

数字化犯罪

〔英〕 尼尔·巴雷特 著

郝海洋 译

辽宁教育出版社

1998年·沈阳

版权合同登记：图字 06-1998-186 号

图书在版编目 (CIP) 数据

数字化犯罪/[英] 巴雷特著; 郝海洋译.- 沈阳: 辽宁教育出版社, 1998.9

ISBN 7-5382-5308-4

I. 数… II. ①巴…②郝… III. 计算机应用-刑事犯罪
IV. D914

中国版本图书馆 CIP 数据核字 (98) 第 25560 号

Digital Crime

COPYRIGHT © 1998 By Neil Barrett,
KOGAN PAGE LTD

ALL RIGHTS RESERVED. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system, without permission, in writing, from the Publisher.

本书中文简体字版由英国 KOGAN PAGE 有限公司授权辽宁教育出版社独家出版, 未经出版者书面许可, 不得以任何方式复制或抄袭本书的任何部分。

版权所有, 翻印必究

辽宁教育出版社出版

(沈阳市和平区北一马路 108 号 邮政编码 110001)

朝阳新华印刷厂印刷

辽宁省新华书店发行

开本: 850 × 1168 毫米 1/32 字数: 153 千字 印张: 8 1/8 插页: 4

印数: 1—10 000 册

1998 年 9 月第 1 版

1998 年 9 月第 1 次印刷

责任编辑: 闵凯谭坚 责任校对: 王玲马慧

封面设计: 宋丹心

版式设计: 赵怡轩

定价: 16.00 元

序 言

介绍尼尔·巴雷特的第一本书，《计算机王国》（THE STATE OF CYBERNATION）时，我们形容写因特网方面的书就像用弓箭射下子弹那么难。果真如此，写一本关于未来数字化犯罪的书简直就像蒙住眼睛开飞机了。

复杂的因特网已经滋生出新一代犯罪分子，这需要全世界的执法机关提供迅速而有效的对策。律师和执法机构现在不得不学习有关的新技术和新法令，才能适应计算机犯罪的新形势。《数字化犯罪》这本书，对用新的证据技术侦破犯罪的必要性进行了论述，并着眼于那些因采用新技术而带来的不可避免的问题：因特网全球司法问题和如何举报计算机犯罪证据，使法律得到有效执行的问题。此外，



本书还论述人工智能的进步、计算机恐怖主义分子的威胁以及专家系统的作用。

《数字化犯罪》首先概括介绍发生于信息通讯领域的技术革命，以及犯罪分子利用这些成果来开发几乎不可侦破的犯罪手段，谋划他们的犯罪行为 and 销赃方法的情况。然后解释加密技术的发展以及计算能力的增强，使得破译在线犯罪分子的信息更加困难，同时使犯罪分子更有可能拦截并劫持合法信息进行要挟的复杂现状。

我同样会料想到电子货币的来临会招致信息高速公路发生史无前例规模的抢劫。抢劫犯穿着数字化伪装比穿戴面具更有效，因为他们不会留下任何指纹。大量无法追踪、完美无缺的电子伪币可以轻轻地按个键产生，银行如果不学习先进的技术，它们的前景难以预测，甚至可能破产。

《数字化犯罪》突出强调黑客和恐怖主义分子对高科技目标如机场造成的威胁，并强调需要与情报机构适当的合作和联系。公安部门已经开始使用数字情报方法，这会对解决重复性的犯罪行为产生重大影响。在下个世纪还没到来的时候，我希望反计算机犯罪机关和 NCIS 成为全国最大的警察机构。作为一个计算机王国的公民，我们需要这样的机构。

以本人的观点，这本书中一个最重要的信息是在大多数的情况下，不要求把安全破坏问题报告给公安部门。如果负有保密责任，你有必要通知客户安全破坏行为已经发生。客户有权利了解真相，如果不通知

你的客户，你就忽略了他们判断危险性以及采取适当措施的能力。如果不告诉你的客户，即使在破坏行为是不可预测的而且采用了最好的系统安全措施情况下，你也应对整个事件负全部的责任。同样的，如果使用不安全的通讯系统，例如发送电子邮件，你有责任保证你的用户知道并了解他们所冒的危险。

