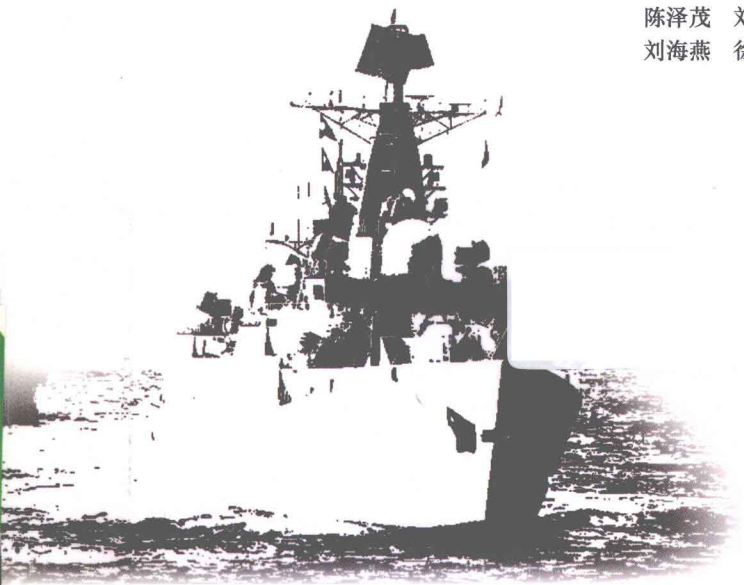
海军新军事变革丛书

总策划：魏　刚　　主　编：马伟明

赛博战与赛博恐怖主义

[新西兰] Lech J. Janczewski
[美] Andrew M. Colarik　等著

陈泽茂　刘吉强　　等译
刘海燕　徐　韬　　主审



CYBER WARFARE AND CYBER TERRORISM

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

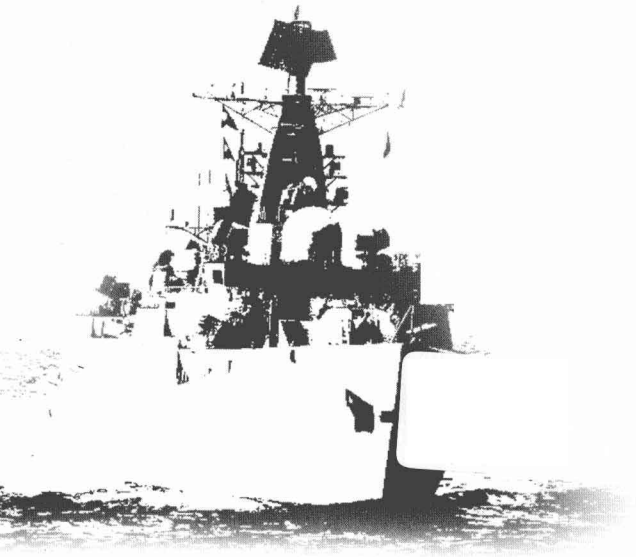
海军新军事变革丛书

总策划：魏　刚　　主　编：马伟明

赛博战与赛博恐怖主义

[新西兰] Lech J. Janczewski
[美] Andrew M. Colarik　等著

陈泽茂　刘吉强　　等译
刘海燕　徐　韬　　主审



電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

版权贸易合同登记号：图字 01-2013-0849

图书在版编目（CIP）数据

赛博战与赛博恐怖主义 /(新西兰) 简泽威斯基(Janczewski,L.J.) 等著；陈泽茂等译.
—北京：电子工业出版社，2013.3
（海军新军事变革丛书）
书名原文: Cyber warfare and Cyber terrorism
ISBN 978-7-121-19610-2

Ⅰ. ①赛… Ⅱ. ①简… ②陈… Ⅲ. ①信息战－文集 Ⅳ. ①E869-53

中国版本图书馆 CIP 数据核字（2013）第 030202 号

责任编辑：张　毅　　文字编辑：吴浩源
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：720×1000　1/16　印张：44.25　字数：640 千字
印　　次：2013 年 3 月第 1 次印刷
定　　价：135.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

赛博战与赛博恐怖主义

主审 刘海燕
主译 陈泽茂 刘吉强
审稿 黄定超
翻译 付 伟 朱婷婷 叶 清 赵俊阁
徐建桥 柳景超 夏学知 卢 飞
常晓林 邢 彬

海军新军事变革丛书

《海军新军事变革丛书》第二批总序

当今世界，国际战略格局正在发生深刻变化。传统安全和非传统安全威胁因素相互交织，霸权主义、强权政治有新的表现，恐怖主义、极端主义、民族分裂主义此起彼伏，和平与发展的车轮在坎坷的道路上艰难前行。

