商业分析

Business Analytics

信息安全

王小萌　马晓玲◎编著

华东师范大学出版社

商业分析

Business Analytics

信息安全

王小萌　马晓玲◎编著

华东师范大学出版社

图书在版编目（CIP）数据

信息安全/王小萌，马晓玲编著. —上海：华东师范大学出版社，2016
（商业分析丛书）
ISBN 978-7-5675-5670-6

Ⅰ.①信… Ⅱ.①王… ②马… Ⅲ.①商业信息—信息安全 Ⅳ.①F713.51

中国版本图书馆 CIP 数据核字（2016）第 204016 号

信息安全

编　　著　王小萌　马晓玲
策划组稿　孙小帆
责任编辑　孙小帆
责任校对　林文君
装帧设计　卢晓红　俞　越

出版发行　华东师范大学出版社
社　　址　上海市中山北路 3663 号　邮编 200062
网　　址　www.ecnupress.com.cn
电　　话　021-60821666　行政传真 021-62572105
客服电话　021-62865537　门市（邮购）电话 021-62869887
地　　址　上海市中山北路 3663 号华东师范大学校内先锋路口
网　　店　http://hdsdcbs.tmall.com

印 刷 者　常熟高专印刷有限公司
开　　本　787×1092　16 开
印　　张　26
字　　数　507 千字
版　　次　2016 年 11 月第 1 版
印　　次　2016 年 11 月第 1 次
书　　号　ISBN 978-7-5675-5670-6/F·371
定　　价　49.00 元

出 版 人　王　焰

本书简介

目标：

本书立足于当前信息安全具体实践，通过对信息安全领域相关知识点的讲解，以及该领域的新理论、新方法和新成果的介绍，帮助阅读者了解信息安全的概念、现状及趋势，学习信息安全攻守双方的具体策略，掌握经典实用的信息安全技术，提升个人和企业的信息安全技术能力、管理水平和信息安全素养。本书最后还对信息安全引发的社会问题、伦理问题进行了阐述和分析，以期引发大家的关注和思考。

内容组织：

本书分为基础编、技术编、应用编、伦理编四部分。

基础编包括第 1、2 章的内容，介绍了信息安全的概念、现状、趋势、研究意义、安全模型策略、信息安全法律等，帮助大家了解信息安全的历史、现状及发展的全景。同时介绍了信息安全的技术基础——密码学，包括经典的信息加密、信息隐藏、身份认证技术等。

技术编包括第 3～6 章的内容。其中第 3、4 章从攻击和防范两个角度介绍了主流的黑客技术和手段及对应的防范措施；第 5 章介绍了各类恶意代码的类型、破坏性及应对措施；第 6 章针对发展迅速、应用广泛的无线局域网的安全和管理进行了介绍。

应用编包括第 7、8 章的内容。其中第 7 章介绍了个人如何在日常工作和生活中提高信息安全素养，做好物理安全、数据安全、办公文档安全和网络应用安全的全方位防护；第 8 章侧重团体和组织如何在技术、管理等方面保护信息安全，特别介绍了在云计算、大数据及移动商务 BYOD 等新技术环境下，企业保护信息安全的新理论、新技术、新举措。

伦理编包括第 9、10 章的内容。其中第 9 章阐述了信息伦理学的基本理论知识，分析了随着信息技术的不断发展和社会信息化进程的加快而产生的现代信息活动的伦理困境；第 10 章重点讨论了国家信息安全、隐私保护、知识产权和数字鸿沟等信息伦理的主要问题。

本书的第1、8章由王小萌编写，第2、3章由曾佳雯编写，第4、6章由陈路瑶编写，第5、7章由张悦悦编写，第9、10章由马晓玲编写，郭劲赤参与了部分案例资料的收集、分析等工作。

