商业和政府决策者花点时间来读这本非常及时的书将是明智的选择。

—John Stanton，美国国家防御体系联盟

INFORMATION WARFARE

How to Survive Cyber Attacks

信息战

如何战胜计算机攻击

[美] Michael Erbschloe 著　　常晓波 等译

McGraw Hill

清华大学出版社

[美] Michael Erbschloe 著

INFORMATION WARFARE

How to Survive Cyber Attacks

信息战

如何战胜计算机攻击

常晓波 等译

清华大学出版社

(京)新登字 158 号

信息战:如何战胜计算机攻击
Michael Erbschloe: Information Warfare: How to Survive Cyber Attacks
EISBN: 0-07-213260-4

图书在版编目(CIP)数据

信息战:如何战胜计算机攻击/(美)埃尔布施勒著;常晓波等译. —北京:清华大学出版社,2002
书名原文: Information Warfare: How to Survive Cyber Attacks
ISBN 7-302-05877-6

Ⅰ. 信… Ⅱ. ①埃… ②常… Ⅲ. 信息技术—应用—战争—研究 Ⅳ. E919

中国版本图书馆 CIP 数据核字(2002)第 070902 号

出 版 者:清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
责任编辑:赵彤伟
版式设计:肖 米
印 刷 者:清华大学印刷厂
发 行 者:新华书店总店北京发行所
开 本:787×960 1/16 **印张**:13.5 **字数**:268 千字
版 次:2002 年 11 月第 1 版 2002 年 11 月第 1 次印刷
书 号:ISBN 7-302-05877-6/TP·3484
印 数:0001~4000
定 价:29.00 元

译者序

计算机自问世以来，给整个世界带来了几次巨变，使工业生产、办公方式和生活方式都发生了翻天覆地的变化。然而却很少有人能够觉察到这一片欣欣向荣的景象背后暗藏着的无数危机。在计算机硬件和软件技术空前发展的同时，病毒也开始盛行，特别是20世纪90年代末几次病毒攻击更是给世界造成了不可估量的损失。各种媒体到处充斥着“信息时代”“电子商务”之类的字眼，而病毒和黑客却未引起人们的广泛重视，更不用说人们对信息战的了解和重视程度了。

本书介绍信息时代特有的战争形式——信息战。作者将信息战分为10种战略形式，分析了信息战对经济的影响。然后讲述了一个十分精彩的故事：10个人是如何破坏全球互联网并造成一万亿美元损失的。从而让我们真正见识了信息战的危害。随后，这本书从不同角度、不同层面解释了信息战的各种战略战术，并分析了对策和目前面对的挑战。该书可以使我们从天下太平的假象中清醒，认真思考并作好准备。

在此，我们谨向为本书出版付出过辛勤劳动的所有人致以诚挚的感谢！

在与清华大学出版社计算机引进版图书编辑室合作的过程中，出版社的朋友们一丝不苟的工作态度使我们受益颇多。在此，致以诚挚的谢意！

需要说明的是，本书作者在分析和论证问题时均以美国为基本出发点，其中不乏出现一些与我们的观点不相符的看法。因此敬请读者在阅读过程中自行甄别、品评和参考。另外，由于我们水平有限，书中难免会出现一些错误，真诚欢迎各界朋友批评指正。

译者

2001 年 9 月于北京

本书从一个全新的角度审视了信息战的战略及其对私营公司的运转和经济生存能力的影响。而历史上则多是从军事角度来关注信息战的。虽然从军事角度看待信息战有其特定的优点，但这是建立在战争的传统概念的战略与战术之上的，其目的是为了达到军事目标或保护军事力量和军事工业联合体的基础设施。

我跳出了传统军事领域的视角，对信息战进行了跨越经济、政治、社会行为和国际关系的多学科分析，并研究了这些力量如何影响信息战攻击的发起和响应。本书介绍了一种分析信息战战略与战术的新方法，并对 10 种不同类型的信息战的潜在影响进行了深入探讨。

本书考察了信息战攻击中所用的战术，以及私营公司和政府部门应如何为响应这些攻击进行准备工作。另外本书还探究了信息战士的出现，以及这些战士如何影响国家安全和国际政治关系。本书最后分析了政府部门应怎样更好地为信息战的潜在可能性作好准备，并评估了未来计算机世界的警察所需的技能和个人品质。

致 谢

参与制作本书的 Osborne/McGraw-Hill 小组的主要成员包括 Jane Brownlow(组稿编辑)、Jim Helm(技术编辑)和 Deidre Dolce(项目经理)。其他成员有 Laurie Stewart(项目编辑)、Maureen Forys(计算机设计)、Lunaea Weatherstone(文字编辑)、Sachi Guzman 和 Tory McLearn(校对)以及 Jack Lewis(索引工程师)。他们都为本书的出版做了大量的工作。

