海军新军事变革丛书

总策划：魏　刚　　主　编：马伟明

网络空间战：
互联世界的信息作战

[美] Mike Chapple
David Seidl 著

邢焕革　毛德军　张　立　等译
王航宇　主审

CYBERWARFARE:
INFORMATION OPERATIONS
IN A CONNECTED WORLD

中国工信出版集团　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

网络空间战：
互联世界的信息作战

CYBERWARFARE：INFORMATION OPERATIONS
IN A CONNECTED WORLD

[美] Mike Chapple
David Seidl 著

邢焕革　毛德军　张　立　等译
王航宇　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：01-2016-0782

图书在版编目（CIP）数据

网络空间战：互联世界的信息作战 /（美）迈克·查佩尔（Mike Chapple），（美）大卫·赛德尔（David Seidl）著；邢焕革等译. —北京：电子工业出版社，2017.9
（海军新军事变革丛书）
书名原文：Cyberwarfare: Information Operations in a Connected World
ISBN 978-7-121-32250-1

Ⅰ. ①网… Ⅱ. ①迈… ②大… ③邢… Ⅲ. ①信息战－研究 Ⅳ. ①E866

中国版本图书馆 CIP 数据核字（2017）第 169096 号

责任编辑：张 毅
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：27.75 字数：442 千字
版 次：2017 年 9 月第 1 版
印 次：2017 年 9 月第 1 次印刷
定 价：105.00 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）88254888，88258888。
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。
本书咨询联系方式：（010）57565890，meidipub@phei.com.cn。

海军新军事变革丛书

网络空间战：互联世界的信息作战

主审 王航宇

主译 邢焕革　毛德军　张　立

审稿 陈泽茂　周　浩　詹昊可

翻译 吴志飞　陈长宇　阮旻智

刘　刚　岳　博

《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。

胡锦涛同志指出："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，丛书编委会编译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

随着网络信息技术的快速发展，互联网正以超乎想象的速度向全球各个角落渗透，已经成为承载世界各国政治、经济、军事、文化的全新空间。可以这样说，网络空间已经发展为信息化时代世界大国角逐政治、经济、军事、文化优势的新型空间。从政治视角来看，网络空间已成为信息的“集散地”、舆论的“发酵池”，一旦被敌对势力控制利用，就会成为恶性事件的“催化剂”，严重威胁国家政权巩固和社会安全稳定；从经济视角来看，网络空间已经成为新型企业的孵化器，国家重要基础设施的安全和有效运行依赖于网络空间，对国家经济发展产生重要影响；从军事视角来看，网络空间是对陆、海、空、天自然空间的拓展，网络空间战既可以在陆、海、空、天等实体空间中实施，也可以在虚拟的网络空间进行，其控制力和影响力对夺取陆、海、空、天的控制权具有重要影响，谁掌握了网络空间的控制权、主导权，谁就拥有了网络空间的行动自由，谁也就能掌握陆、海、空、天等自然空间的主动权，也就扼住了对手的命脉。

为了深入研究网络空间战对世界的影响，本书的作者 Mike Chapple 和 David Seidl 将基本信息安全原则与实际应用相结合，从网络空间战的发展历史、攻防对抗到未来发展三个方面向读者提供了有关网络空间战方面的全方位信息，书中内容涵盖广泛，特点鲜明，反映了网络空间战领域最新思想与发展趋势。其主要内容有：

一、网络空间战基本概念

网络空间战是指将信息系统作为武器来对敌方实施作战的一系列行

为。当前美军网络空间战理论对网络空间战的定义包含三个方面的内容，即计算机网络攻击（CNA）、计算机网络防御（CND）和情报搜集。

在网络空间中，由于没有传统武装冲突中存在的所谓边界问题，也没有受到国际条约、道德或者法律的制约，其攻击目标对象很少受到限制，主要有军事目标、非军事目标、工业和民用基础设施，甚至非参战个人都是攻击的潜在目标。

在网络空间战中，其参与者主要有：主管网络系统安全和网络空间战能力的军事机构、情报部门、商业机构、叛乱分子和恐怖组织、执法部门、激进活动团体，甚至是个人，他们都是参与网络空间战的主要力量。

