中国刑事警察学院
教材建设专项资助项目

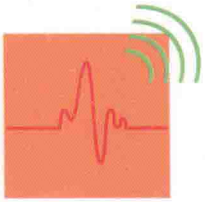
当代世界警务理论与侦查实务译丛
丛书主编　王世全　马玉生

CYBER CRIME INVESTIGATIONS

Bridging the Gaps Between Security Professionals, Law Enforcement,and Prosecutors

网络犯罪侦查

在安全专家、执法人员和检察官之间架起沟通的桥梁



[美] 安东尼·雷耶斯 Anthony Reyes
[美] 凯文·奥谢 Kevin O'Shea
[美] 吉姆·斯蒂尔 Jim Steele
[美] 乔恩·R. 汉森 Jon R. Hansen
[美] 凯普敦·本杰明·R. 吉恩 Captain Benjamin R. Jean
[美] 托马斯·拉尔夫 Thomas Ralph　著

李娜　等译

CPPSUP 中国人民公安大学出版社

中国刑事警察学院
教材建设专项资助项目

当代世界警务理论与侦查实务译丛
丛书主编　王世全　马玉生

CYBER CRIME INVESTIGATIONS

Bridging the Gaps Between Security Professionals,
Law Enforcement, and Prosecutors

网络犯罪侦查

在安全专家、执法人员和检察官之间架起沟通的桥梁

[美]　安东尼·雷耶斯　Anthony Reyes
[美]　凯文·奥谢　Kevin O'Shea
[美]　吉姆·斯蒂尔　Jim Steele
[美]　乔恩·R.汉森　Jon R. Hansen
[美]　凯普敦·本杰明·R.吉恩　Captain Benjamin R. Jean
[美]　托马斯·拉尔夫　Thomas Ralph　著

李娜　等译

中国人民公安大学出版社
·北　京·

图书在版编目（CIP）数据

网络犯罪侦查：在安全专家、执法人员和检察官之间架起沟通的桥梁 / [美] 雷耶斯等著；李娜等译. —北京：中国人民公安大学出版社，2015.6
（当代世界警务理论与侦查实务译丛）
ISBN 978-7-5653-2062-0
Ⅰ.①网… Ⅱ.①雷… ②李… Ⅲ.①互联网络—计算机犯罪—刑事侦查 Ⅳ.①D918
中国版本图书馆 CIP 数据核字（2014）第256945号

本书版权登记号：图字：01-2014-7851

网络犯罪侦查：在安全专家、执法人员和检察官之间架起沟通的桥梁

［美］ 安东尼·雷耶斯 Anthony Reyes　［美］ 凯文·奥谢 Kevin O'Shea
［美］ 吉姆·斯蒂尔 Jim Steele　［美］ 乔恩·R.汉森 Jon R. Hansen
［美］ 凯普敦·本杰明·R.吉恩 Captain Benjamin R. Jean
［美］ 托马斯·拉尔夫 Thomas Ralph 著

李娜 等译

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里
邮政编码：100038
经　　销：新华书店
印　　刷：北京通天印刷有限责任公司

版　　次：2015年6月第1版
印　　次：2015年6月第1次
印　　张：19
开　　本：787毫米×1092毫米　1/16
字　　数：354千字

书　　号：ISBN 978-7-5653-2062-0
定　　价：80.00元

网　　址：www.cppsup.com.cn　www.porclub.com.cn
电子邮箱：zbs@cppsup.com　zbs@cppsu.edu.cn

营销中心电话：010-83903254
读者服务部电话（门市）：010-83903257
警官读者俱乐部电话（网购、邮购）：010-83903253
教材分社电话：010-83903259

本社图书出现印装质量问题，由本社负责退换

网络犯罪侦查：在安全专家、执法人员和检察官之间架起沟通的桥梁

译者名单

李　娜　孙晓冬　肖　萍　许静文

序 一

习近平总书记在2014年中央外事工作会议上强调："认识世界发展大势，跟上时代潮流，是一个极为重要并且常做常新的课题。中国要发展，必须顺应世界发展潮流。要树立世界眼光、把握时代脉搏，要把当今世界的风云变幻看准、看清、看透，从林林总总的表象中发现本质，尤其要认清长远趋势。"2015年中央政法工作会议明确提出，要深入学习贯彻党的十八届四中全会精神，全面推进依法治国，推动政法工作向善于运用法治思维和法治方式转变、向着力解决深层次问题转变、向善于运用信息化手段转变、向更加开放转变。可以看到，开放、发展、合作的观念正在深刻影响着当代中国和中国的法治建设。