还要感谢我的两个弟弟:Kelly Erbschloe 和 Joe Erbschloe。Kelly 对系统与冲突有一种与生俱来的高超理解力,并对未来的信息战有一些独特的见解,这些思想和见解的展现必将对信息战科学有所促进。与 Kelly 的讨论对于我能够系统地表达对信息战的看法是非常有帮助的。而 Joe 则对信息战的潜在影响有很好的理解,他的注释和评论使我深受鼓舞,真心希望所有策略制定者都具有像他那样透彻的理解力和洞察力。

我还想感谢三位以前的同事:Catie Huneke、Adam Harriss 和 Samir Bhavnani,是他们帮助我收集并分析了他们在 Computer Economics 公司工作时所遇到的计算机病毒攻击对经济所产生的影响的大量数据。在"爱虫"病毒攻击期间和攻击后,Catie、Adam 和 Sam 做了很多工作,为研究这些攻击所产生的影响作出了巨大贡献。他们还花了大量时间为评估影响的媒体和私营公司进行演示和分析,并为政府部门和调查员整理信息。他们现在都在追求实现自己的个人价值,我真心希望他们能够获得最大的成功。我还想感谢 Anne Zalatan、Kathryn Hall 和 Ginger Rittenhouse 的支持,他们坚持不懈地准备和发布研究结果。在此,还要表达我对 Bruno Bassi(Computer Economics 的前总裁)的谢意,感谢他大力支持我们的研究工作。正是因为所有这些人的精诚合作和努力工作,我们才得以对这个新领域顺利地开展研究,并取得了丰硕的成果。

简　介

本书从全新的独立视角来看待信息战。与其他信息战观点不同，我们的分析不是以军事为中心，有很多原因使我们抛弃了传统的军事观点。自从军方首次提出了信息战战略后，因特网已经大大改变了整个世界的通信和经商方式。全球化的通信基础设施使更多的人有可能发动信息战。这样就使信息战的威胁远远超过了 1990 年时的情况，而且攻击目标的范围也变得更为广泛。

对信息战的总体考虑

总体上，研究信息战不能脱离战争。从传统意义上讲，很多团体已经有能力发动不同类型的战争。大型的军事组织具有精密的战术和武器，就像我们在海湾战争中所看到的。在越南，专业的但很零散的游击队也是装备精良、集中控制的军事组织。在墨西哥，小股的自由战士决心与整个国家的军队和警察对抗。在阿富汗，本地武装力量战胜了前苏联军队。换句话说，世界上的战争各式各样。

在因特网出现以前，信息战是天才之间的斗争。而因特网的广泛使用、对全球通信系统的易访问性以及丰富的软件工具等，使得信息战的等级降低到了一般类型战争的水平，即几乎任何人都可以发起信息战攻击。

10 种信息战战略的战术都很类似。区分这些战略的是战争目的和这些好战者的方式与动机。例如在破坏性信息战战略中，一次精密的军事行动可以彻底摧毁一个国家或一个地区的信息技术和通信基础设施。在持续恐怖主义信息战战略中，一群资金雄厚但规模较小的恐怖分子可以攻击一个国家、一个城市、一个工业园或一家公司，使其运转停滞或严重地抑制其经济活动。因特网以多种方式使得某些信息战战略廉价并易于实施，从而

几乎任何人都可以使用这些战略。

在我们的分析中，信息战所包含的 10 种不同战略可以彻底摧毁或部分瘫痪目标国家、地区或人群的军事战斗能力以及工业和制造业的信息基础设施，或基于信息技术的民间和政府的经济活动。军事组织、恐怖分子或流氓罪犯可以使用这些战略去攻击军事系统、政府部门、工业基础设施和通信系统，还有民间经济服务（如电子商务）。本书将在第 1 章中阐述这 10 种战略。

是否会发生及何时会发生信息战是问题吗？

第二次世界大战末期，核战争的威胁笼罩着整个世界。或许核战争的危险依然存在，但在世界人民的意识中已经渐渐模糊。核毁灭没有发生，但是有可能发生，而人类所拥有的核武器足以毁灭整个星球。我们现在进入了信息时代，面临着虚拟毁灭的可能性，而不是实际的毁灭。信息战会发生吗？何时发生？敌人是谁？这些是 21 世纪每位信息战规划者和战略家要为下一次大战作准备时所必须回答的问题。

长期以来军事准备工作的重点集中在制定规划以保护自己国家的基础设施免受攻击，并摧毁敌人的基础设施。这当然需要谨慎并值得去投入。但是在面对大批信息战士攻击我们的经济盟国时，应该做些什么好呢？什么都做不了！尤其是考虑到全球经济的动态性质时更是如此。任何有能力发动全面信息战攻击的国家在对一个超级经济大国成功地发动了信息战攻击的同时，必将受到同样的（甚至可能更大的）经济损失，因为全球经济是如此的一体化，以致于根本无法躲避相关的影响。

