

网络空间安全系列教材


Pearson

计算机取证与 网络犯罪导论 (第三版)

*Computer Forensics and Cyber Crime
An Introduction, Third Edition*

[美] Marjie T. Britz 著
戴鹏 周雯 邓勇进 译



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

计算机取证与网络犯罪导论

(第三版)

Computer Forensics and Cyber Crime
An Introduction
Third Edition

[美] Marjie T. Britz 著
戴 鹏 周 雯 邓勇进 译

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书是计算机取证与网络犯罪方面的经典教材。全书首先概述理论,讨论计算机相关术语和传统计算机犯罪。然后讨论当前的计算机犯罪,身份窃取与身份欺诈,恐怖主义及有组织犯罪,起诉途径及政府行为。接着探讨所涉及的法律问题,计算机取证的术语与需求,如何搜索并获取证据,以及证据的处理及报告准备。

本书适合从事计算机取证和网络安全相关工作的技术人员参考,也适合作为相关院校本科计算机取证技术及网络犯罪预防等课程的教材。

Authorized translation from the English language edition, entitled *Computer Forensics and Cyber Crime: An Introduction*, Third Edition, 9780132677714 by Marjie T. Britz, published by Pearson Education, Inc., Copyright ©2013 Pearson Education, Inc.

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 by any information storage retrieval system, without permission from Pearson Education, Inc.

CHINESE SIMPLIFIED language edition published by PEARSON EDUCATION ASIA LTD., and PUBLISHING HOUSE OF ELECTRONICS INDUSTRY Copyright ©2016.

本书中文简体字版专有出版权由 Pearson Education(培生教育出版集团)授予电子工业出版社,未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分。本书贴有 Pearson Education(培生教育出版集团)激光防伪标签,无标签者不得销售。

版权贸易合同登记号 图字:01-2013-6967

图书在版编目(CIP)数据

计算机取证与网络犯罪导论:第3版/(美)布里提(Britz, M.T.)著;戴鹏,周雯,邓勇进译.

北京:电子工业出版社,2016.9

书名原文:Computer Forensics and Cyber Crime: An Introduction, Third Edition

ISBN 978-7-121-27578-4

I. ①计… II. ①布… ②戴… ③周… ④邓… III. ①计算机犯罪—证据—调查 ②互联网络—计算机犯罪—研究 IV. ①D918②D914.04

中国版本图书馆 CIP 数据核字(2015)第 271336 号

策划编辑:马 岚

责任编辑:李秦华

印 刷:北京京海印刷厂

装 订:北京京海印刷厂

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本:787×1092 1/16 印张:24.75 字数:587 千字

版 次:2016 年 9 月第 1 版(原著第 3 版)

印 次:2016 年 9 月第 1 次印刷

定 价:78.00 元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010)88254888,88258888。

质量投诉请发邮件至 zits@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式: classic-series-info@phei.com.cn。

序

“向邻居看齐。”许多年轻读者可能从来没有听过这个说法。它通常指与邻居保持相同的社会和物质水平。但在这里，可能意味着计算机取证分析师和专家们不断试图跟上计算机和我们所有的电子产品技术的发展。在早先的出版物中，Britz 博士提出了计算机犯罪和计算机取证调查技术的基础教育，她再次将其涵盖到本书中。虽然，其中的一些技巧和准则现在看起来有些过时，但是，缺乏计算机及计算机相关的“智能”设备(手机、GPS, 演变成“电脑”的智能手机等)如何工作的基本知识，研究者将会被拒之门外。Britz 博士的计算机取证技术和历史章节向新用户介绍所有相关信息，并向所有不同水平用户阐明标准化技术。这样的说明只是众多原因之一，本书中设置了标准。

文中包含有关网络和计算机调查适用法律的全面讨论。当我们“在云中”时，必须考虑法律和司法辖区，但是网络犯罪并不关心其中的任何一个。调查人员必须具备资料，以便进行适当的调查，本科生必须吸收基础知识，这样的学术研究可能会持续下去。本书以清晰、简洁的方式提供这样的信息，适当介绍了(美国)州和联邦立法、第一和第四修正案以及国际努力情况。

