国家安全译丛
NATIONAL SECURITY 总策划 王吉胜

INTRODUCTION TO CYBER-WARFARE

21世纪网络战 ☆全解码★

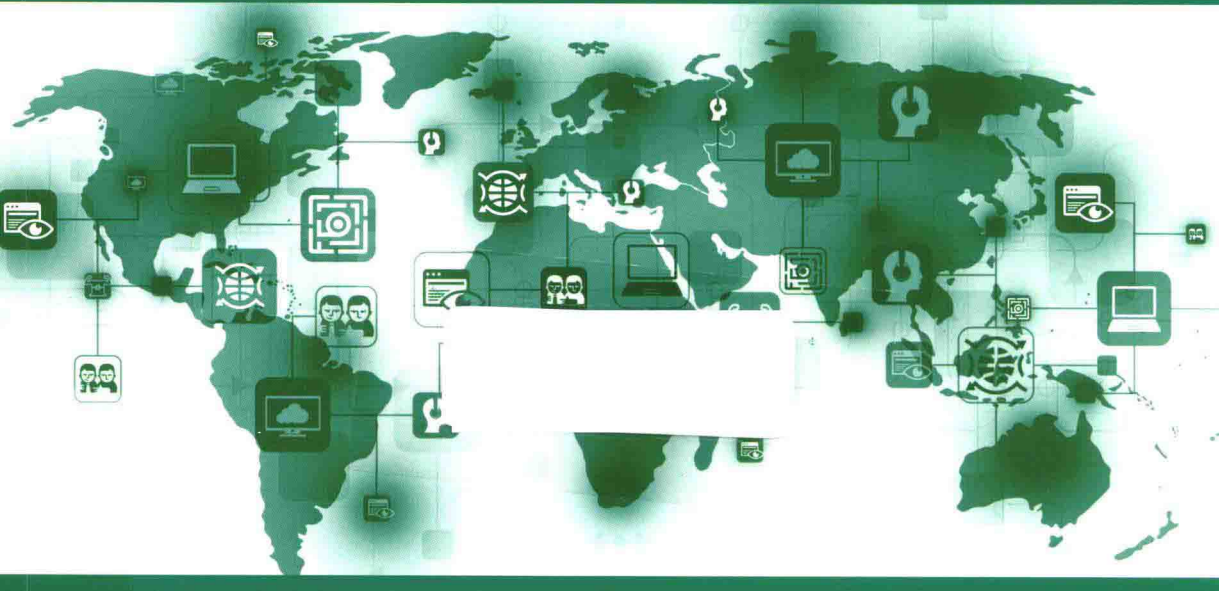
网络战

信息空间攻防历史、案例与未来

A Multidisciplinary Approach

[美] 保罗·沙克瑞恩 Paulo Shakarian 亚娜·沙克瑞恩 Jana Shakarian 安德鲁·鲁夫 Andrew Ruef ◎著 吴奕俊 等◎译

西点军校权威联合打造 · 多维度回顾、分析与预判



透视经典事件和前沿技术 · 对比全球网络军备之现状

金城出版社 GOLD WALL PRESS

国家安全译丛
NATIONAL SECURITY 总策划 王吉胜

21世纪网络战
★全解码★

网络战

信息空间攻防历史、案例与未来

INTRODUCTION TO CYBER-WARFARE

A Multidisciplinary Approach

[美] 保罗·沙克瑞恩 ◎著
Paulo Shakarian

亚娜·沙克瑞恩
Jana Shakarian

安德鲁·鲁夫
Andrew Ruef

吴奕俊 康鹏珍 蒋云君◎译

金城出版社
GOLD WALL PRESS

图书在版编目（CIP）数据

网络战：信息空间攻防历史、案例与未来 /（美）保罗·沙克瑞恩，（美）亚娜·沙克瑞恩，（美）安德鲁·鲁夫著；吴奕俊，康鹏珍，蒋云君译 .—北京：金城出版社，2016.8

（国家安全译丛 / 朱策英主编）

书名原文：Introduction to Cyber-Warfare：A Multidisciplinary Approach

ISBN 978-7-5155-1354-6

Ⅰ. ①网… Ⅱ. ①保… ②亚… ③安… ④吴… Ⅲ. ①计算机网络－军事应用－研究 Ⅳ. ① E919

中国版本图书馆 CIP 数据核字（2016）第 143860 号

网络战
WANGLUOZHAN

作　　者	[美] 保罗·沙克瑞恩　亚娜·沙克瑞恩　安德鲁·鲁夫
译　　者	吴奕俊　康鹏珍　蒋云君
责任编辑	李凯丽
开　　本	710 毫米 ×1000 毫米　1/16
印　　张	26.5
字　　数	435 千字
版　　次	2016 年 9 月第 1 版　2016 年 9 月第 1 次印刷
印　　刷	三河市百盛印装有限公司
书　　号	ISBN 978-7-5155-1354-6
定　　价	69.80 元

