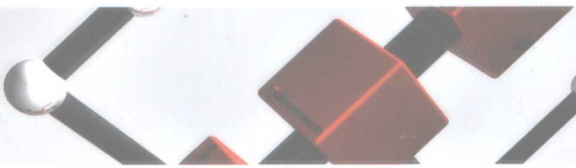
高技术犯罪调查手册

建立和管理高技术犯罪防范计划



（原书第二版）

〔英〕杰拉尔德·科瓦契奇
安迪·琼斯 著

吴 渝 万晓榆
李红波 陈 静 译

科学出版社
www.sciencep.com

高技术犯罪调查手册

——建立和管理高技术犯罪防范计划
（原书第二版）

〔英〕杰拉尔德·科瓦契奇
安迪·琼斯 著

吴 渝 万晓榆
李红波 陈 静 译

科学出版社

北京

图字：01-2008-2164

内 容 简 介

本书以全球信息环境下的高技术犯罪为背景，为以高技术犯罪调查员身份工作在全球信息环境中的人员提供全面的指南。帮助读者了解全球信息环境及其威胁，关注高技术案例及相关调查，建立并管理高技术犯罪调查团队和防范计划，以及拟定高技术犯罪调查职业规划。

本书适合作为高技术犯罪调查员的培训教材，也是政府官员、司法人员、计算机技术人员、企业管理人员的入门培训教材以及重要参考手册。本书适合学校教学和培训使用，尤其是信息安全、计算机专业、司法专业、企业管理专业等本科专业或应用型专业，包括作为工程硕士教材。

图书在版编目(CIP)数据

高技术犯罪调查手册：建立和管理高技术犯罪防范计划/(英)科瓦契奇(Kovacich, G. L.)等著；吴渝等译. —北京：科学出版社，2009
ISBN 978-7-03-024775-9

Ⅰ. 高… Ⅱ. ①科… ②吴… Ⅲ. 高技术-刑事犯罪-研究
Ⅳ. D914.04

中国版本图书馆 CIP 数据核字(2009)第 097818 号

责任编辑：顾英利 沈晓晶/责任校对：李奕萱
责任印制：钱玉芬/封面设计：耕者设计工作室

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

新 蕾 印 刷 厂 印刷

科学出版社发行 各地新华书店经销

*

2009 年 7 月第 一 版 开本：A5(890×1240)
2009 年 7 月第一次印刷 印张：15 7/8
印数：1—2 500 字数：476 000

定价：49.00 元

(如有印装质量问题，我社负责调换<明辉>)

如同第一版，我们将本书献给每个国家的安全、执法和调查领域的专业人员。他们毕生致力于保护他们的公司、社会、国家和这个世界，防止使用高技术的不法分子践踏人类的法律、伦理和道德。

译 者 序

目前，计算机安全形势极其严峻，由于涉及计算机、司法、企业管理、政府决策等不同领域，在学术界和工业界有较明显的分水岭。计算机出身的专家和技术人员主要研发安全硬件、软件或产品，司法工作者和政府方研究相关的司法和政策问题。相对而言，企业管理一方作为安全问题发生地、安全产品的主要使用者，整体表现较为被动，尤其是面对高技术犯罪行为时，在技术、人员、认识等方面都存在不同程度的欠缺。国内企业这一点表现更为明显，通常是遇到问题解决问题，没有事先建立健全的安全管理体系，也没有规范的操作流程，大都不得不依赖安全人员和司法人员来辅助工作。从国外发展趋势来看，计算机、司法、企业管理、政府决策领域几方联动程度越来越高，学科交叉性的安全工作者是社会亟需的人才，涉及以上几方的安全教材和手册、指南尤其受到社会欢迎。

