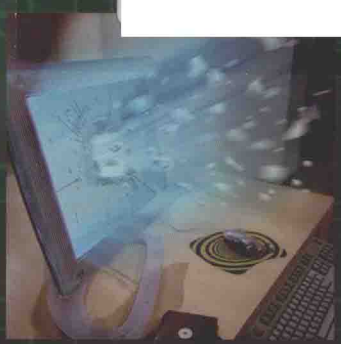
◆ 国家十二五规划图书 · **前沿科技聚焦**

丛书顾问 / 谢家麟　刘嘉麒

信息领域的幽灵

黑客

许榕生◎著



科学普及出版社
POPULAR SCIENCE PRESS

国家十二五规划图书·前沿科技聚焦

丛书顾问：谢家麟　刘嘉麒

信息时代的幽灵

黑　客

许榕生　著

科学普及出版社
·北　京·

图书在版编目（CIP）数据

信息时代的幽灵——黑客 / 许榕生著 . —北京 : 科学普及出版社，2015.8
（前沿科技聚焦）
ISBN 978-7-110-08926-2

Ⅰ. ①信… Ⅱ. ①许… Ⅲ. ①计算机网络—安全技术 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字 (2015) 第 169634 号

策划编辑	赵 晖 付万成
责任编辑	付万成 夏凤金
插 图	崔君旺
装帧设计	中文天地
责任校对	凌红霞
责任印制	张建农

出版发行	科学普及出版社
地 址	北京市海淀区中关村南大街16号
邮 编	100081
发行电话	010-62103130
传 真	010-62179148
网 址	http://www.cspbooks.com.cn

开 本	787mm × 1092mm 1/16
字 数	150千字
印 张	6
版 次	2015年9月第1版
印 次	2015年9月第1次印刷
印 刷	北京凯鑫彩色印刷有限公司
书 号	ISBN 978-7-110-08926-2 / TP·220
定 价	30.00元

（凡购买本社图书，如有缺页、倒页、脱页者，本社发行部负责调换）

序 言

本书写于2013—2014年，正值全球空前关注“黑客攻击”的时期。出版社希望有一本通俗的科普书介绍互联网的黑客。鉴于描写黑客的书已经不少，为了不再雷同，本书着重针对目前的热点问题，试图回答、分析“黑客攻击”这一争议不休的问题。本人不是黑客，但算是黑客技术的爱好者，涉足黑客防范领域20年，应该说认识不少黑客朋友，包括国外的一些黑客高手。作者希望用独立的观点来解读中国黑客成长的历史，书中尽可能列出各方面的材料，包括各国有关“中国黑客攻击”的报道，也包括中国政府阐明的立场态度。

按照流行的定义，早期的黑客是褒义的，指的是有电脑技术的人善于发现漏洞，乐于帮助他人。后来的“黑客”指的是攻击他人电脑达到炫耀自己才能或其他目的的人，现在黑客有正义的也有邪恶的，不过有人相信以后的黑客会重回“共享和平利用网络”的道路。本书将黑客视为信息时代的幽灵，一种奇妙的幽灵，它在互联网中游荡。

中国曾经期盼着互联网的到来，互联网在中国普及后，随即便成为网络攻击的最大受害者之一。但现在也被称为“黑客攻击的超级大国”，虽然，还没有人指责中国黑客要摧毁他国的基础设施、刻意进行网络破坏。世界各国正在积极参与国际网络安全建设，共同打击跨国网络刑事犯罪活动，中国也不例外。

渲染“中国黑客威胁论”只不过是某些国家为了强化“网络战力量”的图谋。

美国构建网络攻击力量的历史远远超过外界的想象，还在“中国黑客”出现之前，美国就已经将“网络战”应用到实际战争中了。例如，1991 年的海湾战争，通过植入对方电脑病毒，再在空袭前用遥控手段激活这些病毒，导致美空军飞临巴格达上空时，伊拉克防空系统已经瘫痪。

