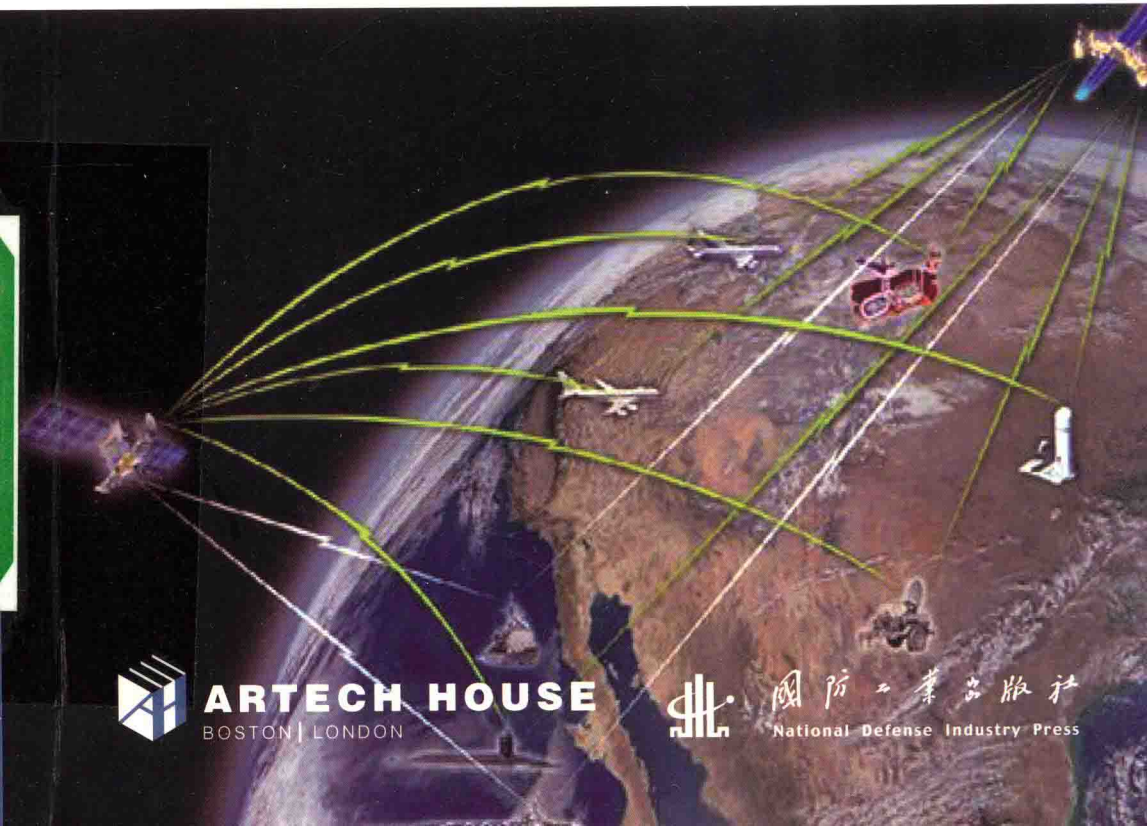
国防科技著作精品译丛

Information Warfare and Electronic Warfare Systems

电子战与信息战系统

【美】Richard A. Poisel 著
兰 竹 常晋聃 史小伟 徐 旺 高由兵 译
刘永红 审校



ARTECH HOUSE
BOSTON | LONDON
国防工业出版社
National Defense Industry Press

电子战与信息战系统

Information Warfare and Electronic Warfare Systems

[美] Richard A. Poisel 著
兰 竹 常晋聃 史小伟 徐 旺 高由兵 译
刘永红 审校

国防工业出版社
National Defense Industry Press

著作权合同登记　图字：军 -2014 -094 号

图书在版编目（CIP）数据

电子战与信息战系统/（美）理查德·A·波塞尔（Richard A. Poisel）著；兰竹等译.
-- 北京：国防工业出版社，2017. 12
（国防科技著作精品译丛）
书名原文：Information Warfare and Electronic Warfare Systems
ISBN 978-7-118-11513-0

Ⅰ. ①电… Ⅱ. ①理… ②兰… Ⅲ. ①电子对抗—研究②信息战—研究
Ⅳ. ①TN97②E869

中国版本图书馆CIP数据核字（2017）第 315950 号

电子战与信息战系统

[美] Richard A. Poisel　著

兰　竹　常晋聃　史小伟　徐　旺　高由兵　译

刘永红　审校

出版发行　国防工业出版社
地址邮编　北京市海淀区紫竹院南路 23 号　100048
经　　售　新华书店
印　　刷　天津嘉恒印务有限公司
开　　本　710 × 1000　1/16
印　　张　23
字　　数　377 千字
版 印 次　2017 年 12 月第 1 版第 1 次印刷
印　　数　1—2000 册
定　　价　98.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010) 88540777　发行邮购：(010) 88540776
发行传真：(010) 88540755　发行业务：(010) 88540717