本书定位为高技术犯罪调查的全面指南，不是定位在纯技术性书籍上。它围绕高技术犯罪调查问题，全面介绍了计算机、企业管理、司法和政府等相关方面的对策和处理，尤其是如何建立和管理高技术犯罪调查组，成就对此职业有兴趣者的成功之路。本书在安全、管理等交叉学科领域具有国际视野、先进性和应用价值，可以很好弥补我国在企业、政府、司法等安全领域普及方面的工作，也能够培养大量符合社会要求的交叉性安全人才。杰拉尔德·科瓦契奇博士和安迪·琼斯博士在安全领域有丰富的实践和教学经验，在美国政府、司法、企业、高校有丰富的相关任职经历，这保证了本书的学术价值和应用价值。本书第二版与第一版相比，有不少内容更新和调整，保证了本书的时效性。

本书以培养高技术犯罪调查员为目标之一，适合作为高技术犯罪调查员的培训教材，也是政府官员、司法人员、计算机技术人员、企业管理人员的入门培训教材以及重要参考手册。同时适合学校教学和培训使用，尤其适合信息安全、计算机专业、司法专业、企业管理专业等本科

专业或应用型专业，也可作为工程硕士的参考用书。

特别需要指出的是，本书附带了部分详细的参考资料，不但会使已经进入该行业的读者在实践中受益颇深，也是课程教学中很好的综合练习资料，或者是以大作业方式，或者是以课程设计和实践任务的方式。

同时，作者在写作中充满对高技术犯罪调查职业的热爱和期许，以及对高技术发展趋势的哲学思索，这让我们在翻译过程中也不由得备受鼓舞及触动，相信读者阅读完毕掩卷沉思的时候，同样可以感受到冷静、信心和希望！本书作者对中文译本的出版也表示了极大的兴趣和关注，这也是译者的工作动力之一，在此特别鸣谢！

全书主要包括 27 章和部分附录。吴渝、万晓榆、李红波、陈静组织并参加了本书的翻译、审校工作。参加翻译工作的研究生和教师还有张溢华、刘子睿、曾立梅、席海峰、陈安荣、周凯、吴焕政、肖开洲、王玮、刘文静等。

本书部分参考资料来自网上，原链接地址在本翻译版出版之际可能已经失效，建议读者用新闻标题搜索在因特网上保留的其他新闻网页。鉴于这些案例的经典性，这种搜索在大部分情况下是可行的。

本书的翻译工作得到了科学出版社的顾英利、沈晓晶等编辑和出版社海外合作部的大力支持，是他们的远见和积极高效的工作使得本书能够顺利与读者见面。

本书得到重庆邮电大学出版基金、国家自然科学基金、“973”前期研究计划专项课题、新世纪人才支持计划等多个经费来源的联合支持，特此致谢。

由于译者水平有限，译文中的不当之处在所难免。我们真诚地希望同行和读者朋友们不吝赐教，以期重印时修订改进，请将您的建议发往：spdic@163.com 或 wuyu@cqupt.edu.cn，我们将不胜感激！

译　者

2009 年 3 月

第二版序言

无论其身份是公司职员、小偷、诈骗犯、企业主管、帮派成员、职业杀手、少年犯、政府机关人员、国际黑客、恐怖分子，还是诸如此类的其他人员，当今社会的网络罪犯都比调查员做好了更充分的准备来应对其犯罪生涯中的各种挑战。这些犯罪分子利用计算机、传呼机、扫描仪、移动电话、传真机、彩色打印机等各种现代高技术设备来从事简单或复杂的犯罪。他们使用的最新方法、精密仪器和高技术设备妨碍、拖延或阻止了调查工作的开展。

本书第一版已经出版五年多了，糟糕的是这个世界的改变并不大，如今高技术犯罪人员的装备通常依然比执法人员和调查员更加精良。与全球高技术犯罪分子们相比，为了从事高技术相关的调查工作，许多联邦、州、郡和地方的执法部门和民间调查机构在获得高技术设备、方法并接受培训方面还是远远落后的。并且，如今这些网络罪犯们的触角确实已遍及全球。

在过去的五年甚至更长时间中，美国与其他发达国家或地区的安全和执法人员的地位已经有了极大的改变。这种变化是“9·11”事件引起的。全球性反恐战争使得高技术犯罪调查员原本有限的资源手段得到了进一步扩展。

