[美] 詹姆斯·F·邓尼根 著
武鹏 译

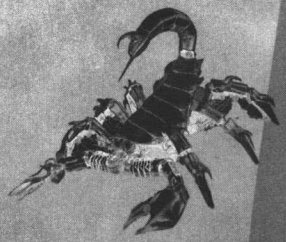
黑客的战争

——下一个战争地带

【关键词：战争 黑客 美国】

上海科学普及出版社

[美] 詹姆斯·F·邓尼根 著　　武鹏 译



黑客的战争

——下一个战争地带

上海科学普及出版社

图书在版编目（CIP）数据

黑客的战争——下一个战争地带/（美）邓尼根著；武鹏译. —上海：上海科学普及出版社，2006.7
ISBN 7-5427-2968-3

Ⅰ. 黑... Ⅱ. ①邓...②武... Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2006）第 019048 号

责任编辑 李重民

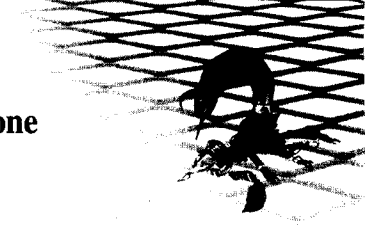
黑客的战争——下一个战争地带
［美］詹姆斯·F·邓尼根 著
武 鹏 译
上海科学普及出版社出版发行
（上海中山北路 832 号 邮政编码 200070）
http://www.pspsh.com

各地新华书店经销 常熟市新骅印刷有限公司印刷
开本 787×960 1/16 印张 17.75 字数 234 000
2006 年 7 月第 1 版 2006 年 7 月第 1 次印刷
印数 1—4100

ISBN 7-5427-2968-3/I·13 定价：28.00 元
本书如有缺页、错装或坏损等严重质量问题
请向出版社联系调换

感　谢

这本书的选题是沃尔特·札查里尤斯想出来的，鲍勃·舒曼帮助我按时完成了这本书。我还要感谢其他一些帮助我收集与这个选题有关信息的人，遗憾的是他们都不愿意看到他们的名字放在有关网络战的书上。他们确实喜欢这本书，但他们不愿受到那些脚本小子复仇性的骚扰。



前　言

本书是为普通读者写就的。尽管有一些历史和技术的问题，但我想大家还是能从中得到乐趣。其中一项挑战就是，如何通过可怜的英语将这些问题表达出来。当谈到个人电脑和因特网时，几乎不可避免地会遇上一些技术名词，所以在每一章前面都有一个小小的术语表，而且所有这些技术词汇在本书最后单词表里都可以找到。要把这些因特网术语用英语而不是术语（Geekish）写出来，要花费很多的精力，相反用术语表达会非常轻松，但如果用术语也许只有10%的人可以理解。因此别怕你对某些单词无法完全理解，其实你已经很接近答案了。

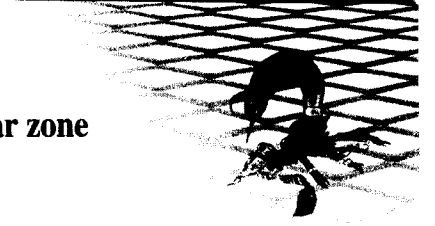
这些不可避免的技术语言（目前已经设计出来的）暗示着因特网和个人计算机将永远不会变成“工具”，最后所有这些计算和通信技术将变得更加简单且更具人性化，人们将不再为工具而烦恼，但是到那时候，它们将无法再被称之为“个人计算机”，而且许多所谓的工具使用起来将不会像它们的制造商所说的那样简便。许多工具与不断发展的微处理器革命（为保证个人电脑正常工作而安装在一块芯片上的微电脑）有关。小型计算机在当今应用广泛，通常被当作游戏机、手机和汽车的关键部件。有些制造商制造的微电脑控制的产品，已经让我们意识不到它们是由电脑控制的了。但是，迅速发展的科技总是像我们在商业活动中所说的“双刃剑”。人们在追求最新、最好的时候，往往会带来一些欠思考的低级缺陷。个人电脑，特别是因特网，已经纳入了那个范畴，因特网底层的技术非常复杂，没有人真正知道因特网是如何依靠上千种程序来进行工作的。这有点像一个游戏，但许多游戏规则还没有被揭示出来。不