除了法律，本书给我们带来最新的信息技术和实践，这是调查人员必须了解和掌握的，以便开展高科技调查和分析。如果计算机专家不紧跟技术发展，他们将在数月之内、而不是几年后被甩下。试想这么短的时间内，所有的智能设备变得如此丰富。本书帮助分析师和调查人员达到与技术发展曲线保持同步的速度。此外，它提供了一个可供领域内新人理解的框架。

本书进一步探索了电子卡、电子现金、因特网或其他在线交易和购买行为，很少有人没有经历过其中一个或另一个事物。随着身份诈骗和其他方式使用计算机、智能手机和其他电子设备非法获得资金的扩散，对资金窃取的调查一直在不断变化。本文中有关身份盗窃章节显示了这个领域中新兴的趋势，并提供加强个人安全和机构决策的建议。

最后，本书包括一个对调查人员和研究人员都至关重要的其他领域的全面讨论。这些讨论包括，网络，因特网，黑客，知识产权盗用，其他类型的计算机相关欺诈，最重要的是与科技社会相关的恐怖主义、有组织犯罪和性犯罪，以及如何进行涉及这些问题的计算机调查。

总之，Britz 博士再次概括了那些具有重大历史意义的计算机、法律和技术话题，这是当今计算机取证分析师、调查人员和专家必备的知识。与其他文章要么是太“技术化”，要么完全缺乏深度相比，本书是一本全面且具有可读性的书籍。简而言之，本书涵盖计算机研究人员和本科学学生感兴趣的话题。总之，它对每个人都有用。

Dan Mare

目 录

第 1 章 计算机取证和网络犯罪的概述和简介	1
1.1 简介	1
1.2 网络空间和犯罪行为	2
1.3 术语解释	4
1.4 与计算机犯罪相关的传统问题	5
1.4.1 物理和司法权问题	6
1.4.2 无意义、刻板和无能印象	6
1.4.3 检察官的不情愿	8
1.4.4 缺乏报案	8
1.4.5 资源匮乏	9
1.4.6 法律上的矛盾	12
1.5 问题延伸	12
1.6 电子货币的出现：执法的新问题	16
1.6.1 预付卡	16
1.6.2 储值卡	16
1.6.3 移动支付	16
1.6.4 因特网支付服务	17
1.6.5 数字贵金属	17
1.7 小结	17
讨论题	18
推荐读物	18
网络资源	18
参考文献	19
第 2 章 计算机术语和历史	22
2.1 计算机简史	23
2.2 计算机语言	25
2.3 计算机硬件	25
2.3.1 输入设备	25
2.3.2 输出设备	26
2.3.3 硬盘和其他大规模存储设备	27
2.4 计算机软件	28
2.4.1 启动顺序	28
2.4.2 操作系统	28

2.5	超越 DOS: 现代操作系统	29
2.5.1	微软 Windows	29
2.5.2	UNIX	32
2.5.3	Linux	32
2.5.4	智能手机	33
2.6	应用软件	34
2.7	互联网简史	35
2.8	网络语言	36
2.9	网络世界	39
2.10	贝尔大妈, 司法部, 反垄断	40
2.11	带宽数据的传输速率	40
2.12	因特网通信分类	40
2.12.1	万维网	40
2.12.2	新闻组/公告板 (Usenet 组)	41
2.12.3	互联网实时聊天	42
2.13	未来的问题和小结	43
	讨论题	43
	推荐读物	44
	网络资源	44
	参考文献	44
第 3 章	传统计算机犯罪: 早期黑客和元件盗窃	46
3.1	介绍	46
3.2	传统问题	46
3.3	认识和定义计算机犯罪	48
3.4	三个偶然事件	49
3.5	飞客: 昨天的黑客	53
3.5.1	什么是电话盗用	53
3.5.2	关于电话盗用的战争	54
3.6	黑客行为	56
3.6.1	定义黑客行为	56
3.6.2	黑客社区的演化	56
3.6.3	当前动机	57
3.6.4	当前网络犯罪的层次结构	59
3.7	作为商品的计算机	61
3.8	知识产权侵犯	63
3.8.1	软件	63
3.8.2	电影盗版	65
3.9	小结	65