二、网络空间战的主要攻击样式

网络空间战的攻击行为从最初的黑客行为已经发展到高级持续威胁，其攻击方式主要有如下典型样式：

（一）现代黑客

现代黑客拥有先进技术，其攻击类型可以分为如下三种：机会攻击、半定向攻击和精准攻击。

1．机会攻击

攻击者运用暴力方式对数以千计甚至数以百万计的目标进行攻击，试图找到系统中的一些漏洞。其常用的攻击方法主要有：恶意病毒软件、网络钓鱼攻击、密码猜测等。

2．半定向攻击

半定向攻击比机会攻击要进一步，它是寻求渗透到特定的组织或特定目标。半定向攻击不是将目标对准特定的个人或者系统，而是在特定的组织内寻求可入侵的计算机。

3．精准攻击

精准攻击，又称为定向攻击，是寻求对特定的系统或个人用户进行攻击，通常是为了入侵特定账户来进行有针对性的设计。

（二）高级持续威胁

高级持续威胁是运用先进的攻击手段、针对特定的目标，持续地保留对锁定目标进行长期关注，直到攻击得手而成名。

采取高级持续威胁的攻击者通常可能是军方机构、政府主导的实体组织，或者是非政府行为体控制下的组织机构，如企业维权组织，或者是有组织的犯罪团体。其特点是拥有技术工具先进；运用社会工程学渗入组织内部，操纵他人行为；目标清晰明确；丰富的财力和人力资源；严明的组织和纪律等。

高级持续威胁使用的技术手段主要有：零日攻击、先进恶意软件、社会工程学和网络钓鱼、网络入侵策略。

（三）网络杀伤链

网络空间战专家使用网络空间杀伤链的概念来描述网络空间战不同阶段的攻击行动。根据这个概念，网络杀伤链是从侦察跟踪阶段开始，攻击者搜集有关目标尽可能多的信息，然后进入武器构建阶段；攻击者根据所选目标来开发特定的武器；在载荷投送阶段将武器投送至目标后，进入突防利用和安装植入阶段，就可以对目标系统进行访问，在设备上留下永久的足迹；攻击者在命令控制阶段保持对目标系统的访问；最终在目标达成阶段完成其战略目标。

（四）社会工程学攻击手段

社会工程师利用人性的弱点，运用互惠、承诺和一致性、社会认同、权威、喜好和稀缺性等方式达到操纵行为人目的。针对网络空间攻击，其手段主要包括以下方面：

- 欺骗个人泄露信息系统、网络或者其他操作细节，为网络空间战攻击的侦察阶段提供必要的关键信息，以便助其发起网络空间战进攻行动。
- 对个人施加影响，使其绕过物理安全防护控制，允许攻击者访问物理设施设备，而此物理设施设备可能正是攻击者发起网络空间

战进攻行动的地方。

- 说服个人采取有关行为使电子安全防护控制系统失效，如绕过防火墙或者允许虚拟专用网络同未经授权的网络相连。
- 骗取内部人员在组织机构所保护网络的计算机中安装软件，暗中创建后门，从而使攻击者获取网络访问的通道。

三、网络空间多层次防护策略

多层次防御策略思想是指：当网络攻击者对保护的系统、数据或网络发起攻击时，网络防御者应该有多个层次的防护手段。网络空间战中的多层次防御思想与传统军事领域里的纵深防御非常类似。它采用不同的方法来构建不同层次的防御结构，如果进攻者突破了系统的某层防护，它也将会被后续的防护层阻挡。多层次网络防御技术包括防火墙、入侵检测与防护系统、反病毒软件、认证授权、注册登录管理、反击以及系统恢复能力等。

（一）实现多层次防御策略的方法措施

要确保网络空间数据符合可用性、保密性、完整性、真实性，以及不可否认性等要求，多层次防御策略不仅要涵盖人员及技术，还包括保障、监视与维护等日常机制，做到人员、技术与机制的三者有机结合。