警察作为人类社会发展到一定阶段所共有的社会现象，既有一定的历史延续，也存在着国与国之间的横向联系。近二百年来，随着五次警务革命的潮起潮落，西方国家的警察科学研究日趋繁荣，学术成果硕果累累，形成了较为先进、完善的警察科学理论体系与操作模式。尽管西方国家与我国的社会制度、国情、治安状况不同，但是其百余年的警务革命和实践对我国警务工作的发展不无启示。作为人才培养的主阵地和科教强警的生力军，公安教育战线更应树立世界眼光，积极借鉴世界警

务理论发展成果，切实加强对事关公安工作全局性、前瞻性、规律性重大问题的研究，不断丰富具有中国特色的现代警务理论，努力为解决在警务实践中遇到的新情况、新问题提供有力支持。

为深入了解和借鉴国外先进的警务理论研究成果，推动现代警务理论研究和实践创新，更好地服务公安教育和公安实战，中国刑事警察学院组织开展了“当代世界警务理论与侦查实务译丛”的翻译出版工作。本译丛包括12本译著（其中英文版著作10种、德文版著作1种、俄文版著作1种），具有以下特点：一是原著作者普遍具有较高的研究水平和学术影响力。他们中有的是学术造诣精深的学者，有的是警务实战经验丰富的专家，其成果代表了相关专业领域的最新进展以及发展趋势，权威性强，学术水平高。二是在警务理论研究学派的选择上具有广泛性和代表性，包括了英美法系国家、大陆法系国家以及其他具有独特法律传统的国家等多个具有代表性的流派。本译丛内容的广泛性有助于全面客观地认识和借鉴具有代表性的国家在警务工作中的共性特色和个性魅力。三是具有很强的警务理论研究和实用价值。本译丛包括警务工作的诸多领域，涉及警务与执法、全球缉毒、刑事侦查、网络犯罪侦查、鞋印证据、实用爆炸现场调查、司法语言学、犯罪与恐怖主义、犯罪现场摄影技术等专业科技领域。这些成果贴近警务工作实际，对警务理论研究和实战应用具有重要的借鉴价值和指导意义。

“当代世界警务理论与侦查实务译丛”的付梓是中国刑事警察学院教材建设的重大推进，凝聚了有关方面和专家学者的辛勤付出，不仅填补了公安学和公安技术两个一级学科专业译著的空白，也为我国公安教

育训练工作、警务理论研究和公安实战应用带来了新理念和新方法。作为一名在公安教育战线工作了30多年的“老兵”，我很高兴为本译丛作序。冀望“当代世界警务理论与侦查实务译丛”的面世能够激发越来越多的公安院校和学者对世界警学名著引进与翻译的热情，能够对公安学和公安技术的学术研究有所推动，为公安工作和公安队伍建设提供更加有力的理论支持和智力保障。

是为序。

中国刑事警察学院党委书记、院长 王世全

2015年5月

序二

由中国刑事警察学院编译的“当代世界警务理论与侦查实务译丛”即将出版，邀我作序，我很高兴。中国刑事警察学院与我渊源极深，1960年至1962年期间，我曾经在民警干校任教，也就是中国刑事警察学院的前身。

近日收到书稿，认真阅读了这部译丛，不禁生出许多感慨，既被书中原著很多的新理念所触动，又感动于编译者的辛苦付出，于是迫不及待地拿起笔，翻出一些记忆，写下一些感受。

这部译丛收录的原著，大多是关注现场或者证据的，贴近实战，非常受用。这倒十分符合我从事刑事侦查工作多年的经验和认知。国内也好，国外也罢，关于刑事侦查的很多理念和实践往往是趋同的。记得2005年，我这个所谓“中国的福尔摩斯”和有“当代福尔摩斯”之称的美籍华裔专家李昌钰博士在中央电视台同做一档节目，我们的人生经历不同，遇到的案件不同，但我们对犯罪现场的重视和刑侦现场证据理论的推崇却高度一致。每到一个案件现场我常说的一句话是“现场，现场，还是现场，现场是破案的源泉”，我参与侦办的如“马加爵案”、“5·7”空难、“彭妙计案”等一系列重大要案的关键线索，无一例外