讨论题	65
推荐读物	66
网络资源	66
参考文献	66
第 4 章 当代计算机犯罪	68
4.1 网络犯罪活动	68
4.2 恶意软件	70
4.2.1 病毒与蠕虫	71
4.2.2 DoS 与 DDoS 攻击	73
4.2.3 僵尸网络与僵尸部队	74
4.2.4 垃圾邮件	75
4.2.5 勒索软件与信息绑架	79
4.3 信息盗窃、数据操纵与网络入侵	80
4.3.1 传统的专有信息盗窃方法	80
4.3.2 商业秘密与版权	81
4.3.3 政治间谍	82
4.4 恐怖主义	83
4.5 新传统犯罪——新瓶装旧酒	85
4.5.1 刑事违禁品或非法材料的传播	85
4.5.2 通信威胁与干扰	91
4.5.3 网络欺诈	93
4.5.4 电子赃物贩卖	98
4.5.5 欺诈工具	99
4.6 附带犯罪	99
4.7 小结	103
讨论题	104
推荐读物	104
网络资源	104
参考文献	105
第 5 章 身份盗窃与身份欺诈	108
5.1 引言	108
5.2 身份盗窃/欺诈的分类	109
5.2.1 身份假冒	110
5.2.2 就业和/或边境入境盗窃	112
5.2.3 犯罪记录身份盗窃/欺诈	113
5.2.4 虚拟身份盗窃/欺诈	113
5.2.5 信贷身份盗窃/欺诈	114

5.2.6	受害者和与受害相关的损失	117
5.2.7	未来的增长	118
5.3	身份盗窃的物理方法	119
5.3.1	邮件盗窃	119
5.3.2	垃圾箱搜索	120
5.3.3	计算机盗窃	121
5.3.4	包操作	122
5.3.5	儿童身份盗窃	123
5.3.6	内部人员	124
5.3.7	虚假或虚拟公司	124
5.3.8	卡盗读、ATM 操纵和假机器	125
5.4	虚拟方法或通过互联网实施的方法	125
5.4.1	网络钓鱼	126
5.4.2	间谍软件与犯罪软件	128
5.4.3	按键记录器与密码盗窃程序	128
5.4.4	木马	130
5.5	利用身份盗窃/欺诈进行的犯罪	131
5.5.1	保险与贷款欺诈	131
5.5.2	移民欺诈与边境穿越	132
5.6	小结与建议	134
	讨论题	136
	推荐读物	136
	网络资源	136
	参考文献	137
第 6 章	恐怖主义与有组织犯罪	140
6.1	恐怖主义	140
6.1.1	恐怖主义的定义	141
6.1.2	根据动机分类	142
6.1.3	当代恐怖主义的根源	143
6.1.4	戏剧般的恐怖主义	144
6.1.5	网络恐怖主义的概念	144
6.2	网络恐怖活动	145
6.2.1	宣传、信息传播、招募和筹款	146
6.2.2	培训	147
6.2.3	研究与计划	148
6.2.4	通信	149
6.2.5	攻击机制	150
6.3	恐怖主义与犯罪	154

6.3.1	犯罪活动	155
6.3.2	对恐怖主义行为的定罪	155
6.3.3	政府的努力	156
6.3.4	本节小结	156
6.4	有组织犯罪	158
6.4.1	有组织犯罪的定义	158
6.4.2	有组织犯罪与网络犯罪团伙的区别	162
6.5	有组织犯罪和技术	164
6.5.1	敲诈勒索	164
6.5.2	货物抢劫和武装抢劫	165
6.5.3	诈骗	165
6.5.4	洗钱	166
6.5.5	性交易	167
6.5.6	骗局	167
6.5.7	赃物买卖	168
6.5.8	数字盗版和假冒商品	169
6.5.9	偷渡	171
6.6	应对当代有组织犯罪	171
6.7	有组织犯罪与恐怖主义的交集	172
	讨论题	174
	推荐读物	174
	网络资源	174
	参考文献	175
第7章	起诉途径与政府努力	179
7.1	引言	179
7.2	传统法规	180
7.3	计算机相关法规的演变	181
7.3.1	1986年的《计算机欺诈与滥用法案》	182
7.3.2	1996年的《国家基础信息设施保护法案》(NIIPA)	184
7.4	儿童色情作品法规的演变	184
7.5	身份盗窃和财务隐私法规	186
7.5.1	1998年的《防止身份盗用及假冒法》	186
7.5.2	1999年的《金融服务现代化法案》	186
7.5.3	2003年的《公平准确信用交易法案》	187
7.5.4	2004年的《身份盗窃惩罚力度增强法案》	188
7.5.5	2008年的《身份盗窃惩罚及赔偿法案》	188
7.5.6	保护个人信息的其他努力	189
7.6	联邦政府资助项目与协作	190