管是什么人，谁发现了新的技巧就能前进一大步，或者成为大麻烦的制造者。

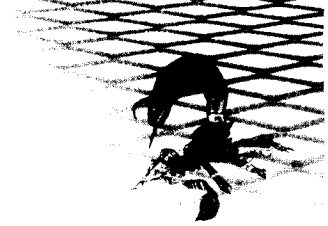
现在，大公司和银行已经不是因特网犯罪的主要牺牲品了，他们都有能力保护他们自己。目前最可能成为牺牲品的，就是普通的民众。而这本书就是希望给他们一个反击的机会。

Jfdummigan@ aol. com（另外还有 10 多个电子邮件地址，有的已经使用了 20 多年，其中有的还能够使用。）

詹姆斯·F·邓尼根



目　录



第一章　网络战和你

［本章术语］

电子公告牌（BBS）　一个允许用户通过电话线或因特网联接到公告牌的程序。通过该程序，用户可以阅读信息或向该公告牌的所有成员发布信息。因特网版本的电子公告牌是一个新闻组网络（Usenet），包含着数千个不同类别的独立部分。

网络战士　通晓如何利用通信网络如因特网进行攻击或保护己方网络不受此类攻击的军方或政府方面的专家。从第二次世界大战开始，这类“战争”被称作“电子战”，当因特网被牵涉进战争以后，平民志愿者也常常从事此项工作。

分布式拒绝服务（DDOS）攻击　使用不同的计算机向一个网站发送大量的数据。网站在同一个时间内只能为有限的客户服务，所以通常不会引发很大的问题，但如果有人有意识地通过分布式拒绝服务攻击、抢占一个网站的所有资源，该网站自然就无法对其他用户提供服务了。

服务器　一台操纵网站的电脑。服务器有点像我们在家里使用的个人电脑，但它装备了特殊的软件和高速的因特网联接线路。一般来说，只要有相应的软件和昂贵的高速因特网联接线路，任何个人电脑都能作为服务器使用。

系统管理员　负责维护网站、服务器或本地网运转的人。这是一个棘手的活儿，最基本的工作是保障服务器、网站或本地网运行的软件不断得到升级，以保证所有的程序运转正常。除此以外，还要防止闯入者危害系统安全。好的系统管理员总是比较缺乏，这使得大量的网站在遭

到黑客攻击时显得非常脆弱。

木马 黑客将其编制的程序放入疏于防范的目标电脑里，这台电脑有可能是一台服务器，也有可能是一台拥有有线电视调制解调器或数字用户网联接的个人电脑。木马程序有许多种，但它们有一个共同的特点，就是会和黑客进行联系，并能让黑客夺取一部分该电脑的控制权。通常，防病毒程序能够检测并删除木马程序。

我们正身处战争之中。我指的不是正在阿富汗或其他地方进行的反恐战争。这是一场通过因特网进行的战争。这个战争每天都在发生，你也许已经成为这些冲突的受害者了，它正在不断引起将军和政治家们的担忧。这就是**网络战**。这种新型的战争会进入连在因特网上的每一户家庭，上千万的因特网使用者将会受到很大的影响。

网络战是以电子网络和信息为武器，或者严格地说，是作为武器系统的一部分。网络战的这种形式起源于战斗机用电子手段对抗敌方的电子传感器和导弹。我们大多数的时候总是凭想像，以为网络战只会发生在网络上，但事情并非如此，尤其是当它可以被用于军事方面的时候。这里，我举一个最近发生的非常恰当的例子，那就是在2001年的阿富汗战争中，通过黑掉塔利班银行账户和服务器的网络战，和以信息、新闻为武器的信息战混合在一起。随着接下去的解释你会发现，信息战已经有几千年的历史，网络战也有超过100年的历史。真正与此不同的是，未来的网络战将发生在你自己家里的个人电脑上。