对尼尔·巴雷特对未来计算机犯罪引人入胜而又令人恐惧的描述，公司设计者、零售业者、银行家以及所有关心数据和数字资产安全性的人是必须要阅读的。通过写作这本书，作者不仅展示了蒙住眼睛开飞机的能力，而且还具备安全降落的本领。在打开你的计算机或上网之前，请首先阅读这本书。

尼克·洛克特大律师

1996 年 12 月

前言

随着计算机和通讯网络成为我们工作和生活中快速增长的一个方面，计算机在支持合法行为的同时，也在日益扶持非法行为，这已成为大家习以为常的事情了。

计算机，尤其是因特网，它们代表着当今人类社会所用过的最强大的一套全球性工具。这套工具使我们实现了全球范围的即时通讯，这样的通讯又使我们产生了一种日益增长的“大社会”概念：一个自由的、迅速成长进化的计算机王国（CYBERNATION）。她吸引了各种各样的人成为她的公民：从家庭主妇到总经理，从小学生到退休的老人，当然也不可避免地包括了犯罪分子。

因特网可被用来从事从简单的敲



诈到复杂的国际性洗钱等各种犯罪活动。计算机文件可用来存储加密甚至隐蔽的假账号（海外的远程主机只对这些账号作周期性的读取）；黄色照片可能会以几乎不可侦破的格式存储；计算机病毒、信用卡诈骗、软件程序的非法复制和黑客攻击，所有的这些非法行为已经成为计算机世界（WORLD OF CYBERSPACE）越来越猖獗的一面。

随着计算机的使用和因特网的流行，企业和个人越来越依赖电子数字技术；同时对有价值的部件，像内存或处理器的偷窃也变得越来越普遍。

虽然有这么多的问题，而且新闻媒介不断加以报道，但对处理这些犯罪行为，从查获、读取并分析一台可疑分子的微机或诈骗集团的计算机，到谨慎实施计算机、网络和其他的技术安全措施来防止这类犯罪，再到使用计算机为法庭提供证据，还没有一套完全得到理解和国际性认同的方法存在。不幸的是，随着计算机和全球性因特网的使用越来越普及，越来越多的个人通过计算机连线来选购商品，越来越多的机构日益对他们辛辛苦苦收集的数据具有依赖性，计算机犯罪也一定会继续激增。

对于警方和法院而言，计算机犯罪最大的问题是犯罪证据收集的困难性。不仅在英国，而且在整个欧洲和美国，即使是起诉最小的诈骗案，与计算机相关的证据也很难得到承认。多数没有专业知识的调查员已意识到技术复杂和查获错综复杂的计算机记录证据的操作困难，没有专业知识的法庭同样意识到判定这

种证据的真实性向他们提出了挑战。

随着计算标准和数据格式的成倍增加，获取并处理这样的电子数据证据变得非常困难，更不用提使它成为确凿证据的手段了。然而，在英国，对于计算机证据的获取及处理程序已有了一个草案，尽管它还没有得到英国调查机构的广泛支持。

在其他的方面也获得了一些进展。已经有几件成功的并众所周知的针对非法行为的起诉案，诸如恶意传播计算机病毒和以数字形式存储儿童色情资料案。这是良好的开端，并会引发更多的法律制订。美国有更进一步的进展，虽然他们还没有一个普遍接受的获取和处理证据方法提案，但他们已经建立了特别调查机构和有关的机构，而且这些机构已证实发挥了巨大的作用。

英国高级法院法官沃尔夫向民事司法厅提出的改进提议中，包括广泛推行计算机技术来准备和处理各种案件的建议，这些建议已被刑事犯罪厅采用。

因此，计算机对执法的影响，已远远地超出与证据收集相关的这一个方面。就像计算机可以被企业和犯罪分子使用一样，计算机也可以被警察、法院和其他调查机关使用，来协助分析复杂的诈骗交易，或查出隐藏在大量复杂证据之后的犯罪规律。从与计算机网络相关的高级加密和保护系统，到商店、银行和市中心的监视闭路电视，这些技术对防范措施的推广都有积极影响。

鉴于电子数字技术的应用在执法机关的潜力，有

两种对信息时代的不同反应不但是无效的，而且是非常错误的。第一种是对“新技术”置之不理。新技术会以难以想象的各种形式改变起诉和调查工作的过程，排斥数据开采（DATA MINING）和人工智能技术、闭路电视或信息技术应用，认为它们“不是真正的监察”的做法是不可原谅的；到本世纪末这种观点将会令人费解。