7.7	美国的执法行动与工具	191
7.7.1	包嗅探器和键盘记录器	192
7.7.2	数据挖掘	193
7.7.3	协作和专业协会	196
7.8	国际努力	198
7.8.1	经合组织(OECD)与欧洲委员会计算机犯罪专家特别委员会	198
7.8.2	欧洲委员会(CoE)的《网络犯罪公约》	200
7.9	小结	202
	讨论题	203
	推荐读物	203
	网络资源	203
	参考文献	203
第8章	第一修正案在计算机犯罪中的应用	205
8.1	引言与总则	205
8.2	通常意义上的淫秽	206
8.3	传统的正派概念	206
8.4	新兴法规和儿童对淫秽材料的可获取性	208
8.5	将儿童色情作品判为非法的传统尝试	209
8.6	判例法在传统儿童色情法规中的应用	209
8.6.1	New York v. Ferber 案	210
8.6.2	Osborne v. Ohio 案	211
8.7	与技术相关的法规——法庭上的争辩	212
8.7.1	《儿童色情防治法案》	213
8.7.2	Ashcroft v. Free Speech Coalition 案	214
8.7.3	《结束当今儿童侵犯的检控补救及其他手段法》(PROTECT)	215
8.7.4	U.S. v. Williams 案	216
8.8	互联网赌博	216
8.8.1	2006年的《非法互联网赌博强制法案》(UIGEA)	217
8.8.2	互联网赌博法规中的判例法	217
8.8.3	国际合作的缺乏与WTO	218
8.9	将来的问题和小结	219
	讨论题	220
	推荐读物	220
	网络资源	220
	参考文献	220
第9章	第四修正案与其他法律问题	223
9.1	第四修正案	223

9.1.1	合理根据	224
9.1.2	合理怀疑	224
9.2	有证搜查与计算机	225
9.2.1	特定性	226
9.2.2	证据扣押	227
9.2.3	第三方来源	228
9.2.4	有证搜查使用中的其他问题	229
9.3	无证搜查	229
9.3.1	同意搜查	230
9.3.2	紧急情况和突发状况	230
9.3.3	逮捕附带搜查	232
9.3.4	一目了然法则	232
9.3.5	边境搜查	233
9.3.6	其他无证搜查	233
9.4	证据排除法则	234
9.5	电子监控与隐私权	235
9.6	私营与公共部门搜查	236
9.7	将 Ortega 原则应用到电子邮件: Simons 案与 Monroe 案	236
9.8	《电子通信隐私法案》与 1980 年的《隐私保护法》	238
9.8.1	1986 年的《电子通信隐私法案》	238
9.8.2	ECPA 的三个章节	238
9.8.3	《隐私保护法》	240
9.8.4	ECPA 和 PPA 中拦截的定义	241
9.8.5	《通信协助法律执行法》	242
9.8.6	对 CALEA 的挑战	243
9.8.7	《窃听法》在电子邮件拦截中的应用——U.S. v. Councilman 案	243
9.9	《爱国者法案》	244
9.9.1	总统权力的加强	245
9.9.2	电子监控与刑事调查	245
9.9.3	国家安全信函和第四修正案的其他问题	247
9.10	其他隐私问题	248
9.10.1	点对点或文件共享	248
9.10.2	Internet 服务供应商用户记录	249
9.10.3	网站	249
9.10.4	移动电话	249
9.11	其他法律问题	251
9.11.1	邻近地区	251
9.11.2	密探技术	251