中国网民必须保持互联网的自律，尤其在国际发生重大事件、突发事件时，要及时引导民间黑客保持理性头脑，避免过激行为。特别是避免发生黑客们的自发性、群体性、集中性的过激行动。在打击对网络空间恶意破坏和应对网络战方面，做到有法可依、有法必依。中国不应该也不能够被扣上张牙舞爪的“黑客超级大国”帽子。

各国的未成年人都正面临着“黑客门”的危机。有一位六七岁的中国小女孩不经意听完黑客犯罪的故事对大人说：“我觉得黑客很了不起！”她的盲目崇拜提醒了我们，要让孩子们正确认识黑客。怎样让他（她）们不误入歧途，已经是未成年人思想道德教育的一个重要任务。孩子的好奇心、炫耀心比较强，如果对黑客盲目地向往和崇拜，一旦掌握了一些黑客技术就想试试，期望一举成名，这值得全社会的警惕。家长和老师应该从心理上“把好脉”，从技术上“占上风”，这样才能更好地跟孩子沟通、教育好孩子成为信息时代的新人。

本书按时间顺序，从互联网传到中国，黑客的涌现和演变，以及近年发生的“黑客攻击”潮，作者划分四个阶段，分六章来写。其中，第一章讲述黑客的由来，第六章针对网络战专题。书中介绍了中国网络安全研究的启动，以及网络安全人才的培养问题。信息技术发展迅速，人才是关键，书中作者力求体现“以人为本”的特点。黑客是善于“独马行空”，但也不乏聚会结伴，团队配合。正因为如此，每年的世界黑客大会能够聚集数千人来“朝拜”，而且，在世界各地相聚，或许有一天国际黑客大腕也要到我们中国来会合呢。

中国不必要被指责为“网络攻击源”，但中国决不可忽视黑客技术和网络战人才。今天，哪个国家不重视网络安全的技术与人才，那就是自废功力。那种认为有了经济后盾，或者储备了核武器、航空母舰就能成为军事强国的思维并不全面。当今是信息技术时代，网络战正在悄然到来，这与一百年前的甲午海战或第二次世界大战时期的军事交手形式绝对不一样。在全球范围也好，或者周边地区也好，想成为战无不胜的军事强国，网络空间的主导权必须要占据优势，也即必须具备信息技术的杀手锏以及掌握这些技术的各个层次人才。

目录

第一章 黑客的由来

黑客（hacker）最早出现在美国，早期的黑客是褒义的，指的是有电脑技术的人乐于帮助他人解决一些电脑网络的问题，不局限于老的模式，提倡“自由创新就是一切”。演变到后来的黑客指的是用软件攻击他人电脑，达到炫耀自己才能或其他目的的人。现在，“黑客”还常常是双重含义，有正义的，指的是计算机网络高手；也有邪恶的，指的破坏计算机网络系统的犯罪分子或敌对方。

黑客（Hacker）一词，最初曾指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员，逐渐区分为白帽、灰帽、黑帽等，其中黑帽（black hat）实际就是cracker。在媒体报道中，黑客一词常指那些软件骇客 (software cracker)，而与黑帽子相对的则是白帽子。