体例特点：

本书每个章节均以信息安全方面的现实案例开头，内容中结合了信息安全主流技术、现实应用以及发展趋势等方面，并且从技术、管理等方面给出保护个人及团体组织信息安全的对策和方案。每章结尾部分均有本章小结、思考题，有助于帮助阅读者进一步总结和思考。

目录

第二编　技术编　103

第一编 基础编

1 信息安全概述

当今社会是一个信息化社会，计算机网络在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大，整个社会对计算机网络的依赖性也日益提高，尤其是计算机技术和通信技术相结合所形成的信息基础设施，已经成为反映信息化社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集中于计算机中。但是这些信息系统都是依靠计算机网络接受和处理信息，实现其相互间的联系和对目标的管理、控制，以网络方式获得信息和交流信息已成为现代信息化社会的一个重要特征。

随着网络的开放性、共享性及互联程度的扩大，特别是因特网的出现，网络的重要性和对社会的影响也越来越大。随着网络上各种新兴业务的兴起，例如，网上购物、网上炒股、视频会议、远程教育、电子政务、网络银行、数字图书馆，以及各种专用网络的建设，网络与信息安全问题受到了前所未有的关注和重视。

信息技术在带给人们前所未有的便利和巨大效益的同时，也使人们面临信息安全方面的巨大挑战。在网络世界内，每个个人、团体、国家，都可以自由表述自己的观点，实施自己的行为。而网络与信息系统的开放性和潜藏的商业、经济、军事利益，给恐怖分子、犯罪集团、黑客组织和敌对势力等创造了大量可乘之机。恐怖分子、犯罪集团也在利用网络组织和实施恐怖犯罪活动；黑客组织直接以网络为目标进行恶意攻击；敌对势力对意识形态领域的渗透和对政府、军队秘密信息的窃取，给国家主权、国家安全和社会稳定带来极大的威胁。

更令人担忧的是，我国信息化规模的高速发展是建立在大规模引进国外新兴信息技术基础之上的，我国信息化产品自主化水平还很低。在计算机和公用网络的软硬件技术方面，中央处理器和操作系统几乎完全建立在美国公司产品的基础上。在大型设备和通信设备方面，运行在其上的系统软件、支撑软件也大多数是国外的产品。一旦我们所依赖的国外核心技术得不到保证，或存在严重的安全隐患，势必对我国的信息安全和国家安全造成严重后果。因此，对信息安全知识和动态的学习与研究无论是对个人、企业还是国家都是非常必要的。

1.1 现实中的信息安全问题

信息安全已经深入到社会生活的各个领域，以下从一些典型的事件、案例入手，让大家更好地了解信息安全的问题和现状，理解信息安全的重要性。

1.1.1 信息安全与国家政治

案 例

斯诺登与“棱镜门”事件

2013 年 6 月，前中情局(Central Intelligence Agency，CIA)职员爱德华·斯诺登将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》，该资料称美国国家安全局有一项代号为“棱镜”(PRISM)的秘密项目，是一项由美国国家安全局(National Security Agency，NSA)自 2007 年起开始实施的绝密电子监听计划。该项目要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。美国国家安全局和联邦调查局还通过进入微软、雅虎、谷歌、Facebook、PalTalk、YouTube、Skype、AOL、苹果九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。《华盛顿邮报》获得的文件显示，美国总统的日常简报内容部分来源于此项目，该工具被称作是获得此类信息的最全面的方式。

图 1-1 爱德华·斯诺登

报道刊出后外界哗然。保护公民隐私组织予以强烈谴责，表示不管奥巴马政府如何以反恐之名进行申辩，不管多少国会议员或政府部门支持监视民众，这些项目都侵犯了公民的基本权利。斯诺登也称，他是出于对隐私权的担心才采取爆料行为的。他表示：“我不想生活在一个做那些事情的社会里，我不想生活在一言一行都被记录的世界里。”

而奥巴马表示“棱镜”项目在防止恐怖袭击方面发挥了重要作用，至少有 50 起恐怖图谋是因为“棱镜”监控项目的存在而破产的。他欢迎就国家安全与隐私权的平衡问题展开

讨论，他说："很重要的一点，是要认识到你不可能有百分之百的安全，也不可能有百分之百的隐私。"