9.11.3 量刑指南	251
9.12 小结	252
讨论题	252
推荐读物	252
网络资源	253
参考文献	253
第 10 章 计算机取证：技术与需求	257
10.1 计算机取证——一门新兴学科	258
10.2 计算机调查中的传统问题	259
10.2.1 资源不足	260
10.2.2 部门间缺乏沟通与合作	260
10.2.3 过分依赖自动化程序和自封的专家	260
10.2.4 报告欠缺	261
10.2.5 证据破坏	261
10.3 磁盘结构与数字证据	262
10.3.1 磁盘结构与数据存储	263
10.3.2 分区表	265
10.3.3 文件系统	266
10.3.4 固件——操作指令	267
10.3.5 数据完整性	269
10.4 推动计算机取证能力的发展	269
10.5 最低空间需求	271
10.6 最低硬件需求	272
10.7 最低软件需求	275
10.7.1 数据保存、复制和验证工具	275
10.7.2 数据恢复/提取工具	277
10.7.3 数据分析软件	280
10.7.4 报告软件	283
10.7.5 其他软件	283
10.8 部分流行取证软件	287
10.8.1 Guidance Software 公司	287
10.8.2 Access Data 公司	288
10.8.3 其他取证工具	289
10.9 小结	290
讨论题	291
推荐读物	291
网络资源	291
参考文献	292

第 11 章 计算机相关证据的搜查与扣押	294
11.1 数字证据查找方面的传统问题	294
11.2 搜查前准备	295
11.2.1 搜查令的准备与申请	297
11.2.2 计划制定与人员召集	300
11.2.3 工具包的准备	302
11.2.4 传统设备	303
11.2.5 计算机相关设备与材料	304
11.3 现场活动	305
11.3.1 敲门、告知与记录	306
11.3.2 犯罪现场保护	306
11.3.3 确定是否需要其他协助	307
11.3.4 现场处理	307
11.3.5 查找证据	312
11.3.6 证据扣押与记录	314
11.3.7 装袋与贴标	316
11.3.8 询问证人	318
11.3.9 离开现场并将证据运到实验室	319
11.4 小结	320
讨论题	320
推荐读物	320
网络资源	321
参考文献	321
第 12 章 证据处理与报告准备	322
12.1 数据分析方面	328
12.1.1 建立干净的取证环境	329
12.1.2 确保分析工具的合法性与功能	330
12.1.3 物理检查	330
12.1.4 映像创建与验证	330
12.1.5 使用跳线清除 CMOS 密码	332
12.1.6 芯片短路	332
12.1.7 取出电池	332
12.1.8 密码恢复	333
12.1.9 映像验证	334
12.1.10 逻辑检查	334
12.1.11 文件恢复	335
12.1.12 文件列表	336
12.1.13 检查未分配空间中的数据残留	337
12.1.14 文件解锁	337
12.1.15 用户数据文件检查	338

12.1.16 证据的输出	339
12.1.17 对可执行程序的检查	339
12.1.18 互联网活动证据	340
12.2 非 Windows 操作系统	343
12.2.1 Macintosh 操作系统	343
12.2.2 Linux/UNIX 操作系统	344
12.3 智能手机与 GPS 取证	345
12.3.1 智能手机	345
12.3.2 流行产品举例	346
12.3.3 导航系统	347
12.4 报告准备与最终文档	348
12.5 小结	349
讨论题	349
推荐读物	349
网络资源	350
参考文献	350
第 13 章 结论与将来的问题	352
13.1 传统问题与建议	352
13.1.1 制定与技术无关的法律	353
13.1.2 建立 Internet 用户问责机制	353
13.1.3 提高公众认识与研究能力	353
13.1.4 增加跨部门与部门内合作	354
13.1.5 加强调查机构与私营企业之间的合作关系	354
13.1.6 加强国际合作	355
13.1.7 资格认证或专业技术的标准化	355
13.1.8 其他	356
13.2 其他 Internet 犯罪方法	356
13.3 未来趋势与新的关注点	359
13.3.1 无线通信	359
13.3.2 数据隐藏: 远程存储、加密等	360
13.3.3 对行为准则与虚拟色情的管控规定	361
13.3.4 数据挖掘与互操作性的增强	362
13.4 小结	363
讨论题	364
网络资源	364
参考文献	364
参考文献	365