如今，许多调查团体仍然没有资源手段来更新处理流程、过程和工具以便胜任此项工作。虽然已经有了一定改进，却仍然落后于需要。糟糕的是我们依然不断看见调查被拖延，在准备和提交调查报告时出现了耽搁，在精确收集和跟踪数据方面面临挑战，案件管理不善，对趋势统计的开发很差劲，数据的全面分析不足。调查员作为执法官员的一面强过作为调查员的一面。然而，调查员必须学习智能搜集和分析技术，这是当今高技术调查员的必备技能。

仍然有些管理者和监管人员高估了执法部门、政府部门和民间的

企业调查团体，他们缺少足够的专业知识，或者拿不定主意是否要使用目前调查和情报部门可得到的许多高技术自动工具和方法。此外，用令人理解和信服的方式向法庭和法官出示证据仍然是非常困难的。即便如此，我们还是看到这个领域的情况在改善。我们可能永远没有机会去炫耀完美的调查工具和环境，因为财务预算总是会首先考虑暴力型物理犯罪的调查工作。至少，那些暴力犯罪调查已经采用了高技术支持手段，而高技术取证对暴力犯罪调查带来了很大的改变。

既然我们已身处反恐战争时期，除了反恐之外的防御和调查工作以及一直存在的暴力犯罪正在得到最大的预算关注（它们本该如此）。由于可提供的资源手段有限，在阻止和调查其他类型的高技术犯罪方面，在执行高技术调查、培训和提供支持方面，有可能进展缓慢。管理工作会遭受到人手减少、经常性资金削减的压力，时常面临决策工作优先度的考验。为高技术犯罪调查员提供资金并装备他们迫切需要的最新资源手段，依然是一项值得关注的事，尤其是民众及领袖们意图打击贩毒、暴力犯罪、恐怖分子、黑帮的时候。当这些可以理解的压力出现时，很难充分确定这些高技术工具会对这些领域内的战斗有帮助，特别是因为它们与为企业提供调查服务有关。

我们经常看到，众多统计收集方法的升级手段只不过是一个简单的数据库或者报表应用程序的开发和应用。许多机构使用的最复杂的案件管理系统可以得到简化，使人不费吹灰之力就可以自动得到大量信息。目前制作的大多数应用软件都有非常好的使用指南，甚至可帮助那些最不熟悉高技术的高技术犯罪调查员去学习程序基础知识，开发满足日常事务所需的解决方案。这些工具目前被广泛使用，也将继续给调查员提供很好的帮助。这就是我们的世界，对调查高技术犯罪感兴趣的人们、高技术犯罪调查员们以及罪犯们必须工作的世界——全球信息社会。

此书是独一无二的，它的作者杰拉尔德·科瓦契奇博士和安迪·琼斯博士都是网络安全领域的经验丰富的安全专家、著名作家和讲师。此书不仅简要介绍了高技术犯罪领域，更重要的是，它是我发现的一本绝无仅有的主要目的不是介绍调查高技术犯罪，而是强调建立和管理高技

术犯罪调查团队的书。我强烈将此书推荐给：建立和管理高技术犯罪调查机构的管理人员，对高技术犯罪调查感兴趣并有志于从事高技术犯罪调查的人们。

霍华德·施密特
R&H 安全咨询公司，总裁兼首席执行官
美国白宫前网络安全顾问

给第一版的赞誉

高技术犯罪仍然是一个快速增长的全球性威胁。如果你有兴趣了解这种犯罪类型的基本知识并学习对抗它的专业工具和技术，那么推荐你阅读此书。联邦和地方政府机关的人员、企业管理人员应当阅读这本安全专家写的书，学习领会保护公共和私有资源免遭高技术攻击的必要策略和方法。我尤其希望联邦和地方政府机关的人员能够熟悉并遵循书中所描述的基本原则来保护纳税人的资源，意识到工作中的安全缺陷并加以纠正。希望企业管理人员能更好地增强安全意识，获得一些在生意中用于（或应该用于）保护用户/客户资源的防范措施。拜读此书之后，我的确更深刻地理解了银行和信用合作社所面临的困难，比如在保护我的钱财时。