在互联网时代的今天，"棱镜"给政府、企业及个人上了一堂现实版的信息谍战课。

1.1.2 信息安全与军事战争

未来网络空间将成为国家间竞争和博弈的新战场。从2010年开始，就已出现国家间网络空间安全对抗的态势。"棱镜"计划的曝光让人们更加认识到这种对抗的真实性和严重性，会有更多的国家尝试做类似的事情。网络安全已成为一个国际性问题，它不仅影响到社会领域，也影响到军事领域，"网络军事化"已渐渐走到台前来。

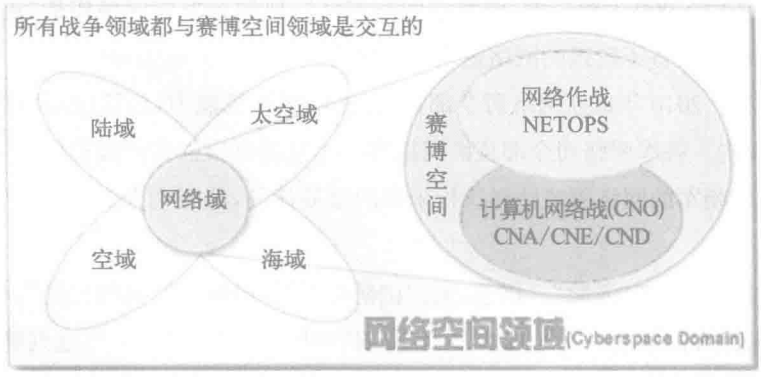

图1-2 网络空间

自20世纪90年代以来，网络便像一只无形的手伸向社会各个领域。无处不在的网络甚至成了无所不能的代表。整个地球变成了一个巨大的网络空间。网络在提高人们生活质量的同时，也带来了潜在的威胁。如果说网络黑客的破坏与干扰还只是个体威胁的话，那么美国建立网络战司令部已将这种威胁升格为一种国家行为。

(1) 网络部队

美国率先在全球开启网络较量。2009年1月，美国国防部发表的《四年任务使命评估》，将"网络中心战"列为美国的"核心能力"。5月29日，美军战略司令部对媒体宣布，他们正在征召2 000～4 000名士兵，组建一支网络战"特种部队"。2009年6月，美国国防部长盖茨宣布创建网络战司令部，网络战司令部将对美军现有的网络作战力量进行整合，是一个将空间、信息对抗

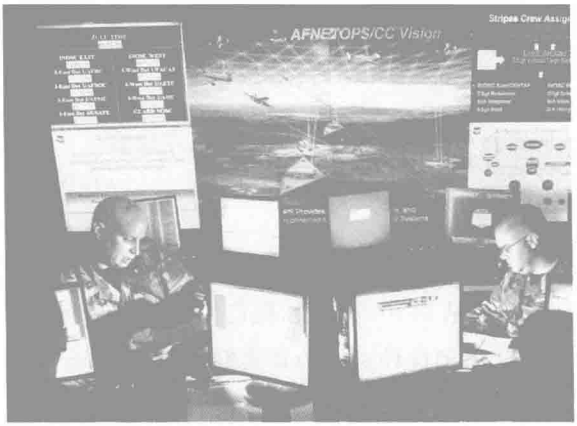

图 1-3　美军网络战司令部内景

和进攻打击能力有机结合在一起，执行空间和全球打击、全球范围内防止大规模杀伤性武器扩散等任务的一个机构。这表明美国将网络战作为一个全球性的作战方式来看待。

美国并非是在演“独角戏”。在美国的“模范”带头作用下，世界各国似乎不约而同地都嗅到了来自网络领域的危险，纷纷“招兵买马”扩网军，以维护本国网络安全。“网络建军潮”在全球范围悄然兴起：