第二个错误是不加怀疑地迎接电子数字的未来，乐于把这样的技术当做发现、解决问题的万能之宝。犯罪分子和恐怖分子可以像当局一样容易地利用科学技术，甚至经常比当局拥有更多的资源和更高的技术，特别是从技术牟利的强烈欲望。

然而，除了这些纯粹犯罪行为之外，像黑客和其他形式的技术故意破坏分子也在更极端的冲突中找到了一席之地。无论是全副武装的地理政治冲突，还是恐怖主义或游击队的袭击活动，被称作“计算机大战”的信息战争已经迅速地成为至关重要的成功关键。以计算机为全国基础结构的美国、英国以及其他国家，其计算机基础结构已成为战争的最明显攻击目标，但是，这样的目标在不公开的内部攻击情况下也容易受到破坏。

计算机战争可帮助公司打败竞争对手，国家战胜他们的敌人，抗议者反对那些对他们有威胁的人。想象一下军事战略中或恐怖主义分子使用这些黑客技术的情况，那是令人心惊胆战的。

同时，就像我们所看到的，越来越多的计算机技术的

应用会带来极大的好处。这本书介绍的是安全性专家、警探和法院运用电子计算机技术打击犯罪分子的各种方法。书的技术性不是很强，涉及技术问题的讨论尽量加以解释。书是针对那些对技术知识不是很理解的读者而写的。尤其是关于黑客行为、病毒写作和相关的主题在此加以说明：本书不是黑客学员或计算机战争游击队的教科书，而是为那些对神奇的快速发展的计算机执法和计算机技术感兴趣的人而写的。

这本书在网络空间方面的内容是我早期作品《计算机王国》中有关内容的更加细致的描写。然而，那本书侧重于因特网对社会、政治和经济所产生的问题，这本书则讨论更广泛的技术范围，侧重于法律方面的问题（美国和英国），以及对相对无害的黑客攻击不可避免地发展成更险恶、危险，更恶意的计算机战争行为趋势的针对性研究。

本书围绕着信息时代计算机犯罪的各个方面来作结构安排，并提供有详细的技术注释。第1章讨论信息时代的主要组成部分，描述犯罪和侦察经常发生的计算机社会环境。第2章讲述那些直接针对这些信息时代组成部分（计算机，数据库，网络等等）的犯罪行为，展示那些最明显的犯罪行为发展成复杂犯罪的方法。

这些犯罪手段进一步地得到了发展。在第3章里，我们会对那些经常使用电子数据技术的犯罪行为加以讨论，从存储或传播计算机色情图像到因特网诈骗和计算机洗钱。因此，第2和第3章对信息时代犯罪行为的许多方面加以详细描述，这些犯罪行为对于当局



者是一个挑战。

第4章，我们会介绍法律和规章对这些新的电子数字犯罪挑战所作出的反应。在有些情况下，现行的法律得到了加强，而在其他的情况下，新的法律必须制定。新法律的实施，并不总是那么有成效，尤其是我们的法律制定人尚在努力地理解新技术所带来的危害与好处之中。

第5章，讨论法律在实际应用中的一些情况。因此，这一章将着重讨论使用信息时代的技术来帮助侦察、防止犯罪以及起诉犯罪分子。一旦侦破并逮捕了这些犯罪分子，起诉他们的司法过程就变得非常重要。在第5章里会概述从数字化计算机数据的证据问题到计算机化的法庭和法庭程序。

第6章，我们会讨论技术、司法和犯罪行为的发展方向。随着黑客潜在能力的增加和其他信息时代行为形成经济和政治势力范围甚至成为未来的战场，计算机犯罪行为不可避免地会演变成计算机冲突。

整个世界，各种军事、司法和政府机关都在试图定义和理解一个受益并依赖于以计算机、通讯和高智慧软件为数字基础的全球社会，一个不太受地理和现存司法真实世界限制的社会——“计算机社会”对他们所提出的紧急要求。在这本书里，我们会讨论这些要求和反应。我希望这本书会对计算机社会的治理做出贡献，能成为专业警探、安全人员或法律工作人员有用的和增进知识的工具，也为业余读者提供一本有趣的读物。