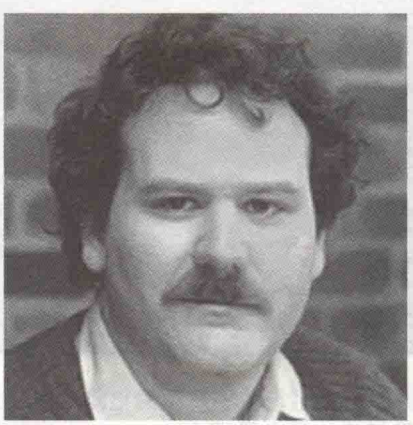
第一节 四位著名的黑客

在这里，我们盘点一下历史上典型的几位国际黑客，看看他们的人生轨迹：

1. 弗雷德·科恩（Fred Cohen）

计算机先驱者冯·诺伊曼在《复杂自动装置的理论及组识的进行》里，描述了病毒程序的蓝图。不过在当时，绝大部分的电脑专家都无法想象会有这种能自我繁殖的程序。1975 年，美国科普作家约翰·布鲁勒尔写了《震荡波骑士》一书，该书塑造了在信息社会中，计算机作为正义和邪恶双方斗争工具的故事，成为当年最佳畅销书之一。1977 年夏天，托马斯·捷·瑞安的科幻小说《P-1 的春天》再次成为美国的畅销书，作者在这本书中描写了可以在计算机中互相传染的病毒，病毒最后控制了 7000 台计算机，造成了一场灾难。虚拟科幻小说世界中的东西，在几年后不幸终于成为电脑使用者的噩梦。

“计算机病毒之父”的桂冠落到了弗雷德·科恩（Fred Cohen）的头上。1983 年，在南加州大学读研究生的弗雷德·科恩师从 RSA 加密算法的三位发明



“计算机病毒之父”弗雷德·科恩，2012 年游览北京名胜，作者（右）陪同。

1977 年夏天，托马斯·捷·瑞安的科幻小说《P–1 的春天》再次成为美国的畅销书，作者在这本书中描写了可以在计算机中互相传染的病毒，病毒最后控制了 7000 台计算机，造成了一场灾难。

者之一——罗纳德·阿德莱曼，在一天下午听阿德莱曼讲课时，一种寄生应用程序的理念突现在他的脑海中。这个理念与RSA算法并没有直接的关系，但著名的RSA这一名称是由加密算法的三位发明者利维斯特（R）、沙米尔（S）和阿德莱曼（A）的姓氏首字母组成。当年的11月3日，弗雷德在UNIX系统下编写了一个会自动复制、并在计算机间进行传染、从而引起系统死机的小程序。他将其方法和程序以论文形式发表，引起了轰动，被公认为是第一个真正通过实践让计算机病毒的概念具体成形的人，并将他编写的那段程序命名为“病毒（virus）”。20多年来，无数的公司和个人虽然付出了巨大的代价，然而，对于越来越多的病毒和蠕虫仍然没有简单的解决方案。人们对互联网的攻击很关注，但是几乎没人注意到病毒的起源，其原型的产生不是小孩子创造的，而是学术研究人员、系统管理员和那些老牌黑客。

弗雷德·科恩创造了计算机病毒，他又教人们如何战胜病毒。科恩认为，现在的互联网病毒的科学基础是在20世纪80年代建立的，其他都是自然而然形成的了。他说：“我们现在知道的那时都知道，我们现在看到的只是以前科学的工程解决方案。”弗雷德·科恩现在是加利福尼亚科学研究所的所长，除了研究、写书、教学外，他也接受技术质询，并着重于网络犯罪的调查取证。2012年9月第一次访问中国，应邀参加在北京召开的国际数字取证与调查研讨会做了《未来的数字取证的工具与方法》主题报告，并和夫人游览了故宫、长城等中国名胜。经佛雷德所长授权，中国人民公安大学、中国科学院及国家信息中心电子数据司法鉴定中心的年轻人共同翻译他的一本最新著作《数字法证证据鉴定》。

2. 凯文·米特尼克（Kevin Mitnick）

凯文·米特尼克被美国司法部称为“美国历史上被通缉的头号计算机罪犯”，他的所作所为被记录在两部好莱坞电影当中：*Takedown*《骇客追缉令》和*Freedom Downtime*《自由宕机时间》。他开始黑客生涯的起点是破解洛杉矶公交车打卡系统，并因此得以免费乘车。他还尝试盗打电话，侵入了Sun、Novell、摩托罗拉等公司的计算机系统。17岁那年，他第一次被捕。他还曾成功地进入了五角大楼并查看一些国防部文件。1995年被跟踪缉拿归案，这也是他最后一