◇ 日本自卫队组建“网络部队”。日本在 2011 年建立了由 5 000 人组成的“网络空间防卫队”，研制开发的网络作战“进攻武器”和网络防御系统，目前已经具备了较强的网络进攻作战实力。

◇ 韩国军方于 2010 年成立网络司令部，以提高网络作战能力，包括应对网络攻击威胁并在遭攻击后实施反击。韩军网络司令部从民间招募一大批拥有很强实战经验的黑客。韩国军方表示，为了积极应对朝军的网络战威胁和执行未来网络战任务，韩国军方要达到美国网络部队作战的水平。

◇ 伊朗网络部队终于“露脸”。据悉，美国国防部下属的机构“防御科技局”，将伊朗列为世界上五个最厉害的黑客国家之一。2012 年 3 月 22 日“美国之音”的网站突然遭到篡改，同时受到破坏的还有 95 个关联网站。伊朗半官方的法斯(Fars)通讯社随后发布消息，确认了伊朗网军实施了这次“攻势”，消息还称，“这次行动是为了回应以美国之音为代表的美国媒体对伊朗颠覆性活动的错误报道”。

◇ 英国拟建英版网络司令部。英国政府官员多次强调英军加强应对网络战的必要性。英国政府公布《国家安全战略》，将网络战列为英国今后面临的最严重威胁之一。在大幅削减国防预算的同时，戴维·卡梅伦政府宣布额外投入 6.5 亿英镑(约合 10 亿美元)用于保障国家网络安全和发展军事电子防务。

◇ 印度招募黑客组建网络部队。印度基于对网络技术的精通和利用网络能够达到何种战争效果的认识，坚持自主研发、军民合作的原则，投入大量人力、物力，力求在网络技术、密码技术、芯片技术以及操作系统方面自成体系。“闪光信使”高速宽带网络以及被称为“第三只眼”的海军保密数据信息传输网络的建成使用，将进一步增强印度军方应对未来网络战争的不对称优势。

◇ 俄罗斯20世纪90年代就设立了信息安全委员会，专门负责网络信息安全。2002年推出《俄联邦信息安全学说》，将网络信息战比作未来的“第六代战争”。俄罗斯已经拥有了众多的网络精英，反病毒技术更是走在了世界的前列，在遇到威胁或有需要时，这些人才和技术将能很快地转入军事用途。

◇ 以色列在1998年就将成功入侵美国国防部网站的青年招入部队，并开始加大对网络作战的研究力度。在巴以冲突、黎以冲突中，以色列利用网络进攻的方式篡改网页、攻击电视台，以达到影响舆论导向的目的；侵入军方电脑窃取机密，以确定火力打击的重点目标和精确坐标；阻断敌人通信指挥系统，以掌握最佳的作战时机。这一切都是以军进行网络战的真实写照。

◇ 中国也已组建“网络蓝军”，以捍卫军队网络安全。与西方国家的网络战部队相比，我国的“网络蓝军”目前处于初级阶段。与其说是一种有建制、成规模的网络战部队，不如说是我国军方开展的一种网上对抗训练模式。

中国现在对网络的依赖性越来越大，但中国没有一台根服务器。此外，中国网络的硬件，包括很多软件的生产商基本上都是美国的。从这个意义上来说，中国只是计算机的“用户”，网络安全很脆弱。在这样的环境下，中国组建一支保障网络安全的部队是十分有必要的。但在中国军方证实“网络蓝军”存在的消息后，西方媒体却质疑中国“网络蓝军”有“黑客”之嫌。现代化战争打的是科技和网络，而不仅仅是战士上战场。虽然我们不希望打仗，但需要时刻准备着。加强国防网络建设是维护国家安全的又一新要求，应加大对网络国防的重视。

