每一个和电脑打交道的人都必须读的一本书

网络黑帮

追踪诈骗犯、黑客与网络骗子

【美】米沙·格兰尼（Misha Glenny）著　周大昕 译

中信出版社·CHINACITICPRESS

DarkMarket

Cyberthieves, Cybercops and You

网络黑帮

追踪诈骗犯、黑客与网络骗子

【美】米沙·格兰尼（Misha Glenny）著　周大昕 译

中信出版社·CHINACITICPRESS·北京·

图书在版编目（CIP）数据

网络黑帮：追踪诈骗犯、黑客与网络骗子 /（美）格兰尼著；周大昕译. —北京：中信出版社，2013.1
书名原文：DarkMarket: Cyberthieves, Cybercops and You
ISBN 978-7-5086-3726-6
I. ①网… II. ①格… ②周… III. ①网络经济－通俗读物 IV. ①F062.5-49
中国版本图书馆CIP数据核字（2012）第287182号

网络黑帮——追踪诈骗犯、黑客与网络骗子

著　　者：[美] 米沙 · 格兰尼
译　　者：周大昕
策划推广：中信出版社（China CITIC Press）
出版发行：中信出版集团股份有限公司
　　（北京市朝阳区惠新东街甲4号富盛大厦2座　邮编　100029）
　　（CITIC Publishing Group）
承 印 者：三河市西华印务有限公司

开　　本：787mm×1092mm　1/16　　印　　张：16.5　　字　　数：208千字
版　　次：2013年1月第1版　　印　　次：2013年1月第1次印刷
京权图字：01-2011-6344　　广告经营许可证：京朝工商广字第8087号
书　　号：ISBN 978-7-5086-3726-6 / F · 2785
定　　价：45.00元

前言

crime@21stcentury.com

互联网从诞生之日起即深深契合了人类贪图便捷和刺激经济的欲望，为此，仅仅是在历史长河的悠忽之间，人类生活便对网络系统形成了危险的依赖：在短短20年时间内，大部分所谓“国家关键基础设施”（圈内人常挂在嘴边的CNI）即开始被极为复杂的电脑系统所控制。

电脑对现代生活的渗透几乎是无孔不入：通信系统、交通工具、工商活动、政府服务乃至日常工作与生活背后无不闪烁着高速运行的微处理器。在本人近年所旁听的诸多网络犯罪案中，英国皇家检察署曾对某黑客下达所谓《预防犯罪令》，在这位黑客出狱之日起就必须受此令管辖。按照该令，这位黑客每周登录互联网时间不得超过1小时，且其上网活动必须在现场警员监督之下。对此，这位黑客的辩护律师在听证会上慷慨陈词：“在我当事人服刑期满之时，世上将很

难找出可完全脱离互联网的人类活动。试问届时我的当事人又如何能过上正常生活？"

一点不错！现代人只是几个小时不带手机就会觉得焦躁不安，如果换成"手机达人"，那没有手机更是会失魂落魄。然而有意思的是，如果普通人能坚持远离手机三天，那么这种茫然无措的失落感就会变成如释重负的轻松感，或许还能惊喜地发现手机并非生活必需品，没有手机的日子依然可以过得井井有条。但对于大部分现代人而言，没有手机的日子是无法想象的。

在人类发展史上，或许只有汽车的发展情况与电脑最为相似。从20世纪40年代起，在西方发达国家，汽车开始驶入千家万户，但只有极少数驾驶员真正知道发动机罩下的机械动力原理。当然有些人虽对理论一窍不通，但对修车却轻车熟路，也有不少人知道在紧急情况下如何调整化油器来进入"跛行回家"模式[①]。即便是最缺乏修车技能的驾驶员也知道如何更换备胎。

时至今日，如果汽车故障仅仅是车胎漏气，那么或许大部分人还是可以慢悠悠地开车找修车店，但汽车抛锚越来越常见的原因却是控制箱故障，汽车控制箱一般是安置在发动机后的塑料机盒。如果是控制箱出了故障，那么即便你是坦克机械师，也难以把车修好。如果走运，你会碰到电脑工程师来排除故障，但在大部分情况下，方案只有一个：换控制箱。