发端于20世纪70年代的世界新军事变革，从酝酿、产生到发展，经历了近四十年由量变到质变的过程。海湾战争、科索沃战争、阿富汗战争以及伊拉克战争这几场高技术条件下局部战争确定了世界新军事变革的发展轨迹和基本走向，展现了未来信息化战争的主体框架。这场新军事变革就是一场由信息技术推动，以创新发展信息化的武器装备体系、军队编制体制和军事理论为主要内容的世界性军事变革。

世界军事变革大势促使军队改革步伐加快。世界范围的军事变革正在加速推进，这是人类军事史上具有划时代意义的深刻变革。美国凭借其超强的经济和科技实力，加快部队结构重组和理论创新，大力研发信息化武器装备，积极构建数字化战场与数字化部队。目前正大力深化军事转型建设，通过发展航空航天作战力量等40多项措施，进一步提高军队信息化程度和一体化联合作战能力。俄军也以压缩规模、优化结构、组建航天军、争夺制天权等为重点，全面推行军事改革，着力恢复其强国强军地位。英、法、德等欧洲国家和日、印等亚洲大国，则分别推出军队现代化纲领，努力发展最先进的军事科技，谋求建立独立自主的信息化防务力量。

世界新军事变革的发展趋势是：在人才素质方面，加速由简单操作型向复合知识型转化；在军事技术方面，加速由军事工程革命向军事信息革命转化；在武器装备方面，加速由机械化装备向信息化装备过渡；在战争形态方

面，加速由机械化战争向信息化战争转变；在作战理论方面，正在酝酿着全方位突破；在军事组织体制方面，正朝着小型化、一体化、多能化的方向发展。此外诸如战争本质、军事文化、军事法规等方面都在悄然发生变化。

胡锦涛主席指出："我们要加强对世界新军事变革的研究，把握趋势、揭示规律，采取措施、积极应对，不断加强国防和军队现代化建设，为全面建设小康社会、加快推进社会主义现代化提供可靠的安全保障。"今天的人民海军正承担着完成机械化和信息化建设的双重历史任务，时不我待，形势逼人，必须顺应潮流，乘势而上，积极推进中国特色军事变革，努力实现国防和军队现代化建设跨越式发展。

信息时代的人民海军，责无旁贷地肩负着国家利益拓展、保卫领土完整的历史重任，我们只有以大胆创新和求真务实的精神全面推进军事技术、武器装备、作战理论、体制编制、人才培养等方面的变革，才能赶上时代的步伐，逐步缩小与西方强国之间的差距，最终完成信息化军队建设的重大任务，打赢未来的信息化战争。

根据海军现代化建设的实际需求，二〇〇四年九月以来，海军装备部与海军工程大学以高度的政治责任感和思想敏锐性，组织部分学术造诣深、研究水平高的专家学者，翻译出版了《海军新军事变革丛书》。丛书着重介绍和阐释世界新军事变革的"新"和"变"。力求讲清世界新军事变革进入质变阶段后的新变化、新情况，讲清信息化战争与机械化战争、信息化军队建设与机械化军队建设在各个领域的区别和发展。其中二〇〇四年至今陆续出版的第一批丛书，集中介绍了信息技术及其应用， 出版以来深受读者好评。为更好地满足读者的需求，丛书编委会编著出版了第二批系列丛书。与第一批丛书相比，更加关注武器装备、军事思想、战争形态、军队建设编制等全局性问题，更加关注大型水面舰艇、新型潜艇、作战飞机、远射程导弹等新一代武器装备，是第一批系列丛书的发展深化。

丛书编委会和参加编写的同志投入了很大精力，付出了辛勤劳动，取得了很好的成果。相信第二批丛书为深入学习领会军委国防和军队建设思想、了解和研究世界新军事变革提供有益的辅助材料和参考读物，在加速推进中国特色军事变革的伟大实践中发挥应有的作用。