都源于对犯罪现场的缜密分析。

曾有人说，我有所谓的“超能力”，所以才能找到犯罪分子的蛛丝马迹，这当然是一句笑谈，如果说要找到一个途径去获得这所谓的“超能力”，我想那就是要坚持不断地学习。当今世界，国际合作日渐紧密，科技发展日新月异，刑事犯罪侦查也正面临着越来越大的挑战，只有经验是不够的，更不可能闷头过日子，必须要学习世界最前沿的科学理念，掌握最先进的侦查方法和技术，我们才能始终保持优势、先发制敌，让犯罪无处遁形。

本译丛严格地讲是一套教材，读者更多应该是有志于从事刑事侦查工作的同志，笔尖停留之处，我更想对你们说点什么，就算于书内容不妥，我想也算得题中之义。如何做一名合格的刑事侦查工作者，除了技术，除了学习，究竟还需要点什么？我想应该是对事业的忠诚，还有对生命的敬畏吧。每一件大案结案之际，我都不会有太多的轻松和愉悦，因为刑事侦查是以罪恶发生和人民群众生命财产安全被侵害为起点，那么结局就注定不会有什么完美可言。我们刑侦人所能做到的，就是尽早地发现真相，尽早地还世界一份清宁。真心地希望你们用心体味生命，热爱生活，做一个有血有肉、侠骨柔肠的神探。

“风雨多经人不老，关山初度路犹长。”本译丛的编译工作是在中国刑事警察学院65周年华诞之际启动的，65年栉风沐雨，65年薪火传承，中国刑事警察学院这所中国刑警的最高学府已桃李天下、硕果累累，作为老校友，我倍感骄傲和欣慰，同时感谢中国刑事警察学院领导和各位同仁多年来的关心和帮助。衷心希望中国刑事警察学院在这项工

作中有更多的新成果面世！祝愿中国刑事警察学院在建设国际一流刑警院校的新征程中取得新的更大的成绩！

是为序。

公安部首席特邀刑侦专家 乌国庆

2015年5月

译者说明

计算机网络始于美国，网络犯罪案件也始于美国，在办理网络犯罪案件方面，美国的理念也更先进，值得我们借鉴与学习。美国的法律非常健全，要求也相当严格，办理网络犯罪案件时如果程序出现问题，甚至是勘查工具或取证软件有问题，案件则很难胜诉，这正是我们应该学习的方面。

本书的思路非常务实，介绍了警察办理网络犯罪案件的整个过程，即从现场到取证，最终到法庭，并提出了在警察办理网络犯罪案件过程中新的理念和思路。本书不仅介绍办理网络犯罪案件的过程与思路，还着重说明警察在各个环节需要做什么、怎么做、注意什么，既顾全全局又注重细节。难能可贵的是，本书介绍了我国没有出现的网络犯罪案件形式，并提出了办理思路与方法。

本书用浅显的语言表达了深刻的内容，有助于读者的理解与掌握。

本书适合作为公安高等院校信息安全、网络犯罪侦查等专业的研究生、本科生、双学位学生的授课教材或教学参考书，也可以作为网络犯罪执法人员的参考书。

本书译者李娜负责全书的整体结构设计和内容统编，并翻译第1章、第3章、第4章、第7章、第8章、第10章、附录B、致辞、原著作者简介；译者孙晓冬翻译第5章；译者肖萍翻译第2章、第6章、第9章；译者许静文翻译附录A。中国刑事警察学院的秦玉海教授、汤艳君教授、刘晓丽教授审阅了全书内容，并提出很多宝贵意见；中国刑事警察学院的胡永吉老师对本书的完成给予了大力支持；中国刑事警察学院2010级本科生王明珠同学作为本书的第一位学生读者也提出了宝贵意见，在此一并表示衷心的感谢！

本书译者李娜在2002年本科毕业于大连外国语学院英语信息工程学院，2010年取得中国人民公安大学诉讼法专业的硕士学位。自2002年起在中国刑事警察学院任教，讲授过双语课程、“网络犯罪案件侦查专业英语”、“网络犯罪侦查”等课程，并发表包括英语论文在内的论文10余篇，具有扎实的英语功

底与业务基础。译者孙晓冬是中国刑事警察学院“网络犯罪侦查”课程的开创人之一，并为各个层次的学生讲授“网络犯罪侦查”等专业课程，在全国公安院校中享有盛誉。译者肖萍在中国刑事警察学院讲授“网络攻防”、“网站分析与构建”等课程，在网络攻防领域具有独到的见解。译者许静文本科毕业于大连外国语学院，2013年毕业于中国刑事警察学院侦查系诉讼法学专业，同年留校任教，具有扎实的英语功底和业务基础。