较之内燃发动机的机械系统，电脑系统更为复杂和脆弱，只有极少数的人才算真正行家，而普罗大众面对电脑故障只有那一板斧——电脑重启。

因此当今世界的局面已然至此，只有极少数人（可称之为极客、解码高手、黑客、编程员、网络大侠、安全专家等等）才真正通晓网络技术，而此项技术对人类日常生活的影响从广度和深度上说都前所未有，普罗大众对此技术

① 跛行回家是指发动机带故障运行的一种模式。——译者注

却完全不甚了了。本人正是在开始撰写《超级黑帮》[①]时对此有了切身感受，当时我赶赴巴西去调查那里的网络犯罪。巴西的热辣风情举世闻名，但鲜为人知的是，巴西也是网络江湖的藏污纳垢之基地。

在巴西我碰到了技艺高超的网络盗贼，泛滥互联网的钓鱼邮件正是其杰作。钓鱼邮件迄今为止依然在互联网犯罪兵器谱上位列前端，并演化出两大支系。一类是普通钓鱼邮件，当受害者打开邮件后，邮件所含的病毒就会自动运行，由此在世界某角落的另一台电脑上，即可监控受侵电脑上的所有操作，包括输入网银密码。另一类钓鱼邮件则假冒为某银行或机构电邮，要求对方输入账号和密码确认。如果有人上钩，那么网络黑客即可获得目标电脑上的部分甚至全部互联网账户。巴西的网络飞贼在我面前逐步演示，他们如何用钓鱼邮件的金钩从巴西、西班牙、葡萄牙、英国和美国的银行账号中钓走了数百万美元的资金。

随后我又参观了巴西利亚的互联网警察部门，当时他们刚追查到某网络犯罪团伙的4名成员（但该团伙至少还有另外8名成员依然逍遥法外），随后我又采访了美国互联网安全系统公司（ISS）秘密行动组的负责人。在连续一周的密集采访后，我发现，尽管传统式组织犯罪看上去形式多样，但实际上现实世界的黑帮所承担的风险要远远高于其在网络上兴风作浪的同道。

那些凭借着20世纪技术手段在江湖打拼的传统黑社会组织若想发财致富又能安然无恙，必须闯过两大难关。现实世界的警力自然是首当其冲。各国的执法效力或有差别，执法严苛程度在各个时期也有所不同，黑社会组织必须采取措施来顺应环境。逃避警界和执法力量责罚的手段无非四种：其一是从力量上完全压倒，其二是拉拢腐蚀警察队伍，其三是渗透政界并从上端对警界施压，其四则是三十六计走为上策。

---

① 这是作者在本书之前所撰写的著作，全名为《超级黑帮：揭秘全球地下经济》。——译者注

但现实中的黑社会还必须面对另一挑战——黑帮火拼。在某黑帮的地盘上可能还有其他黑帮要来争食。对付同样虎视眈眈的同道，黑帮的策略无非三种：其一是硬拼并取胜之，其二是形成江湖同盟，其三则是拜入对方门下。

无论是对警察还是对黑道，犯罪组织均不可等闲视之，若是处理不善，轻则失财，重则殒命。因此现实黑帮的生存或发展之道是要在黑白两界都拿捏得度，绝不可惹毛一方。

然而在巴西，我很快就发现，21 世纪的网络犯罪是完全不同的江湖。

更为重要的是，在网络上打家劫舍，外界往往难以追查黑手。各国对互联网的监管法律有着很大差别。这对于网络犯罪具有重要意义，因为网络犯罪通常是通过某国的IP地址向另外一国的个人或公司下手，而具体套现行为又是在第三国。举例来说，哥伦比亚警方可能会发现有人试图攻击当地银行网络并查明该攻击来自哈萨克斯坦，但在哈萨克斯坦，这样的网络攻击行为却并不构成犯罪，那么哈萨克斯坦当地警方也就没有理由发起刑事调查。

许多网络罪犯都有相关信息来研究分析各国的法规差异所形成的漏洞。某位瑞典“盗卡者”[①]大佬就曾对我说：“我从来不对美国的信用卡或借记卡下手，因为这会将我置于美国的法律管辖权内，无论我身在何处。所以我只动欧洲或加拿大的银行卡，这样我既安全又能发财，他们永远都抓不到我。”