中央军委委员
海 军 司 令 员 吴胜利

二〇〇九年七月十五日

译 者 序

随着全球信息网络化的发展，世界各国的军事力量、经济力量、社会生活和国家管理越来越依赖关键基础设施和以网络为基础的信息系统。这些关键基础设施日益自动化并相互联结，使得以关键基础设施和信息网络为攻击目标、采用网络手段实施的各类赛博攻击行为，对国家安全和社会稳定构成的威胁也日益严重。2000 年 12 月克林顿总统签署的《全球时代的国家安全战略》文件，将赛博安全列入国家安全战略，成为国家安全战略的重要组成部分，这标志着赛博安全正式进入国家安全战略框架，并具有独立地位。

为便于读者阅读，我们给出下面的“导读”。“导读”对基本概念进行了阐述，概要介绍了近年来该领域的发展动向，使读者能够从整体上了解该领域，帮助读者理解和区分一些相似的概念，在时间受限时去重点选读感兴趣的章节。

赛博战与赛博恐怖主义的概念

赛博战（Cyber Warfare）是指使用计算机入侵技术和其他能力对敌方信息基础设施实施作战，试图影响其国家安全或者影响其军事行动。它强调的是赛博空间的争夺和控制。作为信息时代战争的一种表现形式，近年来，赛博战受到了广泛重视。

赛博恐怖主义（Cyber Terrorism）是英国《反恐怖主义法案 2000》中首次明确提出的一个概念，“9 • 11”恐怖袭击事件发生后，美国国会通过的反恐法案，将“赛博恐怖主义”列为新的法律术语。美国国防部将赛博恐怖主义定义为：利用计算机和电信能力实施的犯罪行为，以造成暴力和对公共设施的毁灭或破坏来制造恐慌和社会不稳定，旨在影响政府或社会，实现其

特定的政治、宗教或意识形态目标。

1. 赛博空间概念及作战内涵

20 世纪 90 年代，学术界对赛博空间（Cyber Space）的概念进行了不断的探讨，形成的看法是，赛博空间基本与互联网同义。进入 21 世纪后，赛博空间受到了美国政府和军方的广泛重视，并随着对其认识的不断深入，多次对其定义进行了修订。美国国家安全第 54 号总统令将**赛博空间**定义为：相互交织的信息技术基础设施，包括互联网、通信网络、计算机系统以及关键工业领域中嵌入式处理器或控制器，是美国国家基础设施的一部分。2006 年 12 月，美国参谋长联席会议发布的《赛博空间行动国家军事战略》将**赛博空间**定义为：利用电子学和电磁频谱，经由网络化系统和相关物理基础设施进行数据存储、处理和交换的域。2008 年 3 月，美国空军发布的《美国空军赛博空间战略司令部战略构想》将**赛博空间**定义为：通过网络系统和相关的物理性基础设施，使用电子和电磁频谱来存储、修改或交换数据的物理域，主要由电磁频谱、电子系统以及网络化基础设施三部分组成。由此可见，对赛博空间的认识经历了从传统的网络空间概念到一种涵盖所有电磁频谱的物理领域的过程。

美军认为，通过对赛博空间的控制来确保攻击敌人，并确保免受敌人攻击的行动自由，是维护美国安全的关键因素，而夺取赛博空间优势的关键是实现跨越整个电磁频谱的“三个全球能力”，即全球警戒、全球到达和全球作战能力。全球警戒是在整个电磁频谱内的感知能力和信号发送能力。全球到达要求具有连接和传输能力，利用广泛的通信网络在全球范围近乎光速移动数据。全球作战能力是威胁或打击任何电磁能量目标，并最终在所有领域内实现动能或非动能作战效果的能力。通过这三个能力确保美军在必要的时候保护己方基础设施，指导军事作战，同时削弱或消除敌方军事能力。

2. 与赛博战相关的其他概念

电子战（Electronic Warfare）是为了打击敌人或为了控制电磁频谱而采取的任何使用电磁或者使用定向能武器的行为。电子战的形式有：电子攻击、

电子防护和电子支援。

信息战（Information Warfare）的概念比较宽泛，有很多解释。一个早前被军方采纳的观点是：信息战是用来使用和管理信息以达成针对对手的全面优势。在美军 2006 年颁布的《信息作战条令》中，已经删除了信息战的提法，取而代之的是信息作战（Information Operations）。

信息作战，包括心理战、军事欺骗、作战安全（Operational Security）、计算机网络作战（Computer Network Operation）、电子战五个核心能力。信息作战概念起源于 20 世纪 90 年代，其内涵源自广义的信息战和早期的指挥控制战，目前已被写入美军的作战条令。