（1）人员

对人员提出以下要求：

- 在既有制度与程序的要求下，人员知道应该做什么。
- 通过训练，他们知道应该怎样去做。
- 所处的环境应符合网络系统管理和物理安全保障的要求。

为了做到这一点，对所用人员的背景应进行调查与考核，并确保人员所使用的设施设备是在安全、监督与隔离方面能够达到合理的安全水准。

（2）技术

技术关注的领域强调的是应从以下方面来加强防护：

- 网络和基础设施的防护。
- 外围边界的防护。
- 计算机工作环境的防护。
- 诸如密钥管理、公钥基础构架、检测与响应等保障设备的防护。

多层次防御策略是将各层次的防护工作结合起来，确保某一层防御失效时，受到保护的数据、服务或者网络系统不至于暴露在攻击者面前。要强调的是，对每层防御设置各不相同的技术障碍，从而使得单一的攻击无法同时攻破所有的防御层次。

（3）机制

机制是基于多层次防御策略信息安全保障的三部分组成之一，其关注的焦点问题有：

- 安全政策。
- 认证和授权。
- 安全管理。
- 密钥管理。
- 状态评估。
- 攻击感知。
- 警告。
- 响应。
- 恢复和重构。

（二）清单制对策措施

为了适应网络系统的多样化环境使用需要，针对不同的威胁采取相应的防御对策手段，运用清单就具有非常现实的实战意义了。

- 采用应用程序白名单制。
- 限定管理员权限。

- 限制工作站之间的流量发送。
- 使用信誉服务较好的杀毒软件。
- 实现逆向开发功能。
- 实施主机入侵防御系统规则。
- 设置一套安全基准配置。
- 利用网络域名系统的信誉。
- 利用软件升级或补丁的优势来确保已知的缺陷和问题及时得到解决。
- 将不同类型的网络和功能进行合理隔离，可以确保网络或系统的某一部分被攻陷以后，其他部分不会同时被攻陷。

四、终端防护

（一）终端设备及攻击方法

终端设备种类繁多，从网络安全的角度来看，主要包括计算机、移动设备、工业控制系统、军事系统以及嵌入系统等。

从网络攻击的角度来看，对终端设备进行攻击的方法主要有如下：

- 需要进行物理接触的攻击。例如，需要在系统中插入一个硬件键盘登录工具，或通过活动的内存捕获密钥后对磁盘进行一个物理备份，在进行这些活动的时候没有无线访问通道。
- 需要通过网络访问的攻击。例如，拒绝服务攻击，或者针对系统提供的网络服务发起的攻击，如网页服务器或文件服务器。
- 需要用户或管理员参与采取某种行动的攻击。例如，网络钓鱼攻击，或通过其他形式的社会公关，使得某个用户失去对机器的控制权，从而不自觉地帮助了攻击者。
- 针对设备的硬件或固件的攻击。这种攻击通常需要在设备进行设计或制造时，就有某种形式接触的渠道，从而在设计阶段对设备设置陷阱，或在系统出售之前在其固件中植入某种缺陷或木马。

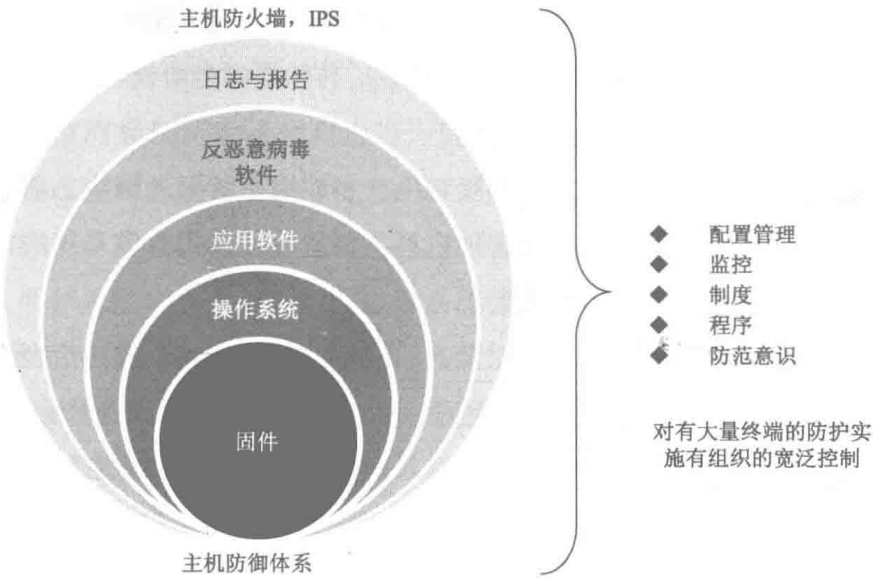
- 针对应用软件的攻击。例如，网页浏览器；大多数针对应用软件的攻击需要攻击者能够发现应用软件的缺陷，不管是通过测试的方法，还是通过分析源代码来找出其缺陷所在。
- 使用终端的正常功能来发起的攻击。例如，向入侵检测系统提供虚假反馈，以阻塞正常的通信流量；又如针对无人机系统进行的GPS攻击，可以尝试将无人机降落在错误的地点。