美加和美欧之间的法律差异对网络罪犯而言极其重要，欧洲和加拿大目前是网络犯罪的重点攻击领域，而美国却让网络罪犯心存忌惮。因为欧洲和加拿大更注重公民在网络中的个人自由和权利，但美国政府却赋予了执法部门让许多欧洲国家三思而行的庞大权力，美国的执法部门能以调查犯罪或反恐之名轻

---

① 本书中将Carder统一译为“盗卡者”，在其他文献中也有“洗卡者”或“盗刷信用卡罪犯”等其他翻译。盗卡在本书中泛指以非法手段获取、复制他人银行卡信息，并从盗窃或复制的银行卡中取现或消费的行为。——译者注

易获取私营公司的数据。

这种差距所造成的影响是深远的，在当前阶段也难以完全厘清。在互联网世界里，惩治罪行、网络监控、私密保护、公私机构的数据收集、言论自由（维基泄密的口号）、网站接入的全开放（所谓的网络中立原则的辩论）、社交媒体的政治功能以及国家安全和利益等议题，从来都是各有各的道理而无法完全廓清。

有人或许会说，像Google（谷歌）这样多平台多任务的全能网站违犯了美国的反垄断法规，Google所收集的海量个人信息完全有可能制造犯罪机会或损害个人自由。但Google也完全有理由反驳说，Google的创新精髓和成功奥秘正是其多平台多任务的全能模式，Google的强大恰好能为美国赢取更多的商业利益并让美国更加安全。假如美国政府愿意做，那么美国政府可以在数小时之内就通过合法程序来获得Google的数据，由于Google的数据来自全球各地，因此美国政府可取得其他国家政府只能艳羡的明显战略优势。中国、俄罗斯或中东等国政府如要获得Google数据只能通过黑客攻击方式，但美国政府却可光明正大地查看Google的秘密。美国政府撑死也只是惹上一场官司而已。既然如此，美国还有必要或有理由用反垄断法来对付Google吗？

互联网就仿佛是个大气球，在某处捏住一块，谁也不会知道又会在何处冒出来新的一块。

对于全球执法机构而言，互联网犯罪最大的问题就在于其匿名性。到目前为止，任何具备相应条件和技能的人都可以做到在上网时隐匿自己电脑所处的实际位置。

要在网络上隐蔽有两种方法，首先是通过VPN（虚拟专用网）手段，即多部电脑使用相同的IP地址。通常该IP地址是分配给某一电脑，但通过VPN，世界各地的若干电脑都可隐匿其实际位置，因为其IP地址可能显示这些电脑都位于博茨瓦纳。

对于那些不满足于VPN手段的人而言，他们也可以通过代理服务器的形式为自己多搭建一层网络保护墙。某台位于塞舌尔的电脑可以使用远在中国或危地马拉的代理服务器。代理服务器不会暴露这台电脑的塞舌尔IP地址，即便可以追查到，这台使用塞舌尔IP的电脑也可能是位于格陵兰岛而只是运用了VPN而已。

当然要设计这些需要高超的电脑技巧，因此在网络犯罪中运用这些手段的通常是两类人：真正的黑客或真正的网络罪犯。这些代表着新兴网络组织犯罪形式的极客大盗构成了电脑犯罪群体中的“精英阶层”。

大部分的网络罪犯都是小偷小摸的个体户，这些可称之为互联网蟊贼的群体甚至不值得执法部门去一一追查抓捕，毕竟网络执法部门的资源是宝贵而有限的。但即便是这些小角色从来不使用VPN、代理服务器或其他隐蔽手段，如果他们对自己的通信方式进行加密处理，警察要想将他们绳之以法也并非易事。

加密是网络安全中常见的重要技术手段。它是用电子生成密匙重新编排语言的方法，要破译这些密码必须经过浩繁的数理运算，因此一般而言，只有真正掌握了密码的人才可破译加密文件。从目前来看，加密文件基本是安全的，但作为全球实力最盛的数字情报机构，位于华盛顿的美国国家安全局（NSA）却始终在不断破译各种加密文件。在网络黑帮中，有关国家安全局的传说从来不断，传说美国安全局以及其加拿大、英国、澳大利亚和新西兰的情报机构已具备了通过上天入地的Echelon系统[①]来破译公共加密系统的能力。据说