另一方面，恐怖分子和流氓罪犯并不顾虑有什么需要保护的，也常常不需要依靠什么，所以他们有可能从成功的攻击中获利。美国军方依然在准备打大规模的战争，其装备精良足以对抗大规模的军队。军方的注意力集中在保护基础设施上，而刚刚萌芽的数字经济的基础在此堡垒之外，很容易成为攻击者的目标。实际上，基础设施的确应该保护，但也真正到了需要开始考虑基础设施之外的保护战略的时候了。第 1 章在一个全新的框架中分析了信息战的经济性，从全新的角度审视了信息战的动态性质及特性。

信息战士的新目标

恐怖分子攻击的是系统的弱点，而流氓罪犯是盗取最有价值的和保护措施最弱的信息。这两种人有自己的成本/收益计算方式。恐怖分子和流氓罪犯是未来的信息战威胁；他们不会攻击基础设施，这不仅是因为那里的防卫太严密了，而且也因为那里很少有机会让恐怖分子完成个人表演或让流氓罪犯得到金钱。恐怖分子和流氓罪犯更不会去攻击军方。

当然，恐怖分子喜欢头版头条消息和个人表演，而且喜欢让人们害怕自己，同时让一

国或多国的政府陷入尴尬的境地。流氓则喜欢金钱，他们更愿意去偷而不是去战斗。流氓的动机是钱，而不是名，当然更不会像如此之多的恐怖主义斗士那样出于宗教救助的目的为他们的国家和神开展圣战而践踏自己的生命。

恐怖分子和流氓会在完全避开军方的情况下，给国家经济带来巨大的损失。他们会攻击最容易攻击的对象，而诸如电子商务公司、银行和股票经纪人等机构相对于庞大的军方通信系统和防卫严密的电子工具和电信基础设施来说，是非常容易受到攻击的。在第2章详细讨论信息战的经济影响。

第3章描述了一个大规模攻击的场景，但不是由军方发起的，而是由恐怖分子发起的。它讲述了10个人如何造成严重的经济损失。该场景名为PH2(Pearl Harber Two)，即珍珠港第二。这是完全可能会发生的一个惊心动魄的事件，实际上，PH2小组在攻击中使用的所有方法、黑客工具和漏洞都不外乎是那些已被提出的战术和技术。这种恶作剧和战争之间的区别仅在于如何将这些战术和技术组合使用、以什么次序、什么频率使用。

新的武器和防卫战略

信息战的发动方式依赖于攻击者在发动攻击时所拥有的资源。不断有新技术涌现出来帮助防御者抵御攻击者，而同时又有很多可供攻击者用来攻破防御者防线的新武器。第4章介绍了一种评估防御信息战和进攻信息战能力的过程。第5章则从军事角度研究了信息战的战略与战术。

第6章通过从公司角度考察信息战的战略与战术，讲述了可能变成信息战直接目标的私营公司的防御性战略。第7章讲述了计算机恐怖分子和罪犯的出现，并分析了恐怖分子和流氓在信息战中占上风的原因。第8章阐述了信息战中工业动员的重要性和过程，即分析信息战中技术公司的协调需求。

大多数战争都会造成平民的伤亡，信息战攻击则会在经济上伤害甚至打垮平民。第9章研究了信息战对在信息高速公路上旁观的无辜百姓(也许不是无辜的)的影响。重要的是计算机人士要理解发生了什么，或者更为重要的是，军事规划者必须了解下一次战争对每个人的经济影响，尤其是那些其资产与计算机产业相关的人，或者是那些其资产依赖于由西方国家金融机构维护的大量数据所构成的信息系统的人。

新型的信息战士

并非所有的新型信息战士都是好人。实际上，坏人的数目很容易超过好人。第10章阐述了游荡在计算机世界中的新兴恐怖分子和流氓罪犯。重要的是要去了解这些人，因为他们最有可能成为信息战侵略者。第10章审视了过去的犯罪并推测了未来的犯罪，从

而深入分析了新技术恐怖分子和罪犯的想法和动机。第 10 章阐述了信息战士的动机，这些人有一些服务于好人，另外一些服务于邪恶势力。这一章还研究了为什么有些计算机天才会感到做一名黑暗的信息干将要比在新泽西某银行工作，过那种单调的程序员生活更具有吸引力。

计算机司法部门面对的挑战

处于信息战前沿的防御者们已经发现，找到合格的信息战士并不是一件容易的事。如果需要招募足够的人选，那么信息战士的招募和培训就十分关键。第 11 章讲述了其过程和挑战，还讲述了好人的智力和动机，以及他们的培训需求、薪资范围和防卫人员可能面对的各种诱惑。另外还研究了司法部门的需求，即发展信息高速公路巡警和描绘计算机恐怖分子和流氓罪犯的方法论。

阅读本书时需要记住的事情

作者在最近五年间会见了数百名涉及计算机安全、信息战规划、情报收集和司法部门的人士。这些会见导致了各种项目，包括市场分析、产品评估和期刊杂志的论文。需要说明的是，在所有项目中会见的人都没有危及任何机密材料。虽然他们的信息有助于作者描绘出分析的基础框架，但本书的工作是基于一个完全独立的视角，绝对没有任何内部人员泄密的内容，也不包含与军事组织和司法部门相关的任何机密信息。