凯文对一切秘密的东西、对解密电脑系统十分痴迷，为此可以放弃一切。他被人称为是“迷失在网络世界的小男孩”。美国法庭宣布他假释出狱，规定在 3 年内，不允许他接触任何数字设备……

次被捕。获刑 5 年零 8 个月的监禁之后，米尼克现在经营着一家计算机安全公司。凯文·米特尼克由于家庭环境的变迁导致其性格十分孤僻，但他玩电脑、入侵网络似乎仅仅是为了获得一种强大的权力，他所做的一切似乎都不是为了钱，也不仅仅是为了报复他人或社会。他对一切秘密的东西、对解密电脑系统十分痴迷，为此可以放弃一切，被称为："迷失在网络世界的小男孩"。美国法庭宣布他假释出狱，规定在 3 年内，不允许他接触任何数字设备，包括程控电话、手机和任何电脑。

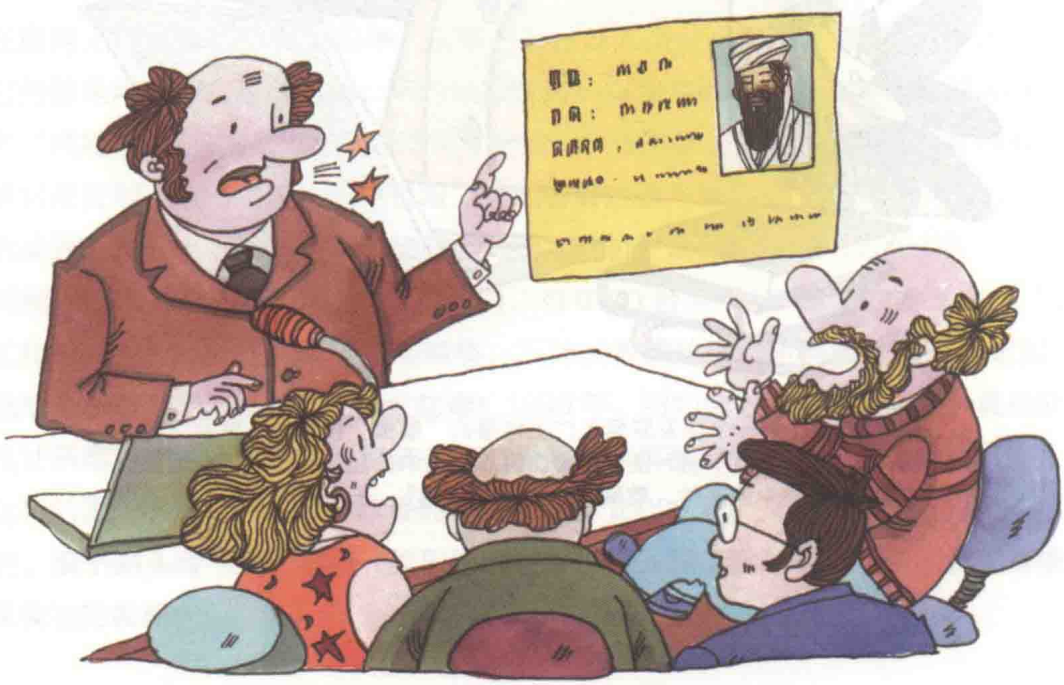
3. 罗特·莫里斯（Robert Morris. Jr.）

根据报道，20 世纪 60 年代的美国安全局（NSA）计算机专家罗伯特·莫里斯在家里给一项对弈游戏研究一种具有极大杀伤力的程序，以便成功地攻击对手。这使他的儿子罗特·莫里斯从小接触到计算机。12 岁的罗特就编出高质量的电脑程序，18 岁时，就具有在最负盛名的贝尔实验室和哈佛大学当过程序员的赫赫经历。1988 年 11 月，在美国康乃尔大学一年级读研究生的罗特，创建了第一个在互联网上广泛传播的蠕虫程序。互联网的管理人员首次发现网络有不明入侵者，它仿佛是网络中的超级间谍，不断地截取用户口令等网络中的文件，欺骗网络中的"哨兵"，长驱直入互联网中的用户电脑。入侵得手，立即反客为主，并闪电般地自我复制，抢占地盘。用户目瞪口呆地看着这些不请自来的神秘入侵者迅速扩大战果，充斥电脑内存，使电脑莫名其妙地死机。从美国东海岸到西海岸，互联网用户陷入一片恐慌。短短 12 小时内，有 6200 台采用 UNIX 操作系统的 SUN 工作站和 VAX 小型机瘫痪或半瘫痪，不计其数的数据和资料毁于这一夜之间。造成一场损失近亿美元的空前大劫难！1990 年，纽约地方法庭根据罗特·莫里斯设计病毒程序，造成包括国家航空和航天局、军事基地和主要大学的计算机停止运行的重大事故，判处他 3 年缓刑，罚款美金 10000 元，义务为社区服务 400 小时。浪子回头金不换，罗特·莫里斯现在担任麻省理工学院电脑科学和人工智能实验室的教授。

