗伯特·莫里斯。

计算机里爬出的“蠕虫”

1988年11月2日，是一个令大部分美国计算机科技人员永远难忘的日子。

美国东部标准时间下午5点刚过，康奈尔大学计算机系统突然变得比以前慢了许多。正在使用计算机系统进行计算的科研人员立刻就此事向计算机系统管理中心发出咨询，因为康奈尔大学当时采用的是当时美国乃至全世界都是最先进的计算机系统，在一般情况下，即使系统连接的终端机同时起用，也不会给计算机造成太大的负担。其实管理中心的管理工作值班员已经发现了这个从来没有发生过的现象，并已经着手进行检测这个被称作“蠕虫”的病毒。几分钟后，计算机系统专用检测软件就找出了系统速度严重下降的原因：系统内多了一段能够快速自我复制、并且占用系统资源空间堵塞系统通讯通道的一段小程序(这段小程序后来被计算机科学家们称作“蠕虫”)。值班员发现这段程序后，立刻对该程序进行分析，分析的结果十分令人沮丧，由于这段程序设计的精巧使其具有快速传播和自我复制的能力，很可能已经传播到了与康奈尔大学相联接的其它计算机网络。值班员立刻把这个十万火急的情况向系统管理中心报告，并且向联邦调查局报案。

果然，时间不到晚上 9 点，康奈尔大学获悉位于加利福尼亚的斯坦福大学和著名的智囊机构兰德的计算机系统都出现了蠕虫。紧接着，晚上 10 点，加利福尼亚大学伯克利分校的计算机系统发现蠕虫，并受到其严重危害。晚上 11 点，麻省理工学院人工智能实验室找到蠕虫。11 点半，戴维斯和圣地亚哥的加利福尼亚大学、加利福尼亚州的劳伦斯·里福莫尔实验室、位于加利福尼亚州的美国国家航空航天局计算机网络系统被蠕虫传染，陆军弹道研究实验室也发现蠕虫。

危害还在延续。

次日凌晨 1 点，15 台 Arpanet 网络（我们今天见到的英特网的前身）的主机报告发现蠕虫。

2 点，哈佛大学检测出蠕虫。

3 点半，蠕虫入侵麻省理工学院计算机中心。

4 点，由于蠕虫堵塞信息通道，造成蠕虫的传播速度变慢，但也大约有 1000 台主机被蠕虫击中。

5 点一刻，宾夕法尼亚州的匹兹堡大学报告发现蠕虫。

3 日晨，当人们走到自己的计算机面前，发现的是令他们目瞪口呆的事实，他们的计算机已经基本无法运转了。

蠕虫案件立刻轰动了全世界！全球的新闻媒介由此刮起了报道计算机病毒的旋风。

大约在 2 日晚 11 点，也就是发现第一个蠕虫之后 6 个小时，联邦调查局已经意识到这将是一场最为严重的计算机犯罪案，调查局有关人员立即赶赴岗位，一个由联邦调查局最干练的警探和纽约州最能干的计算机系统分析专家组成的特别侦破小组已经成立，并开始了一项最为特别的侦破工作。

一张全美计算机系统网络图已经展开在警探和计算机专家面前。

发现蠕虫的消息不断传来，并且发现蠕虫的地点呈辐射状不断地扩展开来。特别侦破小组认定，蠕虫的发源点就在这个辐射网的中心：康奈尔大学。

此为试读，需要完整PDF请访问：www.ertongbook.com

立刻康奈尔大学计算机系统在11月2日中午12时到下午3时之间上机的所有用户名单传到了侦破小组。在康奈尔大学计算机科学系的配合下，疑点逐渐集中到了该系研究生罗伯特·莫里斯身上。

11月3日晨，睡眼惺松的莫里斯从床上被叫起来。

令人吃惊的是，莫里斯的父亲竟是纽约州计算机系统安全协会的主席！聪明过人的莫里斯在他20岁那年就考入康奈尔大学计算机科学系，并且对计算机安全产生了浓厚的兴趣，在这方面还颇有些研究，当然，他的成果是十分显赫的，不过只是没有产生正面的效应。