出版发行	**金城出版社** 北京市朝阳区利泽东二路 3 号　邮编：100102
发 行 部	(010)84254364
编 辑 部	(010)64271423
投稿邮箱	gwpbooks@yahoo.com
总 编 室	(010)64228516
网　　址	http://www.jccb.com.cn
电子邮箱	jinchengchuban@163.com
法律顾问	陈鹰律师事务所　(010)64970501

序 言

2010 年，震网病毒的出现使得“网络战”真正成为了一个公众话题。然而，何谓网络战？我们对它的了解又有多少？关于这个话题的文章如恒河沙数，有些从个人信息安全的角度出发，有些纯粹从政策的角度出发。前者的关注点往往是那些在计算机安全书籍中早就被广泛讨论过的基础层面的技术细节，而后者的关注点是高水平决策，而这上升到了大多数读者影响不到的层次。一直以来，人们总是轻易忽略热门网络事件背后非常有趣的细节。因为这种忽略，当前文献并未回答这个非常基本的问题：“人类是如何开展网络战的？”

我们争取在本书中弥补其中的差距，为读者提供大量的案例研究，在案例中重点讲述网络战里我们认为关键的一些问题。我们的跨学科研究法包括许多技术信息安全细节，尽管它们并不是本书的唯一焦点。在每一个案例研究中，我们也尝试突出网络战中涉及军事、政策、社会以及科学方面的问题。我们希望就像笔者们撰写本书时的体验一样，通过阅读本书能给读者带来一次非凡的学习体验。

保罗和亚娜欲借此机会，对在本书撰写过程中所有支持他们的朋友和同事表示感谢，还有他们的宠物狗塞奇，因为它的存在让作者感受到邻居们是多么的可亲可爱。

安德鲁欲借此机会感谢他的太太爱丽丝（Alice）对他的关爱与支持，

同时也感谢他的朋友与同事对他多年的教导。

全体作者欲借此机会感谢所有审稿人（包括一些匿名人士），支持我们的员工，还有帮助出版此书的 Syngress 出版社友善的员工们。在此，我们还要特别感谢（排名不分先后）：史蒂夫·艾略特（Steve Elliot）、本·瑞里克（Ben Rearick）、派特·莫尔德（Pat Moulder）、苏希尔·贾乔迪亚（Sushil Jajodia）、赫拉尔多·I. 西马里（Gerardo I. Simari）、罗伊·林德劳夫（Roy Lindelauf）、乔恩·本特利（Jon Bentley）、尤金·雷斯勒（Eugene Ressler）、J. 斯科特·兰斯博顿（J. Scot Ransbottom）、丹·吉多（Dan Guido）、迪诺·戴·佐伊（Dino Dai Zovi）、T. J. 奥康纳（T. J. O'Connor）、查尔斯·奥茨托特（Charles Otstott）、V. S. 撒布罕马尼安（V. S. Subrahmanian）以及格雷格·康迪（Greg Conti）。

保罗·沙克瑞恩
亚娜·沙克瑞恩
安德鲁·鲁夫

前　言

现今，网络战已成为一个公众常规话题。在**《连线》**（*Wired*）杂志和 SlashDot 这样的流行技术杂志里，到处都是这样的内容，也经常出现在像 CNN 这样的大众媒体中，并已成为美国优先考虑的政治议题，同时它也是全球军事机构主要关注的一个焦点。然而，我们对这种新维度的冲突掌握了多少？许多权威专家的言论让你深信，网络战已将世界置于危机边缘——一个聪明的少年在电脑前就能随时让全球计算机系统陷入混乱。而另一个极端是，有些人认为，网络战其实只是被人们过度炒作而已，是被计算机安全公司和国防部承包商夸大了的小事件，以从中获利。然而，有很多事件让我们明白，真正的答案往往就在两个极端之间。网络武器确实能够带来巨大的潜在伤害，我们必须明白，当这些网络武器成为政治工具时，网络战参与者的活动也在一定程度上受到了限制——对这些高科技工具的使用一定会带来不同的后果。这样一来，问题就成了“网络战士如何在一场政治冲突中使用武器？”这就需要研究相关历史，而“网络历史”正是本书所要讲述的。