尽管本书译者付出了很多努力，但书中仍有不足之处，敬请读者提出宝贵意见！

2014年7月

第一作者和技术主编

Anthony Reyes是纽约市警察局一名退休的计算机犯罪组侦探。在受雇于纽约市警察局（New York Police Department，NYPD）的时候，他负责侦查计算机入侵、诈骗、身份盗窃、儿童性侵、知识产权盗窃和软件盗版案件。

Anthony Reyes是纽约市前州长George E. Pataki的网络安全专门工作组的候补成员（New York Governor George E. Pataki's Cyber-Security Task Force）。现在，他是高技术犯罪侦查协会（High Technology Crime Investigation Association）主席、美国国家司法研究所下的电子犯罪合作伙伴计划的教育和培训工作组（Education & Training Working Group Chair for the National Institute of Justice's Electronic Crime Partner Initiative）主席。Anthony也是《数字取证实践杂志》（Journal of Digital Forensic Practice）的副主编和《国际取证计算机科学杂志》（The International Journal of Forensic Computer Science）的主编。

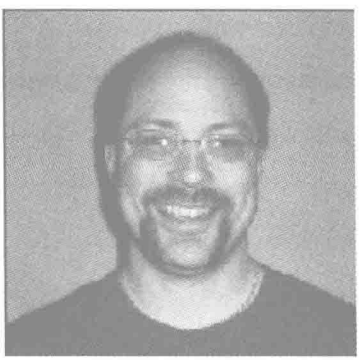
Anthony Reyes是一名副教授，同时也是华尔街的纽约电弧股份有限公司的首席执行官。他在IT企业有20年的工作经验。他为多家政府机构和大公司做计算机犯罪侦查、电子证据发现和计算机取证方面的培训。他还在全世界范围内做计算机犯罪侦查方面的报告。

Anthony Reyes编写了本书第1章、第4章、第5章。

作者简介

Kevin O′Shea现在是受雇于新罕布什尔州大学司法工作项目的国土安全和情报专家。O′Shea先生的这个职位的目的是支持工具和技术的实现，以及培训、辅助执法机构侦查涉及网络的犯罪。在近期的一个项目中，他是远程计算机取证检验技术培训项目的技术顾问和开发者，现在这个项目被新罕布什尔州采用。他还为“新罕布什尔州警察标准”与培训开发了计算机犯罪侦查课程。

Kevin O′Shea编写了本书的第2章、第7章，合作编写了第6章。



Jim Steele［注册信息系统安全师（Certified Information Systems Security Professiona，CISSP），微软认证系统工程师（Microsoft Certified System Engineer，MCSE）：安全，安全+］在安全、计算机取证、网络开发和管理领域拥有丰富的职业经验。在过去15年多的时间里，他在项目管理、系统管理、网络管理以及涉及公共安全和关键任务系统的企业安全管理中发挥了必不可少的作用。作为纽约市警察局“911”紧急中心的高级技术顾问，他为企业安全设计和管理多个系统；在2001年9月11日和2003年“大停电”事件中，他在现场执行支持工作。Jim还参加外国项目，如伦敦大城市警察的开发指挥自动化技术系统

（Communication，Command，Control and Intelligence Systems，C3I）项目，他在这个项目中是设计与建议组成员。Jim还是宾夕法尼亚大学和纽约消防局（Fire Department of New York，FDNY）的技术顾问。他从事各种网络安全领域的工作，还拥有操作系统、网络产品和技术的专业知识，这使他能够胜任现在的职位，即大型无线运营商的高级数字取证侦查员。他的职责范围包括工作站、服务器、PDA、手机和网络取证。他同时还是各个执法机构的联络员，包括美国特勤局和FBI。他的日常工作是侦查诈骗案件、员工操守案件和系统破坏案件。Jim是HTCC、纽约电子犯罪工作组（New York Electronic Crimes Task Force，NYECTF）、InfraGard和高科技犯罪侦查协会（High Technology Crime Investigation Association，HTCIA）的成员。

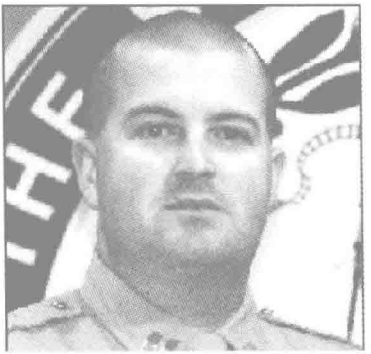
Jim Steele编写了本书的第9章。

Jon R. Hansen是AccessData的销售和业务开发部副总裁。他是计算机专家，拥有24年的计算机技术经验，包括网络安全、计算机取证、大型软件部署以及各种各样的硬件和软件平台的计算机培训。