评论者：罗伯特·斯特洛

美国华盛顿地区克林顿市

不论你是一位执法人员还是一位企业安全人员，在你即将迈入高技术犯罪调查领域之前，你不应当只是阅读一下这本书，而是要彻底消化它。在过去 16 年里，我在政府机构和企业都处理过调查工作，其中既有成功经验也经受过挫折，而且我还直接经历了各种不知情者面临的风险和后果。如果在 1981 年我第一次接触高技术犯罪调查工作时就有了《高技术犯罪调查手册》这类信息资源，我应该很乐意首先去学习知识而不是去亲身经历。此书非常宝贵，它不但教导执法人员要考虑私有产业的利益和立场，同时也教导企业安全人员如何去应对执法介入和成功起诉中的立场测试。如果你只想阅读一本关于高技术犯罪调查的书，那正是本书。不论你是执法部门或企业安全部门的私家调查员，还是一位刑法专业的学生，或者只是对本话题感兴趣，那么这本书就是你的首选——必读的一本书。

评论者：吉姆·布莱克

美国科罗拉多州

如果你想学习调查计算机犯罪的基本原则，那么必读此书。

评论者：安德鲁·布莱思博士

英国威尔士卡地夫市

要想获得更多关于《高技术犯罪调查手册》一书的评论，敬请访问www. amazon. com。

第一版序言

此书的确带给我惊奇。

最近，我和杰里·科瓦契奇在伦敦一家不错的酒吧喝上好的啤酒，他问我是否愿意为他和比尔·伯尼（Bill Boni）著的新书写篇序言。我当然感到万分荣幸，但并不因此而惊讶。我的惊讶是源自他的请求刚好发生在我遭遇一些身边事件之时。因为，你得知道我的两个同事正身陷计算机调查事件之中。

数年来，无论在单位内还是单位外，我一直有机会去跟踪那些“坏家伙”。而且，我发现在大部分案例中受害公司一方所遵循的工作流程多半是临时设置的。

我会问：“你们处理严重外部入侵行为的制度是什么?”

“呃……我们没有这样的制度。”这些首席安全官会如此回答。

“那好，你们自己的法律顾问如何及时处理这类事件?”

“他是一位相当菜的律师，搞不定这类事。你认为我们应该怎么办?”他们会问我。

这的确有点奇特，我跑到离家四千英里的地方来和杰里喝啤酒，又碰巧涉及我正在处理的两起事件。

在第一个案例中，一家大的金融机构发现其两周以来一直遭受相当严重的攻击。安全主管有一定的执法背景，也有一些实战经验。他立即着手进行内部调查，通过提高所有周边系统（防火墙、路由器等）、本地主机和应用软件的审计踪迹（audit trail）敏感度，搜集到了大量的原始审计数据。他们进行了全面分析以了解入侵者的技术，希望知道正在对付的这个攻击者的真正目标是什么，是何种水平。

第二步，他们发现入侵者已经取得了实质性进展，查看了一些非常敏感的公司文件，于是迅速捕获到一个 IP 地址，开始艰难地跟踪和确认入侵者的身份。安全主管凭借丰富的经验找到了访问链上的第一个因

特网服务商（ISP），以此跟踪到下一个路由中继。他在晚上访问了这个路由中继，查找到了入侵者的真实 IP 地址、真实姓名和真实物理地址。以上工作流程就解决了问题，既不用报警，也不需要向警方求助。

公司使用其他调查方式对嫌疑人进行了更广泛的背景调查，有99.999%的把握确认了这个作恶者。安全主管联络了一些同事，询问可否为了公司需要搞一次家访。这种举动和毫不含糊的措辞使入侵者确信：为了个人利益最好立即停止入侵。于是，这个并不微妙的策略起了作用。