(2) 网络战争

著名军事家詹姆斯·亚当斯在其著作《下一场世界战争》中曾预言：在未来的战争中，计算机本身就是武器，前线无所不在，夺取作战空间控制权的不是炮弹和子弹，而是计算机网络里流动的比特和字节。如今，这一预言正在变成现实。每一次敲击键盘，就等于枪击一发子弹；每一块CPU，就是一架战略轰炸机。

事实上，美国第一次运用网络战，可以追溯到1991年的海湾战争期间。美国向伊拉克派出特工，将伊从法国购买的防空系统使用的打印机芯片换上了含有计算机病毒的芯片。在美国对伊实施战略空袭前，美特工用遥控手段激活了这些芯片中的病毒，致使伊防空指挥中心主计算机系统程序错乱，伊防空C3I系统(指挥自动化技术系统)失灵。从这时开始，人们开始重视网络战，网络安全开始被提升到战略高度。

美国总统奥巴马也曾承认对伊朗核设施电脑系统发动过“震网”病毒攻击。众所周知，“震网”给伊朗核设施造成了重大破坏，在一定程度上拖延了伊朗核计划，可以说是一次成功的网络

进攻。这次网络攻击的“低成本、高收益”无疑让美国尝到了甜头，现在，美国扩编网络部队，极有可能准备在必要的情况下，继续对某些国家展开类似“震网”的攻击。

2008 年北京奥运会期间，当全世界都沉浸在激烈的体育比赛中时，一场战争却在高加索地区爆发：在现实世界里，格鲁吉亚的火箭在两个闹独立地区飞蹿，俄罗斯人的坦克则势如破竹为这两个地区提供保护；与此同时，在虚拟世界里，精心策划的俄罗斯网络部队亦暴风般席卷了格鲁吉亚政府的交流系统和银行系统。在一些专家看来，这是真正意义上的第一场网络战争。早在冲突开始前，2008 年 7 月 20 日，一组诡异的信息数据流向了格鲁吉亚政府网站，其携带的信息为“win+love+in+Ru-sia”。伴随而来的是短时间内数以百万计的访问请求汹涌而来，使得格鲁吉亚政府网站瞬间瘫痪。专家们立即指出，这是典型的“分布式拒绝服务”(DDoS)攻击。在黑客攻击中，这是最为普遍而有效的手段之一。格鲁吉亚总统萨卡什维利的网页被多重 DDoS 攻击而瘫痪长达 24 小时。然而，相比 8 月 8 日俄罗斯对格鲁吉亚的大规模网络攻击，7 月的这次网络冲突只能算是一次“带妆彩排”。随着俄军进入南奥塞梯，格鲁吉亚的网络再次受到大规模攻击。交通、通信、媒体和银行的网站纷纷遇袭中招，政府网站系统更是全面瘫痪。甚至，在国家银行的网页上，格鲁吉亚总统萨卡什维利的照片被和希特勒等 20 世纪独裁者的照片挂在一起。格鲁吉亚几乎无法向外界有效发声，无奈之下，格鲁吉亚的外交部新闻只好发布在谷歌下的一个公共博客页面上；此外，萨卡什维利还无奈向波兰总统卡钦斯基求助，将新闻也发布在卡钦斯基的网页上。

尽管格鲁吉亚遭遇的网络战，更多的是一种心理上的恐吓和威慑，但它是全球第一场与传统军事行动同步的网络攻击，具有独特的意义。

1.1.3 信息安全与经济金融

信息安全是维护国家利益、保障经济安全、服务民生的重要基础。金融信息与网络安全事关金融稳定和国家经济安全，一旦出现问题，不仅是经济安全问题，更是社会政治稳定问题。

案 例

比特币交易站受攻击破产

2014 年 2 月，全球最大的比特币交易平台 Mt. Gox 由于交易系统出现漏洞，75 万个比特币以及 Mt. Gox 自身账号中约 10 万个比特币被窃，损失估计达到 4.67 亿美元，被迫宣布破产。这一事件凸显了互联网金融在网络安全威胁面前的脆弱性。