网络战（Network Warfare）一般是指网络支援下的战争，或者网络条件下的战争，其职能是作战保障。在作战中，Network Warfare 处于从属地位，一切服从于物理领域中实体部队的作战需求。

网络作战（Network Operations）是一种作战框架，包括态势感知、指挥和控制三个基本任务。美军对网络作战的指挥权和控制权特指：与国防部和全球网络作战力量协调一致，完成对其全球信息栅格的操控、管理和防御，以确保美国在信息领域的优势。网络作战最开始包括网络管理、信息安全、信息分发管理，目前已经演化成全球信息栅格的企业管理、网络安全和内容管理。

3．与赛博恐怖主义相关的其他概念

传统恐怖主义，指恐怖组织或恐怖分子，继承历史沿传下来的恐怖行为方式，使用常规武器袭击目标，造成一定伤害和破坏的恐怖主义。如采用常规武器对重要人物、重要目标实施枪击、爆炸、绑架劫持等行为均属于传统恐怖主义的范畴。

黑客，英文“Hacker”的音译。早期的黑客是指那些具有高超的计算机技术、勇于探索未知事物并且乐于助人的程序员，这个词起初并无贬义。随着网络的广泛应用和电子商务的兴起，一些黑客凭借自己的技术，侵入个人、企业和国家的计算机系统，破坏、篡改或窃取其中的数据，或妨碍系统的正

常运行。现在，一般把这些以非法方式侵入他人计算机系统，并对他人计算机系统实施破坏活动的人都称为黑客。

赛博恐怖主义与黑客行为的本质区别，在于是否具有政治目的，是否构成恐怖效果。例如，英国政府在《反恐怖主义法案 2000》中将黑客作为打击对象，但只有影响到政府或者社会利益的黑客行动才能被划为“恐怖行动”。

欧洲理事会的《赛博犯罪公约》将赛博犯罪定义为：“危害计算机系统、网络和计算机数据的机密性、完整性和可用性，以及对这些系统、网络和数据进行滥用的行为。”与赛博恐怖主义相比，赛博犯罪的破坏性和影响力较低。赛博恐怖主义是赛博犯罪的恶性发展，它会破坏目标国家的政治稳定和经济安全，引发巨大的轰动效应。

赛博安全领域的新发展和新挑战

正如原著序言中所说的那样，本书是基于作者们在 21 世纪初的理解，对赛博战和赛博恐怖主义领域中的相关难点、问题和研究成果的回顾。作为读者阅读的补充，下面简要介绍原著中较少涉及或没有涉及的赛博安全领域中的重要进展。

1. 可信计算

21 世纪是信息的时代。一方面，信息技术和产业高速发展，呈现出空前繁荣的景象。另一方面，危害信息安全的事件不断发生，信息安全形势十分严峻。人们已经认识到，大多数安全隐患来自于微机终端。因此，必须提高微机的安全性，从终端源头控制不安全因素。这一技术思想推动了可信计算的产生和发展。

目前，关于可信尚未形成统一的定义，不同的专家和不同的组织机构有不同的解释。主要有以下几种说法：（1）国际标准化组织与国际电子技术委员会 ISO/IEC 在其发布的目录服务系列标准中，基于行为预期性定义了可信性：如果第 2 个实体完全按照第 1 个实体的预期行动，则第 1 个实体认为第 2 个实体是可信的；（2）ISO/IEC 15408 标准将可信定义为：参与计算的

组件、操作或过程在任意的条件下是可预测的，并能够抵御病毒和一定程度的物理干扰；（3）国际可信计算组织（TCG）用实体行为的预期性来定义可信：一个实体是可信的，如果它的行为总是以预期的方式，朝着预期的目标；（4）沈昌祥院士认为，可信计算系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统，可信包括许多方面，如正确性、可靠性、安全性、可用性、效率，等等。但是，现阶段，系统可信性的最主要方面是其安全性和可靠性。

下面介绍近年来可信平台模块、可信计算平台、可信软件、可信网络连接和远程证明等方面的研究动态。

1）可信平台模块

TCG 设计的可信平台模块（TPM）是可信计算平台的信任根，是可信计算的关键技术之一。TCG 定义的可信计算平台信任根包括：可信测量根（RTM）、可信存储根（RTS）和可信报告根（RTR）。其中，可信测量根是一个软件模块，可信存储根由可信平台模块芯片和存储根密钥组成，可信报告根由可信平台模块芯片和根密钥组成。TCG 的 TPM 设计在总体上是很成功的，它体现了以硬件芯片增强计算平台安全的基本思想，为可信计算平台提供了信任根。TPM 以密码技术支持了 TCG 的可信度量、存储、报告功能，为用户提供确保平台系统资源完整性、数据安全存储和平台远程证明。但是，因成本方面的考虑以及希望回避对称密码在产品出口方面的政策障碍，TCG 的 TPM 设计存在一些明显的不足。为此，TCG 开始制定 TPM 的新规范，并将其命名为 TPM.next。