好消息，坏消息

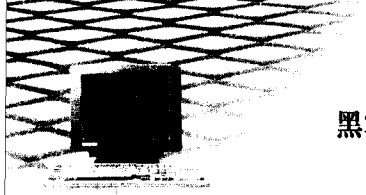
面对网络战也不是只有可怕的形势，这儿还有些好消息。

不过首先我想说说坏消息。是的，有许多黑客行为现在正在发生。你们当中的许多人都遭遇过通过email传来的恼人的蠕虫程序和病毒，或

许有些已经给你的电脑造成了损害。作为因特网基础设施一部分的大型网站也一样受到了攻击。结果就是有时有的网站你无法进行访问。这还不算是最可怕的。像我这样的专家可以坐在电视摄像机前面做出更出格的事情，这才是最可怕的。是的，这虽然是在理论上的，但确实有可能对因特网和联在网上的计算机、商业公司、政府部门、军事单位造成非常严重的破坏。不过，同时想要不成为受害者也非常简单。本书的最后一章将提供几条使你的机器保持相对安全的方法。

互联网用户中最容易受到伤害的，是那些通过永不断线的高速联接（有线电视线 CABLE 和电信宽带 DSL 等）上网的人。这些计算机对黑客有着强大的吸引力。因为它们大多没有被很好的保护起来，而且这样的计算机有很多。它们也是网络战士和黑客们的基本目标。而那些大型网站和大公司的网络中心，有足够的动力和金钱来推动他们采取保护措施。举例来说，从 2001 年 11 月 11 日以来，有记录显示众多来自中东的黑客试图黑掉美国发电站的网站，但从来没有得逞过。电站有良好的因特网保护机制，并装备了发现网络攻击者的装置，能显示出他们的位置。但是，上百万的普通宽带用户并不能得到像电站这样的保护装置。这些个人计算机成了网络战士发动攻击的理想基地。如果中东的黑客不能直接攻入核电站，他们会在成千上万的家庭电脑里放置大量的木马程序，并对军事、商业和政府网站的分布式拒绝服务发动攻击，迫使其关闭数日。实际上，一场真正大规模的攻击，也许可以使已瘫痪的因特网的主要部分瘫痪更长的时间。当然，这现象发生在遭遇攻击时反击措施没有处在“战备状态”的情况下。因此，“家用电脑里的木马”在可预见的未来里将成为因特网上的主要弱点和最有可能的战场。怀有敌意的网络战士可以利用这些暴露的个人计算机来进行各种“恶作剧”。除此之外，因特网上还有很多其他弱点，但没有比这个更明显的了。

不过，在你要去拔掉你的个人电脑的插头之前，这里还有一些好消息。



黑客的战争——下一个战争地带

整个因特网是一头巨大而不断变幻着的猛兽，幸运的是，如果没有一张地图，你就无法开展一次攻击。到今天为止，没有人能弄到这张地图，这并不是说这张地图不存在，这张地图肯定存在，只不过它被视为军事机密而被保护起来。不同于军用地图，因特网地图更像一本天书，它被因特网自身的改变不断地推动着，发生着扭曲。因为它拥有上百万个大型网站、超过20亿个页面和上百万程序员、系统管理员和捐助者不断改变着的因特网内容，所以无论任何人的地图都只能做到暂时的精确。有些国家承认拥有上千名士兵和平民在从事类似的网络战项目，但这是一种需要不断进行的尝试，因为他们中许多人的工作仅仅只是不断地更新这张地图的内容。如果没有准确的信息，网络武器就无法很好地发挥它的作用。

用于军事目的的因特网地图是非常机密的。没有人知道这张地图的内容有多全面。我们仅仅知道，如果你将一台新的服务器联上因特网，几个小时之内，数个匿名组织就会来调查它。如果你将这台服务器装扮成拥有军事和政府的功能，你就可以在几天之内等到更加野蛮的访问者。

尽管无法肯定对新服务器的关注是某些军事行动的结果，但我们知道，保留有价值的军事目标的线索是军事行动的一个标准步骤。到底是谁在做这些事情？这里有几个怀疑对象：美国、中国大陆和台湾地区、日本。因为他们自己宣称拥有网络军事单位。然而除此以外，还有上百万的人正在尝试扫描网络或者潜入网站寻找感兴趣、有价值的东西。这种行为现在被当作是一种业余爱好，而且钻了法律的空子。如果你给你的新服务器装了性能优良的侵入检测和监视工具。你就可以发现是谁在入侵你的网站。如果对某些扫描者进行追查，甚至会追踪到已知的、为网络战士提供基地的国家。但是，更多的入侵者是来自世界各地的黑客。他们可能是script kiddies（使用简单黑客工具的少年）、市场调查公司或黑客爱好者们，还有很多好事的人。他们为了各种各样的原因聚集在网上。