本书是网络战领域唯一一本提供网络案例研究的选集。网络领域的战争在本质上是一场技术战，所以了解关于信息安全方面的细节必不可少。但是，随着网络的不断发展，网络战对生活各方面的影响越来越大，因此在封闭的信息安全环境下进行研究使得这个议题脱离了现实依据。网络战

争领域不断发展，因此网络战士也一样在不断壮大——他们需要从多个不同的维度来看待这个领域的问题。通读本书，你会发现保罗、亚娜和安德鲁是名副其实的跨专业团队。保罗具备计算机科学背景与军事经验，亚娜拥有社会科学和暴力冲突方面的专业知识，安德鲁具有安全专业人员的行业经验。本书将这些跨专业的必备知识融会贯通，让读者从中对网络战有一个总体的了解。

“网络”是当下的一个热门领域，并且在可预见的未来里它的热度将不会减退。社会对技术的依赖是毋庸置疑的，对安全技术的依赖更是必不可少的。本书的目的在于深入了解网络战发生的时间、原因，以及如何发生——当下许多工业、学术、政治以及军事领域中的人们需要对网络战争有所了解。

公司安全人员在国际冲突中，该如何调整自己的姿态？如果重大研究问题可以解决，那么它们对网络领域有什么影响？政治决策与技术现实之间的关系是什么？网络行动如何支援传统军事力量？这些都是萦绕在所有参与者心头的问题，而这正是本书各章节要探讨的地方。

所以，如果我能够让你认识到本书的重要性，并且愿意翻阅它，这固然很好，但笔者觉得因为本书有趣而阅读，会更让人欣慰，而本书恰好兼具以上两种优点——它以一种妙趣横生的方式阐释了一个严肃的重要话题。其中有些事件你可能早已听闻，但阅读本书会让你在这些老掉牙的事件背后，发现更多令人惊讶的地方。

因此，我诚挚邀请你阅读本书，了解为何网络战会成为一个重要的新领域，并且了解其中发生了什么。我承诺本书将会让读者学到新东西。尽管我有二十多年的网龄，我也获益匪浅！

苏希尔·贾乔迪亚

美国乔治梅森大学安全信息系统中心主任及教授

导 言

2006 年，一位美国商人坐在电脑前查看邮件，邮箱里有一封由名叫“以色列网络恐怖分子猎手”（Israel cyber–terrorist hunter）的人发来的一封神秘邮件，邮件声称黎巴嫩真主党为了在网络上传播他们的思想，劫持了该公司的一个 IP 地址。[1] 他本没有把这封邮件当回事，但为了保险起见，他还是打电话询问了公司的 IT 部门。仅仅几个小时之后，那个以色列人的邮件就得到了证实。这个骇人听闻的消息是真的：黎巴嫩真主党这个世界上最激进的叛乱组织，将他们公司的 IT 基础设施用于战略宣传。

两年之后，格鲁吉亚与南奥塞梯（South Ossetia）彻底反目，双方剑拔弩张，这使得俄罗斯与格鲁吉亚的政治局势也处在一种十分紧张的状态中。有报道指出，俄罗斯在格鲁吉亚这个亲西方的国家边境部署了大量装甲部队，对这个高加索国家摆出侵略姿态。格鲁吉亚突然遭到针对其主要网络服务器的大规模分布式拒绝服务（distributed denial of service，DDoS）攻击[2]，切断了他们与外界联系的能力，使得外界无法获悉任何有关格鲁吉亚的消息。这场网络攻击的第二天，俄军长驱直入，越过边境。

2009 年，伊朗纳坦兹核燃料浓缩工厂（Natanz Fuel Enrichment Plant）的科学家们苦思冥想了几个月却束手无策。虽然他们几乎将工厂的离心机数量翻倍，但浓缩铀的产量仍然停滞不前，甚至每况愈下。科

学家们绞尽脑汁也无法解决这个问题。试验排除了由机电故障引发的可能性。而且西门子 Step 7 软件发回的报告也显示控制器卡一直在接收正确的指令，这使得伊朗科学家们困惑不解。随后白俄罗斯一家小规模的安全公司在一台装有控制软件的电脑上发现了带有恶意软件的 U 盘。事实证明，过去几个月这个名为震网（Stuxnet）的秘密软件一直在干扰伊朗的核燃料浓缩设备。[3]