2）可信计算平台

TCG 首先提出可信计算平台的概念，而且具体化到可信 PC、可信服务器、可信 PDA 和可信手机，并制定了相应的技术规范；我国也在制定相应的技术规范。目前，可信 PC 机已经在国内外投入实际应用，武汉大学研制出我国第一款可信 PDA。可信服务器方面，TCG 组织于 2005 年发布了适用于所有架构的通用可信服务器规范，描述了各种具体架构可信服务器所必须

遵循的特性和要求，以及可信服务器对 TPM 的要求。TCG 在 2006 年又发布了基于通用服务器规范的安腾架构服务器信任链建立流程。

3）可信网络连接

面对各种安全风险与威胁，仅有终端计算环境的可信是不够的，还应把可信扩展到网络，使得网络成为一个可信的计算环境。由于网络的复杂性，构建可信网络的目标是困难的。因此，TCG 首先考虑了相对比较容易实现的可信网络连接问题。可信网络连接（TNC）是将可信计算机制延伸到网络的一种技术，它是指在终端接入网络之前，对用户的身份进行认证。如果认证通过，就对终端平台的身份进行认证；如果认证通过，再对终端平台的可信状态进行度量；如果度量结果满足网络接入的安全策略，则允许终端接入网络，否则将终端连接到指定的隔离区域，对其进行安全性修补和升级。TNC 是网络接入控制的一种实现方式，是一种主动性的网络防御技术，能够将大部分的潜在攻击在发生之前进行抑制。2009 年 5 月，TCG 发布了 TNC 1.4 版本的架构规范。目前已经形成了以架构为核心、多种组件之间交互接口为支撑的规范体系结构，实现了与微软的网络访问保护之间的互操作，并将一些规范作为建议草稿提交到互联网工程任务组的网络访问控制规范中。目前已经有多家企业的产品支持体系结构。

4）远程证明

远程证明是架构中可信评估层与可信验证层功能的结合，它是指网络中的两个结点，一个结点将自己平台的某些信息使用约定的格式和协议向另一个结点报告，使得另一结点能够获得这些信息，并判定该平台的可信状态。远程证明的初衷就是允许两个结点在进行交互之前判断对方平台的可信状态，如果平台的可信状态符合交互的要求，则允许结点进行交互。目前针对远程证明的研究主要集中在远程证明的协议、交换的信息，以及信息的格式等方面。

2．移动自组织网络安全

移动自组织网络（Mobile Ad Hoc Network, MANET）是一种在没有固定

基础设施的条件下，由系统中的通信结点通过分布式协议互连或组织起来的网络系统。移动自组织网络所具有的自组织等特点使其在包括军事、救灾抢险等环境受到广泛关注。与其他传统通信网络相比，MANET 具有如下主要特点：

（1）动态变化的网络拓扑。在 MANET 中，网络结点能够以任意速度和任意方式在网中移动，并随时可能关闭无线发射装置，再加之天线类型多种多样、无线信道间互相干扰以及发射功率变化、地形和天气等综合因素的影响，移动结点间通过无线信道形成的网络拓扑随时可能发生变化，而且变化的方式和速度都难以预测。

（2）无中心和自组织。理想情况下，MANET 中所有结点的地位是平等的，没有绝对的控制中心。网络中的结点通过分布式算法相互协同，协调彼此的行为，无需人工干预和任何其他预置的网络设施。

（3）多跳路由。MANET 网络结点的发射功率限制了其覆盖范围，当它要与覆盖范围之外的结点通信时，需要中间结点寻找并转发数据（多跳路由）。MANET 多跳路由是由网络结点协作完成，每个结点兼备主机和路由器两种功能作为主机，结点需要运行用户应用；作为路由器，结点需要运行路由协议，并根据路由策略和路由表参与分组转发和路由维护。