他致力于制定和开发保护计算机信息、恢复丢失或忘记的密码以及获取取证图像的政策和技术。他在全世界范围内出席各种会议，在美国、墨西哥、巴西、英国、比利时、法国、荷兰、澳大利亚、新加坡、中国香港、韩国、日本和南非发表过讲演。

作为微软犹他州的前区域总监，他在很多公司出任顾问和联络官，包括微软、WordPerfect、莲花公司（Lotus Corporation）和数码电子公司（Digital Electronic Corporation，DEC）。

Jon R. Hansen编写了本书第10章。



Captain Benjamin R. Jean的全部执法生涯都在新罕布什尔州，从1992年开始在Deerfield警察局工作。现在他是新罕布什尔州警察标准与培训委员会的执法培训专家和培训局局长。Jean局长教授各种执法主题的课程，包括计算机犯罪侦查。他也是新罕布什尔州首席检察官的网络犯罪项目的活跃成员。他被授予2006年网络犯罪创新奖并从新罕布什尔社区技术学院取得了刑事司法专业的专科毕业证书，从新罕布什尔州立大学取得了信息技术专业的学士学位。

Captain Benjamin R. Jean编写了本书第8章。

Thomas Ralph以优等生毕业于凯斯西储大学（Case Western Reserve University）法学院，曾在法学院的《法律评论》担任编辑。他在担任MassHighway的法律顾问之后，在1998年，供职于密德萨斯（Middlesex）地区检察官办公室，在那里他在地区和高等法院从事审判工作。Ralph先生担任上诉局副局长、搜查队队长和公共记录队队长。Ralph先生多次在马萨诸塞州上诉法院和最高法院参与诉讼活动。2005年，Ralph先生成为了新罕布什尔州总检察长办公室的首席检察官助理，其职责包括主持新罕布什尔州总检察长的网络犯罪项目，以及处理和处置电子证据的创新项目。这个项目得到了国家认可，在以电子方式传播儿童色情信息方面负责监督复杂的侦查行为。

Thomas Ralph编写了本书第3章，合作编写了第6章。

Bryan Cunningham［法学博士，通过国家安全局（NSA：National Security Agency）］的信息安全评估方法学［（INFOSEC Assessment Methodology，IAM）认证，最高机密安全检查］不论是就职于美国政府还是在私人企业，都在信息安全、智能和国土安全问题领域有着广泛的经验。Cunningham现在是公司信息和国土安全顾问，还是Morgan & Cunningham有限责任公司的丹佛法律事务所的负责人，曾是前国家安全顾问康多莉扎·赖斯的副法律顾问。在白宫，Cunningham起草了国家安全法案的关键部分，并非常了解保卫网络空间的国家战略信息。他是前CIA警官、联邦检察官和美国银行协会（American Bankers Association，ABA）网络安全保密工作组的联合创始主席。2005年1月，因他致力于解决信息问题而被授予国家情报成就奖章（National Intelligence Medal of Achievement）。Cunningham入选国家科学委员会研究生物防卫分析与对策（National Academy of Science Committee on Biodefense Analysis and Countermeasures）项目。他是安可国际咨询公司（APCO Worldwide Consulting）的高级顾问，也是信息时代国家安全的Markle基金会工作组（Markle Foundation Task Force）的成员。Cunningham在信息安全项目和其他国土安全问题方面为公司提供咨询，充当信息安全顾问的角色，指导和监督信息安全评估与评价。

Bryan Cunningham编写了本书的附录A。

Brian Contos有十多年的安全工程和管理专业知识，以及实践经历，这些专业知识形成于世界上最敏感、最关键的任务环境下。他是ArcSight的销售总监，在宣传企业安全管理（ESM）空间时，他负责解决关于安全战略方面的方案，为政府机构和全球1000强企业提供咨询服务。

Colby DeRodeff（GCIA，GCNA）是ArcSight有限公司的高级安全工程师。Colby已经在ArcSight工作了5年多的时间，为这家公司的发展立下了汗马功劳。Colby对第一个产品的部署、专业的服务和管理起到了关键作用。

Brian Contos和Colby DeRodeff合作编写了本书的附录B。