① Echelon是非官方承认的美国领导的全球间谍网络，它为监听和传播电子通信操纵一个全自动的系统。据说被监视的传输每天包括高达30亿次的通信，覆盖全球范围的市民，包括所有的电话呼叫、电子邮件信息、传真、卫星传输，以及在互联网公共和私人的组织机构下载。由美国国家安全局领导的Echelon，与美国、英国、澳大利亚、加拿大以及新西兰的情报机构联合操纵。这个组织的名字来源于一个负责监听卫星通信的系统部件的代码名称。

Echelon系统可侵入监听世界任何角落的电话呼叫、电子邮件和卫星传输。

数字加密技术具有十分深远的政治影响，为此美国在90年代就将数字加密技术归类为“军用技术”，而在俄罗斯，如果警方或克格勃发现你的电脑上有加密文件，那么哪怕这份加密文件仅仅是超市购物清单，你也可能会面临长达数年的牢狱之灾。但随着政府和企业不断积累有关公民或客户的个人信息，加密又是为数不多的个人用以捍卫隐私的武器之一。而对于那些在网络上从事违法活动的人而言，加密更是无价的工具。

正如传统黑帮成员要在现实社会中区分敌我，网络恶徒也必须努力认清网上交流对象的真实身份，这也是网络罪犯必须面临的挑战。本书将阐述网络警匪世界的无间道：一方面网络黑帮千方百计用来识别警察认清同道；另一方面全球各国警方又积极反制，以保护网络警察和秘密证人的安全。

在20世纪90年代，啸聚网络的大盗所实行的最为简单的“门禁”措施就是在自身活动的网站设置严格筛选程序和会员体系，借此将非同道中人拒之门外。饶是如此，对于美国特勤局或俄罗斯联邦安全局（FSB，前身为克格勃）等机构，要潜入这些网站也通常不是难事。通过耐心地在网上假扮黑客或说服某些污点证人，这些机构一般只要几个月时间就可完全潜入黑客网站。

某些网络特工的表现几可以假乱真，一些国家的执法部门甚至真的针对兄弟单位的潜伏特工开展调查，因为这些特工在网络上的表现太像真正的互联网大盗了。

经过多年的细致调查和信息收集，警方和情报部门建立起了庞大的黑客数据库：他们的绰号和网名、他们的真实姓名和住址、他们所从事的活动以及经常联络的人员名单等。那些最低级别的网络犯罪分子的数据则被全部销毁。但尽管有了这些信息，要想真正起诉网络犯罪分子却依然难如登天。

互联网具有交互性和匿名性的天然属性，因此现实生活中的司法体系难以

在网络上行使权力：因为无人可以百分之百地确定其在网上交流对象的真实身份。对手是菜鸟级还是殿堂级的黑客？对方是否有很过硬的上层关系？对方是否是真的罪犯还是警方卧底？甚至是正在测试网络黑客技术的军方研究员？对方只是为了挣零花钱还是在为基地组织筹资？

“这如同七维棋局，”未来学家布鲁诺·吉桑尼（Bruno Giussani）评论道，“在任何时点，你都不知道你的对手是谁。”

美国加利福尼亚山景城的Google总部虽然不如印度泰姬陵那样令人震撼，但当我首次把车停在Google总部外的查理斯顿大街旁时，我还是忍不住感到敬畏，因为这里毕竟代表着后工业时代最伟大的奇迹。

Google以前所未有的速度深入我们的思维方式，并如毒品般控制了我们的心神起落。目前能与Google相提并论的也只是其数码近亲，例如Facebook（脸谱网）、微软和亚马逊等，但这三家均无法望Google之项背，Google的庞大服务器矩阵每时每刻都在调动海量数据来回应信息索取，同时又源源不断地搜集储存了数十亿用户的集体和个人数据，由此Google成为人类生活历史上最大的协助者、引导者和监控者。Google所采集的数据甚至比我们自己更能描述我们自身的特征。如果这些数据落入坏人之手，那么情况确实是不堪设想，或许不堪设想的事情已经发生……