（4）无线传输带宽受限。无线信道的理论带宽一般较有线信道带宽低。考虑到竞争共享无线信道产生的冲突、信号衰减、噪声和信道之间干扰等多种因素，实际的无线传输带宽远远低于理论最大值。这样，MANET 结点的网络带宽将非常有限。

（5）存在单向信道。受地形环境或发射功率等因素的影响，MANET 结点间可能产生单向无线信道。

（6）移动终端的局限性。出于移动性考虑，移动结点一般都具有携带方便、轻便灵巧等好处，但是也存在能量受限、内存较小、CPU 性能较低等缺陷。

当前，MANET 已经成为一个热门的研究领域，与之相关的安全技术也

得到了广泛关注。由于MANET采用开放的、无中心的网络结构，结点共享无线资源，网络拓扑高度动态变化，因此其安全性较差，更加容易受到被动窃听、主动入侵、拒绝服务、剥夺“睡眠”等网络攻击。传统的网络安全机制不适用于MANET，需要在安全路由、信息加密、鉴权认证、入侵检测等方面研究适用的安全技术。

3．云计算安全

近年来，社交网络、电子商务、数字城市、在线视频等新一代大规模互联网应用的发展迅猛。这些新兴的应用具有数据存储量大、业务增长速度快等特点，使企业在信息系统的部署和升级方面，面临巨大的周期和成本压力。为了解决上述问题，2006年Google、Amazon等公司提出了“云计算”的构想。

1）云计算的概念

根据美国国家标准与技术研究院（NIST）的定义，云计算是一种利用互联网实现随时随地、按需、便捷地访问共享资源池（如计算设施、存储设备、应用程序等）的计算模式。中国云计算网将云计算定义为：云计算是分布式计算（Distributed Computing）、并行计算（Parallel Computing）和网格计算（Grid Computing）的发展，或者说是这些科学概念的商业实现。Forrester Research的分析师James Staten将云计算定义为：云计算是一个具备高度扩展性和管理性并能够胜任终端用户应用软件计算基础架构的系统池。

虽然目前云计算没有统一的定义，结合上述定义，可以总结出云计算的一些本质特征，即分布式计算和存储特性，高扩展性，用户友好性，良好的管理性。云计算技术具有以下特点：

（1）云计算系统提供的是服务。服务的实现机制对用户透明，用户无需了解云计算的具体机制，就可以获得需要的服务。

（2）用冗余方式提供可靠性。云计算系统由大量商用计算机组成机群向用户提供数据处理服务。随着计算机数量的增加，系统出现错误的概率大大增加。在没有专用的硬件可靠性部件的支持下，采用软件的方式，即数据冗

余和分布式存储来保证数据的可靠性。

（3）高可用性。通过集成海量存储和高性能的计算能力，云能提供一定满意度的服务质量。云计算系统可以自动检测失效结点，并将失效结点排除，不影响系统的正常运行。

（4）高层次的编程模型。云计算系统提供高级别的编程模型。用户通过简单学习，就可以编写自己的云计算程序，在“云”系统上执行，满足自己的需求。现在云计算系统主要采用 Map-Reduce 模型。

（5）经济性。组建一个采用大量的商业机组成的机群相对于同样性能的超级计算机花费的资金要少很多。

计算机资源服务化是云计算重要的表现形式，它为用户屏蔽了数据中心管理、大规模数据处理、应用程序部署等问题。通过云计算，用户可以根据其业务负载快速申请或释放资源，并以按需支付的方式对所使用的资源付费，在提高服务质量的同时降低运维成本。

2）云计算安全挑战

云计算的服务计算模式、动态虚拟化管理方式以及多租户共享运营模式等对信息安全和国家监管带来了新的挑战，主要有[①]：

（1）云计算服务计算模式所引发的安全问题。当用户或企业将所属的数据外包给云计算服务商，或者委托其运行所属的应用时，云计算服务商就获得了该数据或应用的优先访问权。事实证明，由于存在内部人员失职、黑客攻击及系统故障导致安全机制失效等多种风险，云服务商没有充足的证据让用户确信其数据被正确地使用。

（2）云计算的动态虚拟化管理方式引发的安全问题。在典型的云计算服务平台中，资源以虚拟、租用的模式提供给用户，这些虚拟资源根据实际运行所需与物理资源相绑定。由于在云计算中是多租户共享资源，多个虚拟资源很可能会被绑定到相同的物理资源上。如果云平台中的虚拟化软件中存在

① 冯登国，张敏，张妍，等. 云计算安全研究. 软件学报, 2011, 22(1):71−83.