第1章 计算机取证和网络犯罪的概述和简介

学习目标

学习完本章后，将能达到以下目标：

- 探究与科技进步和网络应用相关的社会变化
- 认识对计算机犯罪的起诉和执法带来的挑战
- 探索社会上计算机犯罪的范围
- 熟悉与计算机相关的犯罪分类

关键词和概念

- 计算机犯罪
- 计算机取证科学(计算机取证、数字取证)
- 计算机相关的犯罪
- 计算机犯罪
- 网络犯罪
- 数字贵金属
- 电子前沿基金会[Electronic Frontier Foundation(EFF)]
- 电子钱包
- 信息或数字革命
- 因特网
- 因特网支付服务
- 有限的或封闭系统卡
- 移动支付
- 多用途或开放系统卡
- 盗用电话线路
- 物理属性
- 预付卡
- 储值卡

1.1 简介

历史上，世界经历了几次启蒙运动和进步，例如，约两个世纪前的工业革命带来了空前的知识和机会，这次革命(一般工业自动化)提供了前所未有的便利和进步。交通的发展增加了度假目的地的清单、使得相距遥远的亲人间能保持联系；偏远地区也因为可以方便获得产前照顾，得以降低婴儿死亡率。另外，通信上的巨大进步提高了警察效率、改变了情侣间示爱行为等。个人、家庭和机构更容易获得奢侈品(如空调系统)。通过高效的工具、庭院设备等，家务也变得容易了。通过增加可靠、可信的知识来源，印刷自动化、大量媒体的介入等也极大地增强了信息的分发和传播。遗憾的是，也提高了身体懒散、肥胖、自满、迟钝、子女缺少和犯罪行为的增加。作为信息革命的直接结果，今天的美国社会也正经历着类似的转变。

因特网的引入为商业、科研、教育、娱乐和公共讨论等创造了空前的机会。一个全球性市场开始出现，其中，新想法和对多元文化欣赏的增长日益兴旺。数字化的百科全书、国际公会、世界连通性和通信的引入极大地增强了个人的生活品质。实际上，因

特网作为世界的一个窗口,能满足个人的好奇心,并培养其全球意识。它允许个人体验以前只能在梦中出现的事物,有意者可以参观罗浮宫、在其闲暇时欣赏无价的史前古董或是进行一场非洲狩猎且没有炎热和蚊虫叮咬。他们可以找到最复杂法律或医疗问题的答案,或是搜寻与其性情相投的伴侣;可以下载喜爱餐馆的优惠券,或是搜索到喜爱的食物配方。另外,个人、公司、公众组织和机构能使用图像化的、高亮强调的信息并提供详细的信息或支持的链接,更有效地宣传他们的产品或服务。实际上,计算机化的海量信息访问跨越了传统通信的边界。

与其他机构一样,执法机构也从中受益。因特网成功地为社会成员间交换信息创建了一种不受威胁的平台。另外,速度和效率使得全球的机构之间可以相互通信、巩固关系和加强协作。确实,执法机构通过简单地扩大交流对象就能更好地促进任务的完成。对嫌疑犯或失踪人员的文字描述和图片可以被任何连接到因特网的人看到,有关市民可以用一种有效和高效的方式报告嫌疑犯的行踪。然而,对因特网、数字技术和通信的更多依赖,也有不利的一面——带来了看起来执法部门难以克服的障碍。确实,从马达加斯加岛获得所喜爱食物配方的技术,同样也可用于下载大规模杀伤性武器的蓝图;在网上冲浪的个人在享受此类搜索成果的同时,同样也能跟踪和骚扰特定目标的受害者。事实上,使得因特网、无线技术和智能手机如此吸引人的优势也正是带来巨大危险的因素。

因特网的不利方面还包括对网络信息的依赖不断增加。许多在读大学生只依赖来源于电子化的知识。遗憾的是,在网络空间中所找到的信息质量堪忧,对人工智能的依赖导致对人的取代。更重要的是,新技术在加强传统不良行为模式的同时,往往会培育出一些新的社会不良行为模式。就像印刷出版业的自动化和众多媒体的引入导致违禁品的分发和需求也成指数地增长,如色情和违法物品。因特网上产生了虚拟的儿童侵犯和色情的温床,并建立了武器和毒品等的地下交易市场。事实上,犯罪行为的流行、视频交换或情报的非法交易也达到前所未有的高度。不断增强的无线技术、社会网络和智能电话使得调查领域更加复杂,全球的执法机构都在努力建立和加强新兴技术条件下的法律和制度。