致 谢

就像以往一样，这本书得到了许多朋友和机构的帮助、鼓励和投入，使我受益匪浅。我很幸运能够同来自不同单位的专家们同台演说和辩论问题，这么多的专家，我无法在此一一列举。然而，我希望特别提出一个人：尼克·洛克特大律师。尼克和我曾经在一起讨论过许多书中谈到的观点，通过研究获得了对于计算机化攻击的危险性和法律依据的理解，尤其是“黑客”活动，一旦出现，计算机不仅会立即变成“受害者”，而且还会充当攻击活动的“帮凶”。尼克的贡献、建议和校正是无价的；然而，就像以往一样，任何遗留下来的错误全部由我负责。

KOGAN PAGE 出版公司的葛比·

菲斯 (GABI FACER) 和苏珊·波洛克 (SUSAN POLLOCK) 给了我极大的鼓励和支持, 保证了书的内容与我们预定的目标吻合。我还同时感谢我的有耐心的雇主公牛信息系统 (BULL INFORMATION SYSTEMS), 给我这么一个机会来同我的客户发掘讨论这些题目, 并且允许我来写作此书。

最后, 我要再一次感谢我的妻子和孩子对我的忠心支持和耐心。我们的工作间终于又从成堆的笔记、记录、剪贴和稿纸堆里解放出来, 重新变成一个可用于缝纫的房间了! 感谢大家。

尼尔·巴雷特

1996 年 11 月

目 录

序言

前言

致谢

● 1. 信息时代	1
简介	1
数字化犯罪	5
因特网	7
保护计算机系统	9
破坏计算机的安全性	11
● 2. 针对计算机的犯罪	19
计算机零部件偷窃	22
黑客和数字故意破坏	29
计算机感染	45
小结	60
● 3. 计算机扶持的犯罪	63
计算机色情	65
盗版软件销赃	74



因特网上的诈骗	85
电子洗钱	93
小结	100
● 4. 数字化犯罪和法律	103
有关黑客方面的法律	106
计算机色情图片的管理	123
信息时代的规章制度	132
小结	136
● 5. 信息时代的诉讼	138
用计算机来维护社会治安	140
数字化犯罪的侦察	151
计算机法庭学	162
计算机化的法庭	172
小结	174
● 6. 从计算机犯罪到计算机战争	176
计算机大战	177
计算机战争的战术和武器	183
数字化恐怖主义	191
小结	194
● 7. 结束语：维护计算机社会的治安	196
参考文献	201
注释	205
译者的话	242

1 信息时代

简 介

20 世纪末一定会成为信息时代。公司、机关、政府、教育以及个人生活从来没有像今天这样无法脱离极其普及的计算机、因特网及相关的领域^[2]。

从洗衣机到家庭计算机，从引擎控制器到航空管理，从气象预测到交互式计算机游戏，我们的周围到处都有我们所无法摆脱的电子计算机技术应用的存在。有时，计算机技术的应用很显而易见。比如，当我们使用自动提款机或用信用卡买东西的时候，



我们会很自然地想到这些交易在数据库里记录、分析、存档以备将来参考。

但有些时候，这些应用却不那么明显。开车经过一个城市，就会与交通管理系统、自动闭路电视监视器以及速度分析器打交道^[3]。有时，这些应用我们看不见，比如说，我们使用的电话和乘坐的火车，都需要许多计算机化的系统来协调。

计算机和信息网络，比如因特网，并非是信息时代中惟一重要的技术：以 CD-ROM 为基础的大容量存储系统，物美价廉、经久耐用的便携式彩色扫描仪和激光打印机；以数字化传导数据为基础的卫星和光纤通讯系统，所有这些，还有更多其他的尖端技术都被我们采用。并伴随着数学、工程和计算机科学的发展，使得我们能非常有效地应用这些尖端技术，这包括如下方面：专家系统和其他人工智能方法的开发；对于像无序理论、加密和随机或基因算法那样深奥概念更加深刻的理解；也许最重要的方面——随着这些数字电子奇迹变得越来越便宜，越来越重要，公众对这些技术的接受能力也在飞速增长。

由于当今计算机或数字控制器存在于我们现代生活当中的许多环节，为商店、公司企业或警察收集分析大量的数据提供了可能性，并且高速通讯网络可以让这些收集的数据迅速地传发到世界各地。当然这种能力带来了许多好处，同时也带来潜在的危机。最明显的是那些组织不仅仅因为他们的信息来源而增加了能力，而且越来越依赖于他们的信息来源。我们知道，