同年，美军在伊朗邻国伊拉克境内的一次反武装分子行动中，突袭了一处什叶派叛乱分子藏身的住所，除了一些武器和武装分子的反叛宣传资料以外，美军还缴获了一台电脑。当他们启动这台电脑之后，发现里面居然有美军“捕食者”（Predator）无人侦察机拍摄到的大量视频[4]，原来这些武装分子入侵到无人机的系统之中，因此可实时看到强大的无人机所拍摄到的一切。

2010 年，黑客入侵突尼斯政府网站，并在网络上公开了大量含有敏感信息的邮件[5]，向这个北非国家展示了 21 世纪“公开性”（Glasnost）的定义。尽管这些黑客深谙网络攻击之道，但他们却不属于任何政府或者传统组织，只是一个自发性黑客组织，称自己为“匿名者”（Anonymous）。被公布的资料并没有拉近突尼斯民众与政府之间的距离，反而加剧了本就已经紧张的政治局面。同年 12 月，突尼斯国内一位街头小贩因绝望而引火自焚，这引发了大量突尼斯民众走向街头抗议政府的暴行。自焚事件是整个革命的导火索，此后，这场名为“阿拉伯之春”（Arab Spring）的运动，在地中海周围的阿拉伯国家间如火如荼地展开。

2012 年，英国几位高级军官收到了他们的上司——一位北约指挥官在 Facebook 上发来的“好友请求”。[6] 为了和这位欧洲最高级别的军官之一搞好关系，他们接受了请求。此后这位高级指挥官，也就是他们的“新朋友”，可以轻易获得他们的个人资料并取得联系。但仅仅几天之后人们就发现这位所谓的“北约高级指挥官”其实只是个冒牌货。而这几位英国高级军官也在无意间向身份不明的第三方暴露了自己的私人信息和资料。

近几年，本书作者对网络战产生了浓厚的兴趣，从俄罗斯入侵格鲁吉亚开始到震网病毒和 Duqu 病毒的使用，再到被称为“影子网络”（Shadow Network）的国际网络间谍界等，网络战问题已经在许多国家的议程清单上成了重中之重，它开创了战争的一个新维度。为了更加深入地了解这个令人着迷的新维度，我们查阅了相关文献，但发现所有现有的记载都只是重新拼凑了信息安全的旧有知识，不过新瓶装旧酒而已，囊括的计算机安全领域的一些重要议题也都是尽人皆知的事。其他文献似乎也还能够从一个更加广阔的视野来看待这个话题——以高级政策的角度来认识网络战——探讨由此可能产生的法律责任和对国际关系的影响。这些文献都很实用，但都未能从操作性和战术性的角度来解读网络战。我们要了解三件事：当下网络战是如何开展的；面对冲突时，应该采取哪种网络行动；在什么情况下单一民族国家或者非单一民族国家的行动分子会参与到这些行动中来。我们希望在不忽视“信息安全”重要性的同时，又能超越它的范围去理解它。网络战不只是信息安全和规则的问题。因此本书也会重点从军事、社会、科学的层面去解读网络战。种种迹象表明，以上几点对网络战的形式都会产生显著的影响。但是，当下没有哪一本著作能够充分地从这些视角去探索网络战问题。

从结构上来看，本书与美国陆军军官学校（西点军校）的军事教学法很相似，两者都注重案例分析，在西点军校，军事教学从来不只是停留在武器系统上，而是通过历史上的战争实例来开展。因此，我们想要探讨的内容有：一场网络冲突中主要采取的行动有哪些；它们在何种情况下发生；行动中所应用的策略、技术和程序又有哪些。我们只采用那些已经得到公开的资料来进行案例分析，特别是计算机安全公司报告、学术期刊、会议论文，还有媒体报道。网络战和科技发展之间总是存在内在的联系，因此案例分析里也避免不了会有一些科学实验，在这些条件下进行的实验，比如第 8 章的“罗宾 · 塞奇”（Robin Sage）训练演习和第 10 章的“极光测试”（Aurora Test）试验，在现实世界中显然是可以重复的。此外，作

者会经常结合特定案例中的事件，来对科学发展提出自己的看法，引导我们对未来趋势的重大思考。还有，直到近来我们才认识到有许多大型公司其实都希望通过“军事化风格”来应对网络安全问题。[7] 这也是本书所采用的方式。