在Google自称为“校园”的办公区内，Google标志中的六种亮丽颜色随处可见，散落在空间中的大型物件通常都采用柔软的弧形设计，处处都体现出精心设计的凌乱感。办公区的雕塑通常都供人休憩、观赏甚至把玩，如果你的心灵如同孩童般纯净，那Google办公区在你眼中就仿佛是硕大的幼儿园；但如果你心怀天下而忧愤不已，那么Google办公区就仿佛是美国电视剧《囚徒》中那恐怖的村庄：国家安全风险无处不在，所有公民都在劫难逃。不知是否是我的想象，Google办公区里从清洁工到高级管理人员，似乎每个人脸上都挂着入

迷般的笑容？这样的笑容越发加深了外界对Google本质的胡乱猜想，这也给外界这样的印象：仿佛每位Google员工都在过分努力地践行“不作恶”的理念。我无法揣度这究竟应该是美梦还是噩梦。

因此当我见到Google信用与安全经理科瑞·路易（Cory Louie）时，我甚至有了解脱感。因为从事安全工作的人基本上不会拐弯抹角，此外他们对机密也有天生的嗜好和警觉，这些特质不会随其雇主的变化而更改。因此路易开门见山的风格在Google如佛教般混沌的整体风格中算是另类。路易是30多岁的亚裔美国人，举止利落，对人诚恳，但他却并不是在硅谷的温柔乡中成长，他的网络安全技能来自美国特勤局真刀真枪的磨炼。在我访问他时，他已在Google工作两年半了，他在2006年底加入Google，当他离开特勤局时，他是特勤局电子犯罪科的负责人。因此他对所有的网络攻击形式（所谓的侵入或渗透）都烂熟于胸，此外他也熟稔信用卡欺诈、所谓的DDoS攻击（即分布式拒绝服务攻击，可使得网站或网络瘫痪），以及那些在进入新千年后如失控鼠灾肆虐的有害软件。他对盗卡行为也很熟悉，这是最常见的网络犯罪行为。在盗卡犯罪中，卖家会把盗取或侵入的信用卡信息在网上变卖，然后买家再用非法获取的信用卡信息购物或取现。

那么Google又如何能错过像科瑞·路易这样的优质人才呢？答案显然是否定的。反过来说，路易又如何能拒绝Google所给出的理想职位呢？一边是美国南部太平洋季风下的温暖地带，终年椰风海景，另一边则是阴冷潮湿、冬季漫长的华盛顿，最美的樱花期只有一周；一边是美国西海岸轻松自由的上班氛围，另一边则是西装革履奔波在首都环城高速路上；一边能参与各类项目名利双收，而另一边只能隐姓埋名为美国政府打拼。答案是不言自明的。

如果你从旧金山沿着美国101高速公路驱车向南，那么Google并不是你在路上唯一经过的网络巨头。太阳微系统、雅虎以及迈克菲（McAfee）等其他

耳熟能详的网络公司总部都会在你车窗外闪过。如果你与这些企业谈论网络安全问题，你会碰到许多有过政府职业背景的专业人士，他们来自美国联邦调查局、美国特勤局、中央情报局、缉毒局以及美国邮政监察局等机构。由退休卧底和便衣警察组成的庞大群体作出了与路易相同的职业选择，如同电影从业者向往好莱坞一样，他们也从井然有序的华盛顿郊区搬到硅谷，享受相对轻松宁静的生活。

这些从美国政府机构到私营网络公司的人才流动对于华盛顿而言当然是损失。美国财政部为培养这些网络调查者耗费巨资，但当这些人获得了几年资历后却纷纷投奔更加舒适的生活。然而网络调查并不会因此而终结，因为这些人才的流动也为美国政界和企业界架设起沟通的桥梁。Google并非简单的私营企业，在华盛顿眼中，Google是战略性的国家资产。来自华府的信息无比清晰：谁要是攻击Google，就等同于攻击美国。在此框架下，像路易这样的人可随时拿起电话通知他在美国特勤局的同僚，通知或提醒对方说，Gmail正遭受严重攻击，由此就使美国政商两界在互联网安全方面的合作更为紧密。

虽然我并不是完全清楚内情，但我可以推想，路易的生活水准在投奔Google之后定然是提升了不少，为此他也必须努力工作以证明自己的价值。Google是全世界拥有最大数据存量的两家公司之一，另外一家是Facebook。这也是为何Google可以日进斗金的资本（广告商愿意支付高额资金来获取这些数据所能揭示的个人偏好），当然这也使Google成为全球各地黑客攻击的至高目标，无论这些黑客是单打独斗还是为行业同道或敌对国家工作。