罗特创建了第一个在互联网上广泛传播的“蠕虫”程序。互联网的管理人员首次发现网络有不明入侵者，它仿佛是网络中的超级间谍，不断地截取用户口令等网络中的文件，欺骗网络中的“哨兵”，长驱直入互联网中的用户电脑……

4. 阿丹姆·罗尔（Adam Laurie）

2009 年到无锡报告的有一位国际蓝牙 SIG 的通信安全专家，他是来自英国的著名硬件黑客高手——阿丹姆·罗尔。此人到会那天，刚进五星级宾馆房间几分钟就转身出来对我们说，这家宾馆的门禁不安全，已经被他破解，并复制了一张通用的门禁卡，可以打开所有房间的门。实际上，他从小就是开锁能手，随身总是携带小工具，遇见门窗有锁的地方都要去试试手。但他从没有搞坏过别人家的锁，也从不会偷窃。反之，邻居家的锁坏了或钥匙丢了，就会请这位“好孩子”来帮着修。到了电子时代，出现了门禁、身份证之类的芯片技术，导致他又成了破解数字密码的高手。阿丹姆尤其擅长复制绿卡、电子护照之类的技术，他那年在无锡的报告题目就是告诉人们如何破解正在流行的电子护照漏洞，这种电子护照在各国旅行过海关时，可以无人干预地自动通关，像汽车上装了“电子缴费卡”方便过收费站一样。在报告现场阿丹姆借用一位美国人的



阿丹姆请大家不要对着屏幕照相，他随即把电脑上这本护照号码改成了 123456，把照片换成了本·拉登的肖像，这一连串的动作，引起听众一阵哄笑……

护照（嵌入芯片的），当场用扫描器接收芯片信息，并输入到他的电脑笔记本里。然后，由他的软件很快解析出芯片的所有信息内容，包括个人照片、姓名、出生年月日、护照号等，还显示出指纹、虹膜等图像。这些信息在他电脑里可以任意被修改、替换。这时，他请大家不要对着屏幕照相，随即把电脑上这本护照号码改成了 123456，把照片换成了本·拉登的肖像，这一连串的动作，引起听众一阵哄笑。但他严肃地告诉大家，他知道如何写回到护照去，一旦这样做就改了这本护照，事情就闹大了！

可以举出更多的例子来说明黑客的特征，他们所作所为与通常人们所熟悉的犯罪不同，所做的这一切似乎都不是完全为了钱，当然也不是仅仅为了报复他人或社会。但是，他们却像幽灵一样，出现在互联网时代的上空，划过一道道蓝光，给人一阵阵的惊吓。这一切也让人们思索他们的命运，他们的由来和他们身上的价值。