同时，我们也会研究这些案例背后所蕴含的军事、社会和政策方面的意义。比如，第 12 章中我们将谈到情报搜集在网络作战中的关键作用。第 6 章我们将对臭名昭著的黑客组织“匿名者”和其附属组织进行深入介绍。社会学在网络战争和社交网络相互作用的过程中，也扮演着很重要的角色，因此我们将用一整章的篇幅来对这个话题进行探讨。对于整本书而言，政策是另一条贯穿全书的线索。国家和地区的行动分子在进行攻击前，都显然会有一个决策过程。在谈及以色列、哈马斯（Hamas）以及黎巴嫩真主党（Hezbollah）如何利用网络攻击来扩大信息作战效果和影响世界舆论方面就会涉及政策扮演的角色（第 4 章）。

本书分为三个部分。第一部分主要介绍如何通过网络攻击来达到政治目的。这其中的内容包括：网络攻击是对传统军事行动的支援——具体来说，它是信息战的一个组成部分。我们要探讨的另外一个因政治目的而引发网络攻击的领域是国内矛盾，比如一国对国内持异见者发起网络攻击。在有些情况下，规模大又有能力的黑客组织在对政府非常了解的情况下，发起出于政治目的的网络攻击。(尽管有些组织的推诿否认到了让人信以为真的地步。）我们不使用计算机网络攻击（computer network attack，CNA）这个词的原因在于它的内容与信息安全相关，是一个更狭义的概念。我们将“网络攻击”定义为通过一个网络系统向另一个网络系统发起攻击的行为，是网络战行动的一个组成部分。

本书第二部分将把目光投向网络间谍和网络利用（exploitation）这两个方面。为了重点强调这些问题所带来的新影响，我们并没有使用计算机网络利用（computer network exploitation，CNE）等词汇，而是用网络间谍和网络利用这两个词取而代之。我们将网络间谍和网络利用看作是一种通

过技术来窃取目标信息系统数据的行为。这一部分将呈现的内容有针对无人机的网络攻击、社交网络利用和为达到利用目的而特别开发的高端恶意软件。

最后，本书第三部分是关于通过网络行动从而对一些物理基础设施发起攻击的行为。尽管这些行动都在计算机系统上发动，但目的却是破坏现实世界中的设施。这部分涉及的主题有工业控制系统（industrial control system）、电网，以及震网病毒，这是迄今为止针对基于计算机的基础设施攻击方面最出名的例子。

所以，欢迎来到《网络战》，本书的目标读者定位为信息技术和军事领域的专业人士，除此之外还有决策者、历史学家以及任何对网络战这个新兴领域感兴趣的人士。本书不要求按顺序阅读，因为每个章节都包含了该章节所需的知识（有些地方列明在书上哪些地方可以找到更多的背景知识）。最后，正如序言所提到的，我们在这本书的撰写过程中收获甚多，同时我们也希望广大读者可以和我们一样学有所获。

参考文献

1. Hylton H. How Hizballah Hijacks the Internet. *Time*; August 8, 2006.
2. Bumgarner J, Borg S. *Overview by the US-CCU of the Cyber-Campaign Against Georgia in August of 2008.* US Cyber Consequence Unit Special Report; http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf August 2, 2009 [accessed April 23, 2013].
3. Shakarian P. Stuxnet: cyberwar revolution in military affairs. *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-militaryaffairs; April 2011 [accessed April 11, 2013].
4. Gorman S, Dreazen YJ, Cole A. $26 software is used to breach key weapons in Iraq; Iranian Backing Suspected. *Wall Street Journal*. http://online.wsj. com/article/SB126102247889095011.html; December 17, 2009 [accessed March 17, 2012].
5. Al Arabiya. Wikileaks might have triggered Tunis' revolution. http://www.alarabiya.net/

articles/2011/01/15/133592.html; January 15, 2011 [accessed April 11, 2013].

6. Lewis J. How spies used Facebook to steal Nato chiefs' details. *The Telegraph*. http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html; March 10, 2012 [accessed June 21, 2012].
7. Kelly S. Executives advocate a military approach to cyber security. *CNN.com*. http://security.blogs.cnn.com/2012/08/13/executives-advocate-a-military-approach-to-cybersecurity/; August 13, 2012 [accessed September 14, 2012].