莫里斯研制的计算机蠕虫是一小段程序，它采用截取口令字，并在系统中试图做非法动作的方式直接攻击计算机。蠕虫与一般的计算机病毒不同，它不采用将自身拷贝附加到其它程序中的方式来复制自己。蠕虫一般由许多代码模块构成，欲将其隐藏在操作系统的文件中不大可能，因为它比较大。

蠕虫在进入计算机网络后，利用空闲的处理器测定网络中的计算机跨度。蠕虫程序由许多段构成，在其主段的控制下，蠕虫的某个段运行在单独的计算机上。蠕虫典型的传播方式是采用网络链或电子邮件方式由一台计算机传播到另一台计算机。这不同于病毒对文件的操作系统的感染。计算机系统把需要运算的数据都存放在内存区内，蠕虫可以用重写某个特定内存区的方法来得到对正在运行的内存区数据进行破坏的目的，在蠕虫运行中也可以破坏程序，蠕虫通常造成的后果是系统崩溃。

蠕虫的作乱通常是借助于系统的缺陷，为了说明莫里斯编写的蠕虫工作原理，先介绍一下莫里斯蠕虫所攻击的Arpanet网络的情况。

莫里斯蠕虫攻击的Arpanet网络是为了使计算机专家能够共享电子信息、程序和数据面设计的。因为该网络是一个通用的科学研究工具，所以通过简单的口令字例即可进行读取。Arpanet网络依据容易理解的操作指令运行，并能用命令使之与其他网络拼接。

1983年Arpznet网络分裂为两个网络。一个是Milnet网络，它

用于密级较高的军事通讯，但不涉及极密的军事信息。在莫里斯蠕虫事件中，该网络发言人承认，附加到Arpanet网络和Mil－net网络的非保密部分的几台主机被蠕虫击中。第二个网络是环绕主网联结着数百个民用网络的大网。

在莫里斯蠕虫事件中，有报告报道，在该网络中有300多台计算机被击中，涉及到网络中的大学、医院和研究中心的计算机，其中包括海军研究实验室、宇航局的Ame研究中心、SRI等著名机构。

剖析莫里斯蠕虫程序的计算机专家声称：莫里斯蠕虫程序编程技巧非凡，它利用了Arpanet网的三个安全规则。在莫里斯蠕虫事件中，有数台计算机幸免于难，因为其系统管理人员重写了有关规则的安全程序。

莫里斯蠕虫具有其特殊的工作原则，它窃取口令字，而后伪装成一个合法用户拷贝自身发送到远处的另一计算机中。结果导致蠕虫不受控制地疯狂拷贝，致使英特网计算机通讯网络的10%约6000多台计算机被传染并遭破坏。

莫里斯的程序诡诈而且复杂。此程序长达6万字节，它可以对UNIX操作系统中经过复杂加密处理的口令字进行译码，利用口令字将自己伪装成合法用户。康奈尔大学的负责人说，他们在莫里斯的计算机文件中发现了一张口令字表，它和从网络中的蠕虫中找到的口令字表相像。

根据专家们分析，蠕虫是利用了信息发送程序Sendmail(也称电子邮件)蒙骗计算机的安全机构混入计算机的，而后蠕虫隐藏在内存中，接着它产生一个程序，被该程序命令攻击的计算机能够产生特殊的加过密的口令字文件，利用口令字蠕虫可以混入其它计算机。使用美国伯克利大学编写的UNIX操作系统的计算机系统最容易遭受攻击。

蠕虫利用UNIX程序接触计算机，被认为是一个合法的E—mail信息，计算机打开其E—mail通道，允许蠕虫进入计算机。事实上，蠕虫是由可执行代码构成的程序，就像一个合法的用户调试一个