问题就这样解决了，根本没有和警方打一点交道。无论你赞成或反对这些行动，都并不重要。公司筹划了在没有外人参与的情况下进行的内部调查，实施了调查计划，并在数天之内结束调查。最好的情况是仅有少数高层管理人员知道出现了问题，报纸或者网络上没有出现流言蜚语。在该公司每一个国内、国外的员工看来，一切生意运作都和平常一样。

第二个案例的处理有所不同。有个大型公司尽管有很多商业机密，但是其恰当的安全措施或者技术并不多。它并不像第一个案例那样是由电子传感器发现了非法的异常行为，而是因为收到一封质问其公司 IP 地址对外发起大量攻击的电子邮件才觉察到有恶意的内部人员。在一阵搜集之后，他们追踪到了一些日志记录，并且手工发现了一些他们不能解释的活动，那的确像公司内部人员在从事黑客行为。

公司匆忙地召开了会议。在会上，公司律师无法摆脱其固有的思维模式。他既不了解黑客的能力，也不明白公司所面临的技术局限。每个人却都赞同不与警方打交道，即使几乎不知道要采取什么步骤，他们还是想自己解决。

我帮他们制订了一个快速、简易且巧妙的计划。不久之后，我们就发现一个心怀不满的员工，该人曾供职于其正在攻击的公司。由于这涉及当地法律的敏感地带，他们没有采取我的如下建议：查封他的机器，对硬盘进行扇区级复制，并通过一些取证工具去查看他通过擦除、删除或其他伪装手段所隐藏的信息。我们决定解雇该员工，而人事部门对此感到震惊。他们告诉我们不能这样干的每一条书上所述的理由，而我们

认为必须这样做才能建立一个打击黑客的案例，杀鸡儆猴。

各方人员产生了强烈的受挫感，因为，相当明显地，没有高级管理人员考虑或讨论他们可能面临的问题。时间在缓慢地流失，当管理层在处理案件上达成共识时，至少三周的时间已经过去了。看上去一切都很平静，制度上也是正确的，但是超过 100MB 的信息已经通过 FTP（文件传输协议）传递给了其他公司，而管理层却仍在试图弄清发生了什么事情。

以上两种不同的处理方式都是令人不满意的：一种在于结果，另一种可能在于方法。这就是为什么《高技术犯罪调查手册》是信息安全和企业资产保护管理意识领域的无价之宝的原因。很少有公司慎重考虑过处理以上突发案件的措施。尽管我们很好地学习了如何应对飓风、洪水、火灾等不可抗力，但是在应对人的行为时，我们仍然处于起步探索阶段。

杰里和比尔提供给你的是对整个问题的精彩综述，包括我们目前生活的新信息时代环境，有谁对谁做了什么事情，如何保护信息财产的基本概览，以及对未来的展望。

据我所知，大多数公司不愿意强制执法，除非绝对有必要去做。大多数我认识的人都不相信警方会保密。公共关系是公司形象的重要组成部分，即使上上下下严格控制，也很难确保那些令公司难堪的事不被泄露。人们大都认为执法行为的技术水平低，缺乏知识，盲目无知，或在用落后的方法进行网络调查。此外，个人和企业在调查处理各种事情上有更大的回旋余地。由于执法方式面临法律程序性阻碍，如果在案件早期让警方介入，很可能导致调查失败。

网络犯罪涉及技术人员、安全管理人员、高级执行官、法律顾问，通常还有人事部门。由于环境性质的原因，分析和调查过程通常是非线性的，同时需要多线索并行开展调查。这是一个复杂的过程，必须制订计划。

不管你是否读了《高技术犯罪调查手册》的每个字，由此对这个新的信息时代有了更好的了解并把它用于你公司的工作程序中，这些并不重要。重要的是你建立和设置了适合公司及其发展目标的工作程序。

这本书也是一本“因特网犯罪入门手册”，适合安全专家、执法人员、管理者和任何对此有吸引力的话题感兴趣的人。没有比杰里·科瓦契奇和比尔·伯尼二人更好的向导了。他们对这个领域做出了巨大的贡献，我以有这样的朋友兼同行而感到自豪。