作者简介

保罗 · 沙克瑞恩（Paulo Shakarian）是美国陆军少校，同时也是一名积极开展网络安全、社交网络和人工智能研究的计算机科学家。他在科学和军事期刊上发表过 20 多篇文章，曾写过一篇名为《震网：军事中的网络战争革命》（*Stuxnet: Cyberwar Revolution in Military Affairs*）的文章，发表在《小型战争杂志》（*Small Wars Journal*）上，还有一篇《2008 年俄罗斯针对格鲁吉亚的网络战》（*The 2008 Russian Cyber–Campaign Against Georgia*）的文章，发表在《军事评论》（*Military Review*）上。他的科学研究得到了广泛的认可，许多主流新闻媒体，包括《经济学人》、《连线》和《自然》都刊登过他的文章。保罗在美国马里兰大学帕克分校获得哲学博士学位以及计算机科学专业的理科硕士学位。在西点军校获得计算机科学专业学士学位以及信息安全资深研究者身份。保罗在“伊拉克自由行动”中有过两轮作战经验，同时兼任多个军职。现在，他是西点军校的一名助理教授，讲授计算机科学与信息技术方面的课程。他的军事勋章包括有铜星勋章、嘉奖服役勋章、陆军嘉奖奖章以及美国陆军作战行动勋章。保罗的网址是：http://shakarian.net/paulo。

亚娜 · 沙克瑞恩（Jana Shakarian）是社会科学领域研究网络战、恐怖主义以及暴力行为的独立研究者。在美国马里兰大学计算文化动力学实验室当助理研究员，除了其他关于应用于军事以及安全问题的社会和计算科

学研究之外，还对东南亚恐怖组织做了大量研究。在西点军校网络科学中心担任过顾问。她除了是《对恐怖组织——拉什卡—塔伊巴组织的计算分析》（*Computational Analysis of Terrorist Groups: Lashkar–e–Tabia*）一书的合著者之外，还写过大量文章。亚娜已在德国美因茨约翰尼斯·古藤堡大学获得文化与社会人类学和社会学专业的文学硕士学位，她的论文主要是关于“新战争”理论。亚娜的网址是：http://shakarian.net/jana。

安德鲁·鲁夫（Andrew Ruef）是纽约 Trail of Bits 公司的一名高级系统工程师，擅长信息安全分析。安德鲁有将近十年的计算机网络安全和软件工程的工作经验，参与过的项目包括恶意软件逆向工程、计算机网络流量的安全分析、系统管理以及安全软件产品开发等。安德鲁写过很多关于信息安全的白皮书并在各大会议中发言，包括近日在德国 Dagstuhl 计算机研究中心的会议上发言。读者可以在 http://www.kyrus–tech.com/tag/andrew–ruef/ 找到关于安德鲁技术作品的示例。

本书中的所有观点均源自以上这些作者，不一定反映了美国国防部、陆军或西点军校的观点。

目录

序　言　1
前　言　3
导　言　5
作者简介　11

第1章 当前网络战的面貌　001
什么是网络战？　002
网络战是否确实对国家安全构成威胁？　003
溯源、欺诈和情报　005
信息安全　008

第一部分　网络攻击

第2章 2007年，网络政治攻击到来　015
信息依赖的脆弱性　016
基本却有效：拒绝服务　017
留下不需要的信息：网站篡改　019
拒绝服务攻击工具　020
追究责任的难度：为什么DDoS攻击难以溯源？　021
爱沙尼亚遭到网络攻击　022
对DDoS的一般反应　027
小结　028
推荐阅读　029

第3章 网络攻击如何支援俄罗斯的军事行动？ 032
2008年俄罗斯对格鲁吉亚的网络攻击 033
俄罗斯网络攻击的特点 036
准备应对网络敌人 041
小结 043
推荐阅读 043

第4章 擅讲故事者胜：中东网络战与信息战 046
黑客劫持平民IP地址：2006年黎以七月战争 047
网络战争中的平民："铸铅行动" 053
小结 057
推荐阅读 058

第5章 网络言论自由受限：俄罗斯和伊朗对国内反对派发动网络攻击 061
DDoS成为审查工具：反对派组织在网络战面前为何总是不堪一击？ 063
沉默的《新报》和其他俄罗斯反对派组织 068
伊朗：2009年大选如何招致猛烈的网络攻击？ 078
小结 088

第6章 非政府黑客组织的网络攻击：匿名者组织及其分支 099
"混沌的"开端：混沌计算机俱乐部 103
匿名者：4chan、7chan和其他论坛的起源 105
我们如何被4chan影响：模因 107
匿名者：图片、结构和动机 109
匿名者：外部联系和衍生品 117