UNIX 程序那样。

每个加密的蠕虫的口令字与计算机的各个合法用户口令字相比较时，蠕虫记住严格相符合的那些口令字。在计算机的 3000 多个口令字中，蠕虫可得到 20 个。这些口令字之一可以读写系统用户的数据。在 UNIX 操作系统环境中，系统用户具有读写被保护的数据表和文件的特权，可以读写网络中的其它计算机，具有通过计算机系统读、写、删除文件的能力。此时，蠕虫通过窃取到的系统用户的特权，可以传播蠕虫自身到网络中的其它计算机，它可以对数据和程序文件做更严重的破坏动作。但是，莫里斯蠕虫没有做，惟一感受到的损害是计算机合法程序的处理速度显著变慢。由此可见，莫里斯设计蠕虫时，似乎没有使之具有毁灭性的意图。

根据莫里斯朋友的介绍，第一个被蠕虫击中的目标是麻省理工学院的一台计算机。当时，莫里斯本人在纽约的康奈尔大学他的计算机上使用了远程控制。远程控制是英特网络最有用的特征之一。蠕虫程序具有一种机制，它可以隐藏蠕虫的入侵源点。蠕虫程序自身的全部拷贝作为信息被周期性地发送出，并且在加利福尼亚大学的伯克利分校的计算机上发现了这些信息，这意味着蠕虫已经击中该计算机。

当莫里斯准备检查他的程序的进展时，他发现网络已经过载。他自己也遇到了麻烦，不能读取监控器，也不能中止他的程序。他马上请求在哈佛大学的朋友在英特网上发出报警和指示如何阻止蠕虫。莫里斯的朋友用技术术语发出了一则简短信息。但是，这些信息出现在模糊的电子公告牌上，因为网络严重过载，到处如此，只有很少的计算机用户收到这一信息。被蠕虫击中的哈佛大学一位专家报告说，当蠕虫击中他们学院时，它成了热门话题，引起了恐慌，人们纷纷议论，蠕虫是如何工作的？怎样才能杀死它们？蠕虫是 1988 年 11 月 3 日早晨入侵我们的系统的。我们的系统管理员和工作人员早晨做的第一件事情是按照惯例读取电子邮件信息。他们发现了有关蠕虫的报警信息。其中一些奇怪文件的存在表示系统中有一个或

多个蠕虫，以及如何制服蠕虫。

系统管理员迅速查出了一个正在运行的 UNIX 外壳程序，它与终端不相联系，系统管理员发出了杀毒命令，杀死了第一只蠕虫。

大约一小时后，系统管理员在终端上看到了第二个蠕虫出现的新信息和报警。此时，英特网络已处于一片慌乱之中，建议系统管理员们关闭电子邮件或者将机器同网络脱开。幸而，系统管理员继续监视我们的 UNIX 系统并没有脱网。不久，他们收到了由伯度大学系统员编写的蠕虫治疗程序。这个程序使蠕虫去调用和写入一个空文件，从而消除掉蠕虫的部分代码，以阻止蠕虫通过系统继续传播。蠕虫使学院计算机运行迟缓，为了检测和消除蠕虫花费了系统管理员的一个工作日（大约 120 美元）。

蠕虫的大范围蔓延，促使加利福尼亚大学伯克利分校的 UNIX 操作系统研究室重新分析他们的系统，改写了系统中的错误，关闭了 UNIX 系统 debug 状态，改写了“手指”，使它做阵列边界检查，这使非法入侵者再也不能利用蠕虫程序将自己的代码重写内存的内容。

他受到审判又受到尊崇

在莫里斯受审之前和审判中，新闻媒介对莫里斯的情况做了大量的夸张报道。某些人认为，受害网络是传送敏感数据和保密数据的，另一些人声称蠕虫损坏了珍贵的研究数据。可能最为夸张的是有关蠕虫造成损失的评估报告。

计算机病毒协会的麦克报告说，蠕虫引起的损失大约为 9600 万美元。

哈佛大学的斯多夫认为损失不超过 100 万美元。

伯度大学的吉里估计损失约 20 万美元。

在审判中，几位起诉人提出了修复受害系统花费数值。某些数值似乎太高了。熟悉内情的人认为吉里的估计比较合理，损失总值约 20 万美元的估计是可以接受的。

对莫里斯的审判在一些不懂得计算机的陪审团的陪审下进行，

审判过程曾出现过一些波折，因为法官中有一些相当倾向于莫里斯，并对其行为表示同情。法庭上，莫里斯认为自己的行为属于过失性过错，并表示道歉，他的父亲则认为这是“莽撞不懂事少年的行为”。最后莫里斯被判罚 10000 美元和一定时间的公益服务。