温·施瓦托

Infowar. com 公司总裁，作家

其最新著作《时基安全》（*Time Based Security*）为定义

组织机构的安全级别提供了量化方法和评价标准

前　言

《高技术犯罪调查手册》第二版进行了全面升级：一些章节进行了删除或合并，还加入了一些新的章节。这些新的章节涉及内容如下：

- 高技术全球性威胁
- 会谈和审讯
- 计算机取证，包括讲述如何建立和管理一个计算机取证实验室
- 高技术调查外包的利弊
- 恐怖主义及其对高技术调查的影响
- 如何成为高技术犯罪调查顾问

就像本书在2000年第一次出版时一样，如今高技术犯罪和其他非法活动在全球信息环境下仍在持续快速增长。这是由于在我们的工作和生活环境中，高技术在快速一体化和全球性普及，高技术犯罪的攻击目标正在变得更加多样化，并且这些目标比以前更易于受到更为复杂的威胁和攻击。

众多学院和大学不断开设涉及高技术各个方面的课程，近年就增加了信息安全、执法、调查等课程。尽管这些涉及高技术犯罪调查的课程并没有跟上快速发展的需求，但是也取得了一些进步，比如许多大学开设了计算机取证方面的课程。

如今，尽管许多执法部门和民间培训机构提供了针对先进方法和技术的基本指导和高级指导，在高技术犯罪调查方面的深度技术培训却很少，但这种情况也在慢慢得到改善。要得到更多的基本和更高级的指导，你必须关注私营部门及其主办的安全方面的国际会议。

像第一版一样，第二版的目标是使读者：

- 了解全球信息环境及其威胁
- 更关注高技术案例及其相关调查
- 能够形成建立并管理高技术犯罪调查团队的简要计划
- 建立高技术犯罪防范计划

- 制定高技术犯罪调查职业规划
- 基本了解高技术犯罪及其调查工作的未来发展

本书包括四部分共计 27 章，旨在对高技术犯罪调查职业的现在和未来进行基本概述。本书不是讲述“如何进行高技术犯罪调查”，尽管书中也对这个话题进行了概述。本书讲述的是如何以高技术犯罪调查员身份工作在全球信息环境中，建立和管理高技术犯罪调查计划。

本书非常适合于那些有意担任高技术犯罪调查员的人，或有意学习如何在商业或政府机构中与高技术犯罪作斗争的人。也希望此书能给经验丰富的老手们提供一些提示和启发，或至少是很愉快的阅读体验。

尽管仅仅只有非常少的高技术犯罪调查员被正式授予了这样（或近似）的职业身份，但毫无疑问的是世界上每个信息依赖型和步入信息时代的国家和企业中的私营和公共部门对训练有素、技术精湛的高技术犯罪调查员的需求正在增长。

我们无疑将有很长一段路要走。显然，一些计算机犯罪团伙仍然在使用微软 Windows ME 操作系统，而一些罪犯被传唤去使用封存在证据柜中的没收软件来运行他们的“500MHz 主频的新计算机”。

希望本书能激起人们对高技术犯罪调查员职业的关注和兴趣。如果我们要在 21 世纪取得成功，如果我们的工作生活依赖于全球信息网络（因特网，其他国际、国家和企业网络，全球通信系统），与信息安全专家相呼应的专业高技术犯罪调查员必须经过培训，使其具备知识和能力来保护这个全球信息环境不被那些在网上到处游荡、攻击受害人并逃避处罚的不法分子们侵害。

对于那些勇于接受挑战的人们，再次道一声：祝你们好运，猎捕成功！

杰拉尔德·科瓦契奇博士　　安迪·琼斯博士

美国华盛顿州惠德比岛　　英国英格兰伊普斯威奇

关于合著者变更的说明：威廉·伯尼（第一版的合著者）担任了摩托罗拉公司的首席信息安全官和公司副总裁，在过去几年里一直非常忙。安迪·琼斯博士是我的老朋友，也是我前一本书的合著者，他非常愿意接受挑战来合著此书，并为本书加入他丰富的经验。