Script kiddies 只是要将你的服务器或个人电脑变成他们的娱乐工具，那些市场调查员则是要了解并利用你，还有一些无害的黑客爱好者们只是为了多了解一些网络知识，他们的大多数行动只是为了满足好奇心罢了。但是，如果在战争时期，网络战士会把你的个人电脑也变成战场，通过不断地扫描以发现因特网的新的发展。这是古老的军事侦察惯例的一部分，而且非常有用。这样，网络战士就可以利用那些疏于防范的服务器和一直开着的个人电脑，存放网络武器和其他一些工具。如果你的服务器或个人电脑符合他们的标准，那么它们就会被列入一个名单（然后他们会定期对你的机器加以扫描）或立即被使用起来。网络战士会连续不断地试验他们的工具或者武器，就像是在训练他们的军队。你的个人电脑会变成他们的根据地或者试验场，而你甚至毫不察觉。网络战士不得不学会的一个最重要的技巧就是秘密行动。突然袭击，然后消失得无影无踪，这种举动本身就是一种有价值的武器。

把战争带回家

是的，下一场战争将会发生在一个新的战场上——你自己的家里。网络战争是一场以控制因特网和大量的、组成网络的、我们的经济赖以运行的电脑为目的的战斗。这其中就包括你在家里使用的电脑。其实，小型的战斗已经屡见不鲜。你听说过的那些计算机病毒、蠕虫程序，仅仅是网络武器的一部分。它们可以关闭你的计算机，破坏你的计算机数据，危害国家级的电站、工厂、燃料供应线、通讯系统，甚至包括一些军事设施。许多以前释放的网络武器现在被业余爱好者使用着，而政府级别的网络战单位不断研发出更有威力的武器，准备在决定性时刻使用出来。平时你见不到那些超级病毒和怪兽般的蠕虫程序，因为一旦发动，受害者就会研究出对策来。但是，如果这些病毒是第一次被释放出来，这些军事级别的网络武器将会造成巨大的破坏。台湾曾经自吹它的网络

武器库里拥有上千个军事级别的计算机病毒。在2001年，仅仅3种病毒就占了该年度网络攻击报告的60%。恐怖组织也会把这些武器使用到他们的攻击中去。留心一下就会注意到，第一个感染了大量电脑的网络武器——“脑病毒”（the Brain virus）就是1980年在巴基斯坦被发展出来的。巴基斯坦仍然拥有大量的技术娴熟的程序员和网络专家。他们中的许多人为了过上更好的生活而离开了这个国家，但一些激进分子和组织比如塔利班和基地组织回来了。现在你可以理解为什么美国政府保持数个独立的因特网，使之完全不倚靠我们普通人使用的网络。这个代价昂贵的行动是有充分道理的。因为它对军事因特网用户提供了更多的保护。

为什么你的个人电脑会变成网络战场的一部分？这是一种最普通的伎俩——将木马程序悄悄地埋伏在尽可能多的计算机里。这些程序一旦收到启动信号，就会利用你的电脑对政府、商业公司和某些连在网上的军事单位发动攻击。这些安放在你个人电脑中的程序平时不太容易被检测出来，因此成千上万的个人电脑中任何时候都隐藏着木马程序。平时军事用途的木马程序对它们的宿主不会造成任何影响，不过它们一旦完成了肮脏的使命，还是会破坏宿主电脑里的数据，以达到掩盖其行踪的目的。

普通的黑客罪犯利用木马程序进行捣乱，网络战士又利用它们来赢得战争，为的是尽最大可能破坏敌对国家的经济和军事力量。在平时之所以会有那么多的木马程序出现，是因为那些平民黑客们为了向他人显示他们的聪明，才制造出来并激活它的。问题在于到底有多少台个人电脑被他们放置了木马程序。某些黑客一旦攻入一台机器，会在里面放上一千多种病毒。这些电脑中可能会有你的机器。要在个人电脑中放置木马程序轻而易举，因此如果能将木马程序放置在防范措施严密的服务器中，就会使那个成功的黑客更加声誉显赫。尽管在专业管理的网站中放置木马程序很容易被发现和清除，但还是会有一些野心家敢冒险一试。这有些像是病毒编写者的心态。真正吸引黑客们的，是他们可以利用宿主机