在我将要结束与路易的对话时，他向我推荐了一位当警察的朋友，这位警察长年都在用心与黑客建立友谊。他的潜伏工作成效卓著，目前他已是某大型犯罪网站的管理员。“或许他会愿意跟你谈谈，”路易说道，“他所管理的网站名为‘黑暗市场’。”这是我首次听说该网站，也是我第一次听到美国联邦调查

局特工基思·穆拉斯基（Keith Mularski）的名字。从此我开始了一段充满奇遇的调查之旅。

我开始极尽可能地去约见和采访所有与黑暗市场相关的人士，这些人身份各异且分布在20多个国家，他们中有江洋大盗、警察、双面间谍、律师、黑客以及罪犯喽啰。此外我也查阅了大量与黑暗市场有关的法院卷宗并多方探访。我从诸多已经金盆洗手或还在网络世界角力的黑白两道获得了额外的材料和信息。尽管我未能完全获得该网站的完整历史记录，但我基本上掌握了有关该网站的全部重大信息。在我采访的所有人中，穆拉斯基是唯一拥有黑暗市场几乎全部档案的人士，从他的材料中可窥见黑暗市场的全貌。

除了浩繁难懂的档案之外，其他材料虽然也有其价值，却往往在准确性方面失之偏颇；曾在法庭上多次呈堂的材料即属此列。在我看来，这些材料中的错误并非是出于疏忽或恶意，也不是有人刻意为之。这些错误反映出，在网络案件审判中，所谓证据通常都具有高度的技术复杂性且极其容易让人混淆。当首次直面网络犯罪行为时，许多法官和律师也会对网络世界的奇特生态感到难以捉摸，无法把握。

问题的核心在于分析网络警匪双方的人格和行为。许多证词可能都是个人的回忆，而这些回忆最早会追溯到10年之前。除回忆本身不太可靠之外，所有牵涉各方都有其自身的考量，他们会有意突出自身有关黑暗市场的某些行为，同时故意淡化甚至隐瞒其他行为。互联网沟通的模糊性也可帮助他们自圆其说，毕竟在网络文化中撒谎或隐瞒都是司空见惯。

在我所有的采访之中，我也无法全然分清究竟何人何时是在扯谎、隐匿或夸大，以及何人何时是在陈述真相。我的每位采访对象都似乎有无尽的故事想要倾诉，尽管某些人在谈论网络犯罪时，可能其本身并不占据道德制高点。但随着我对黑暗市场之隐匿世界的了解越来越深入，我意识到许多有关同一主题

的不同陈述，归根到底是相互矛盾而无法调和的。想要全然地还原谁黑谁白以及各方的交锋，或许根本没有可能。

互联网的发展积累了浩瀚的数据和信息，其中很大一部分是毫无价值的垃圾信息，另有一大部分至今无人可理解，但更有一小部分则是危险的虚假信息。人类生活日益网络化，而在网络世界中，由黑客和信息安全机构黑白两道上演的罪与罚、商业间谍甚至网络战争层出不穷，通过黑暗市场的历史等来知晓和理解互联网安全，就成为现代人的私人和社会生活的必修课，即便目前我们所知的网络和现实世界的证据依然零散而片面。

目录
Contents

VII· 前言

第一章　勇敢新世界· 001

002· 突然来电

008· 勇敢新世界

016· 拉各斯的双面高手

第二章　盗卡者星球· 025

026· 敖德萨档案

032· 盗卡者星球

033· 家族事务

042· 博阿落网

048· 重写脚本

第三章　网络江湖· 053

054· 孤独的少年

058· 博弈理论

061· 回头无路

066· 去往印度之路

069· 阴影世界

第四章　黑暗市场 · 077
078· 冰雪侠问世
082· 盗卡者市场
086· 黑暗市场
091· 办公区域
098· 可疑心机
102· 无间道
109· 狡诈计划

第五章　麻烦来了 · 115
116· 德龙传奇
121· 朋友，你惹麻烦了
124· “矩阵 001”归案
128· 法国关系
132· 隐形人
137· 插曲：真实的网络战争

第六章　隐现 · 157
158· 比拉尔在匹兹堡
166· 后台很硬？