上面叙述的米特尼克作为一个计算机程序员，出身贫寒，据说后来开的是一辆旧车，住的也是他母亲的旧公寓。他也没有想过利用自己解密能力进入某些系统后，用窃取的重要情报来卖钱。对于 DEC 公司的指控，他说：“我从没有动过出售他们的软件来赚钱的念头。”当美国的检察官控告他损害了他进入的计算机时，他甚至流下了委屈的眼泪。莫里斯制作计算机病毒也不是有意去散布病毒，而是实验上的一个失误，当然，后果十分严重。至于佛雷德和阿丹姆则都是令人敬佩的学者、专家，是当今网络犯罪调查与国际网络反恐的高手。如果说他们四位值得我们尊敬或同情，但是，下面两位黑客“高手”就是另一回事了。

第二节 “计算机天才”的悲剧

1. 热罗姆·盖维耶尔（Jerome Kerviel）

热罗姆·盖维耶尔是一名法国银行的交易员，从 2007 年上半年开始在上级不知情的情况下从事违规交易，交易类型为衍生品市场中最基本的股指期

货。由于投入大量资金，市场颓势，盖维耶尔管理的账户出现巨额亏损。盖维耶尔使用隐蔽手段，瞒天过海，管理层直至半年后才发现这一重大问题。用法兰西银行行长的话说，盖维耶尔可谓“计算机天才”，居然通过了银行“5 道安全关”获得使用巨额资金的权限，涉及 49 亿欧元的巨额欺诈案。盖维耶尔遭警方拘捕之后，虽经过他的申诉后获释，但目前仍然在接受针对违背诚信、滥用电脑以及伪造文件等指控的正式调查。盖维耶尔的获释是有条件的，他的行动受到严格限制：比如不能进入交易室或交易所，也不能从事与金融市场有关的活动，并且需要每周到警察局报到，不可以在没有允许的情况下离开大巴黎区。

2. 亚伦 · 斯沃茨（Aaron Swartz）

亚伦 · 斯沃茨因涉嫌非法侵入麻省理工学院和 JSTOR（存储学术期刊的在线系统）被指控。2011 年 7 月，美国麻省检察官控告亚伦电脑欺诈，因为亚伦攻击连接麻省理工学院网络上的一台电脑，并下载约 400 万份学术论文。检察官认为亚伦非法持有来自受保护电脑的信息资料，且有意通过 P2P 网络向外散布，面临最高 35 年的牢狱之灾与 100 万美元的罚款。当该案正在认罪辩诉阶段，亚伦 · 斯沃茨却于 2013 年 1 月 11 日在其纽约布鲁克林的寓所内，用一根皮带上吊自杀，年仅 26 岁。

亚伦 12 岁时，写了第一个计算机程序；13 岁时，因建一个网站而获奖；14 岁，他成为万维网发明者蒂姆 · 伯纳斯 - 李领导的 W3C-RDF 核心工作小组的成员，设计了一种排版语言，并参与了其他许多计划。亚伦曾在哈佛大学就读一年。2000 年，他又用“维基”技术开发了一套百科全书的方案；2005 年，他开办的公司被并入美国最火的社交新闻网站（Reddit），当时亚伦还不到 26 岁。这样一位年少成名的计算机天才以自杀的方式走完了人生路，令人惋惜，亚伦的葬礼上蒂姆 · 伯纳斯 - 李为他致了悼词。

不论是热罗姆还是亚伦，他俩的手段似乎都不像恶毒的罪犯，但他们显然踩踏了法律的红线。只要互联网存在，就难以从根本上杜绝黑客犯罪。为了阻止这一高科技领域的犯罪现象，需要尽快制定有关国际法规，各国也应及时强调相应的法律，并设立公正的管理机构。加强网络法律教育非常关键，要让那些具有计