（二）终端设备防护方法

典型终端防护的多层次防御策略包含一系列防护层，主要有：

- 物理安全。
- 制度与程序。
- 配置标准。
- 中央管理。
- 防范意识和信息共享。
- 反恶意病毒软件和杀毒软件。
- 配置管理、更新和升级。
- 白名单和黑名单。
- 测试，包括渗透测试与使用红方小组。

下图描述了计算机工作站典型的多层次防御体系模型。防御从固件和硬件层开始，该层提供了供其他软件和防御运行的底层环境；计算机的操作系统及运行在操作系统之上的应用软件，提供了第二层防御，这就要求操作系统必须采取合适的防护手段，而应用软件必须能够防止攻击者运用这些软件来入侵系统；反恶意病毒软件主要用于检测系统是否被感染，这就要求提供系统日志以及其他能够提供系统状态信息的报告；最后，运用系统级防火墙，或者是使用其他网络防护，在网络与其他的系统或网络连接时，可以对攻击进行过滤或监控。



五、网络防护

（一）网络类型及攻击方法

从目前机构采用的网络类型来看，主要的类型有：局域网、广域网、互联网、专用网络。从网络攻击的形式来看，大量的网络攻击都是围绕获取进入网络系统和设备的访问权限来展开的，而拒绝服务攻击、对关键网络基础设施发起动态攻击都是在网络空间战中可能出现的攻击样式。为此，多层次防御策略提出了使用防护、检测、响应模式来作为防御的样式。

（二）网络防护技术

用于防护网络的技术，已经从基本的网络防火墙和登录系统，发展到了能够探测攻击，并且对出现攻击行动采取有效对抗措施的高级系统。主要有：

1．协议

网络依靠协议来控制如何收发信息、如何编码，协议还包含了一系列确保网络能够正常运行的其他要素。协议在网络安全方面发挥了巨大作用：通过运用数据加密，可以确保收到的数据是完整的和未经修改的，并能确保

攻击者即使能够截获网络流量也无法查看到信息，即使他们拥有数据加密能力也是如此。主要的协议有边界网关协议、传输层安全协议。

2．网络访问控制

网络访问控制是运用技术手段对用户和应用系统接入网络之前对其身份进行审核。同时还可以利用这种信息，将系统接入到与该系统的权限或者安全等级相匹配的网络区段上。

根据网络访问控制系统的配置，如果用户的身份验证成功，则用户可以进入到与其身份相匹配的网络区段中去。反之，如果用户身份验证失败，网络可以拒绝此次连接，或将用户引入到一个虚拟的违规网络区。

3．网络防火墙

防火墙是网络防御技术中应用最为广泛的一种技术手段之一，普遍用于提供网络分隔和防护。当前应用最为广泛的防火墙主要有：数据包过滤器防火墙、状态数据包检查防火墙、应用感知防火墙。这些防火墙在大多数网络安全设计中都得到了广泛应用，以确保只有那些被准许的通信才能通过各网络控制点。

4．网络边界防护

对网络内部的防护，通常依赖于网络边界防护，而网络边界则是由网络和防护管理员根据不同的安全等级或者访问需求，在各网络或系统间建立。网络中的边界通常在网络各个控制点处构建，例如：

- 防火墙或路由器，用于分隔各网络。
- 终端交换机，可以限制与墙壁上插孔和个人系统进行连接，并给连接到指定的网络端口设备打上标记。
- 无线访问点，可用于鉴别各个连接点，并允许用户/设备连接到多个不同的网络。
- 远程访问系统，可用于鉴别用户，并将用户导入到不同的网络组或者不同的地址范围内。

管理员和防护人员都可以利用这些控制点来将各系统进行分隔，分隔的依据可以是根据他们的用户权限、系统配置或系统状态，也可以是根据各系