1.2 网络空间和犯罪行为

网络空间可以定义为一个虚拟的空间,在其中,个人可以交易和沟通。它是空间之间的空间^[4]。尽管最初是在1984年由科幻小说作者 William Gibson 提出,但很难说这是一个新概念。实际上,普通的传统电子通信就属于这个空间,通过有线交换进行穿越时空的电话会谈。然而,熟知的因特网这种新媒体极大地增强了虚拟世界的真实感,相应地带来用户数量呈指数增长。例如,在2009年,大约有78%的美国人使用这个媒体,而1995年还只有10%。在英国,该媒体的用户增长更为明显,由1995年的1.9%增加到2009年的83.2%^[5]。没有其他的媒体能如此有效地融合语音、视频和数据。与传统方法不同,因特网包括了邮件、电话和大众传媒。如先前所述,它展现给个人的是无数的新想法并可作为社会聚集区、图书馆或是独处的地方。个人用户可以在里面结婚、生活、

养育孩子。遗憾的是，这个虚拟世界也经常成为逃避现实社会问题的避难所，在此，个人可以摆脱烦恼并自得其乐。

典型案例

第二生命：虚拟世界的实现

如前所述，在网络空间中存在很多虚拟社团，大多数表现出虚拟世界所具有的优柔寡断、寿命不长的特性。然而，在21世纪初由Linden实验室开发出来的第二生命(SL)，证明因特网虚拟世界可以吸引很多用户。一般所说的SL——第二生命可以表示为一个社会网络地址，用户或居民由一个三维动画代理或化身代表，在里面可以参加各种与人类真实体验相同的虚拟活动。他们可以购买财物、购买衣服、接受手术、确定性关系、结婚、生子，甚至在SIMetery中拜访已故的爱人。他们通过轻点鼠标即可参加大学课程、赌场赌博或完成全球的远距传输。事实上，学术和商业团体也注意到并加入到这个虚拟世界中。然而，很多个人为这个虚拟存在投入了大量的时间和金钱，却没有回报^[6]，以及规范和认识上的停滞不前都值得注意。

虚拟社区不仅跨越地理上的边界，还跨越了文化上的边界。关于种族、种族划分和国家民族血统的期望等被人工创造的自我(即化身)所取代，导致文化定义假设的悬而未决。换句话说，居民认可了肉体自我和虚拟代表之间的一致，接受了能处理物理、社会和经济方面因素的虚拟物，而那些因素在现实中一度困扰着他们。于是，在虚拟世界中的异常行为也仅仅是局限在虚拟中，而非现实中，然而后果未必如此。

随着越来越多的用户混淆了他们的真实生活和第二生命的界线，关于虚拟化身行为的合法性问题就浮现出来。假设一个美国成年男子的虚拟化身与一个12岁泰国小孩的虚拟化身发生性关系，这如果算犯罪的话，算是什么样的犯罪行为呢？在一个网络聊天室里，一个恋童癖与儿童进行交谈，满足了有一个预先安排的会面地点这个条件，但这不够，法律界定仍需是有肉体侵犯或猥亵发生才能确认犯罪。在一个基于虚拟的世界中，关于犯罪意图或犯罪动机的法律要求能被满足吗？

隐私保护主义者经常忽视了这个全球媒体的消极影响，而狂热地讨论这个新兴技术在排除政府对个人监视方面的潜力。这种组织由诸如抒情诗人John Barlow和John Gilmore这样的知识渊博的人发起的“感恩而死”(The Grateful Dead)，John Barlow和John Gilmore是Cygnus Solution、Cyberpunks和DES Cracker的合伙发起人/创建者。Barlow和Gilmore强烈呼吁抵御美国的一些声名狼藉的计算机黑客并支持人权法案。他们认为警察最初目标为侵犯美国公民隐私的游手好闲者，而现在却将注意力集中在他们原来保护的个人身上。实际上，他们创建了Electronic Frontier Foundation (EFF，电子前沿基金会)来提供“资金、指导和法律支持来证明美国特勤局限制出版物、限制自由言论、不恰当查封设备和数据、过度使用武力，且经常处于一种武断、强迫和违宪的状态^[7]。”尽管美国特勤局早期的行为也证实了这种担心，但EFF的种种努力却忽视了全球范围内被快速发展的城市多元化重新构建的社会所带来的负面潜力。