在如何评价莫里斯蠕虫造成的危险后果的问题上，美国的计算机科学团体发生了分裂。一些曾经与蠕虫日夜奋战的计算机管理人员表示了广泛的愤怒。对许多学者和研究人员来讲，蠕虫是一场灾难。它消耗了宝贵的工作时间，增加了额外负担；莫里斯还遭到了使用受害网络的一些科学家的非难，蠕虫延误了他们的研究进度。

但是，一些计算机安全专家认为：蠕虫是计算机潜在的易受攻击的最重要的证明。如果蠕虫的传播促使计算机主人采取措施防御未来的攻击，那蠕虫的后果是极为有益的。另一些人则认为：加强计算机的安全措施可能损害国家的经济或者促使入侵者设计出针对计算机网络的更新的有效的软件。

莫里斯由于使英特网崩溃，已成为最著名的攻击者。他受到法庭的审判，同时又受到一些人的尊崇。由于他的能力，莫里斯被哈佛大学的阿肯中心授予“超级用户”的特权，允许使用该中心所有的计算机资源。

由此可见计算机攻击者具有双重人格。一方面是国家的不可多得的人才，同时又是令国家头痛的人物。未来信息战时代，计算机病毒将被人作为武器，将来有一天，在美国计算机病毒战的专家行列中出现莫里斯，恐怕不是无端的揣测。

二、防不胜防的网上黄潮

信息时代已经来临，我们每天都在生产信息，而且将这些信息传给全世界的人们，20 年前这些都是不可能的。今天，计算机技术和通信技术的高速发展，尤其是近年来信息高速公路的建成和高速扩展，使我们能够实现信息的广泛传播和采纳。然而，信息的产生是随

心所欲的，信息的传播更是泥沙俱下、鱼目混珠，信息在很大程度上没有受到有效限制。现在全球采取对信息的监控基本有两种方式，一种是以美国为代表的电子技术监控，即在信息通道安设一个信息关卡，对包含黄色或暴力的图片文字进行处理，一旦发现，立即采取相应的措施，最近推出 V 芯片即安装在电视机上的信息关卡，据称能有效地控制黄色或暴力的图片显示于电视屏幕上。另一种方式是以中国为代表的警察监控，以强大的法律和警察职能对制黄贩黄进行严厉的打击来实现信息监控功能。无能是哪种方式，都有一种良好的愿望。相信在不远的将来，黄色和暴力将从信息通道中消失。

美国洛杉矶警察局最初接到了不满 15 岁的马克的报案，称他的计算机在访问一些站点时，总是收到一些以电子邮件方式传来的黄色图片，警方接到报案后，立即组织了一个专门小组着手此案的侦破工作。破案小组来到马克的计算机前，年轻人开始访问其中一个站点。

在登录了自己的口令后，很快就进入了对方的计算机系统。站点的第一个反应是出现了一幅画面：一个裸体女人的彩色图片，并且告诉马克只要敲一下回车键就可将这幅图片下载到自己的计算机里，警察记下了这个站点的地址，通过警察局的计算机中心很快就查出这个站点属于另一名年轻人：雷尔。

雷尔以“传播有害媒体毒害未成年人”的罪名被起诉。在未开庭之前，警方发现了一张计算机软盘。上面有不少年轻女孩的色情图片，都没有标明年龄，于是雷尔又增加了一条罪名：色情引诱未成年人。警察没收了雷尔的价值 3000 多美元的计算机系统。

后来的调查表明，雷尔的色情图片并非他自己制作的，而是从一个不知名的 BBS 站传来的，而雷尔将这些图片传播出去也完全是出于偶然。

法庭上雷尔这样陈述道：“我觉得我有权利告诉人们我的 BBS 计算机上有些什么东西，我不敢保证我肯定会阅读所有的电子邮件，但我想让我的访问者知道他有读这些文件的机会。很多警察对计算

此为试读，需要完整PDF请访问：www.ertongbook.com