译者序

随着电子技术的飞速发展，电子战与信息战系统的发展方兴未艾。特别是现代战争中，电子战与信息战发挥着越来越重要的作用。探索电子战与信息战技术新概念、新技术的文章很多，但系统深入的研究较少。《电子战与信息战系统》一书力图系统深入地探讨电子战，特别是通信电子战与信息战系统。

本书作者 Richard A. Poisel 博士是电子战领域的权威专家。本书主要围绕通信电子战，介绍了电子战与信息战系统的相关概念，探讨了信息的本质及信息论基本原理。本书还介绍了网络及网络中心战的概念，重点研究了信息战的架构模型及典型的配置，并给出了两种场景下的作战模拟，是一本电子战从业人员及相关人士的重要资料。

本书由兰竹和常晋聃领衔翻译，并对全书进行了校对。徐旺、史小伟、高由兵等参与了本书的翻译工作。刘永红研究员对全书内容进行了审校。在本书的翻译和出版过程中，得到中国电子科技集团公司第二十九研究所和电子信息控制重点实验室高贤伟、姜道安、何涛、顾杰、华云、刘江、何俊岑、肖开奇和龙晓波等领导和专家的大力支持，特别是胡来招博士提出了许多宝贵的建议。国防工业出版社的编辑对本书的出版工作也提供了大力支持，在此一并表示衷心的感谢。

在本书翻译过程中，我们领略到了电子战及信息战理论的博大精深，深感自己的专业水平有限。因译者水平所限，书中难免会出现未尽或纰漏之处，敬请广大同行批评指正。

译　者

2017 年 10 月

前言

信息战/信息作战（IW/IO）是一种将信息技术（IT）带到战场的对抗。有人甚至认为，它是作战的下一个演化步骤，突破了工业时代的一切都围绕着力量的集结，而是基于效果的集结。在考虑信息战的过程中最关注的是信息优势。谁主宰了信息，谁就会在现代战场上取得胜利。

电子战（EW）是信息作战的五个分支之一。其余几个分支分别是计算机网络作战（CNO），心理作战（PSYOPS）、军事欺骗（MILDEC）和作战保密（OPSEC）。计算机网络作战是以对计算机网络攻击（被动和主动）为手段；心理作战涉及改变人们的态度和意见，无论是军队还是民众；军事欺骗也针对人的头脑，但主要针对敌方的指挥官。它试图制造一个让人可信的但非真实的态势；作战保密采用的方法是让对手不知道己方的实际态势。本书的重点是电子战，以及电子战系统和原理是怎样用在信息战/信息作战中的。

电子战涉及所有在某种意义上能够辐射电磁波（EM）的电子系统。因此，这是一个相当广泛的范畴，本书论述主要集中在通信电子战方面，将研究电子战系统如何阻碍敌方的信息交换。

电子战的分类包括电子支援（ES）、电子攻击（EA）和电子防护（EP）三个不同但相关的领域。

电子支援是对通信信号的非合作拦截。它提供作战信息，也就是指挥官可以立即用于做出决策的信息，以及产生情报信息。这里的区别是把收集到的信息用于做什么，以及产生所需结果的信息总量。

电子攻击是指通过在敌方网络中插入电磁辐射信号阻止网络上信息

正常交换的主动攻击。电子支援在某些情况下为电子攻击提供目标引导。

电子防护是保护友军的通信系统不受敌军电子支援和电子攻击的影响。在这里不把电子防护作为讨论的重点，除非友军的电子支援和电子攻击已经提供了一定程度的电子防护。

本书适合初入电子战领域的工程技术人员，以及试图用不同的角度评估电子战系统性能的专业人士阅读。阅读本书通常需要工学本科学历，具有线性系统理论的知识背景（包括应用矩阵理论的线性代数）。特别是在第2章中的一些材料，把信息的特性理解为一种规律是有用的，它是非技术性的。概率论的应用知识也很有用，不过所需的基本知识本书在需要时会给予介绍。

本书结构如下：

第 1 章介绍电子战和信息战系统，其目的是为理解信息战的军事意义奠定基础。

第 2 章通过研究信息的一些基本特征来探索其本质，把 Boyd 提出的“观察、调整、决策及行动”（OODA）环路作为基本的决策模型进行介绍，还讨论了冲突的三个领域，包括它们的基本原型。

第 3 章研究信息论的原则，介绍必要的概率论的基础，给出作为消息中信息含量的基本度量即信息熵，讨论信息论中广泛采用的通用信道模型以及一些常见的现代通信系统的容量，特别还介绍广播信道，它是第 9 章对电子战系统性能评价的基础。

第 4 章讨论信息战不断发展的模型，Kopp 和 Borden 根据香农的信息论提出这个模型，用来研究信息战属性的分类法。用这个模型提出信息战的四个规范形式。我们建议把电子支援也加入这些规范的形式，以便完整地分析电子战系统，因为对于收集信息，它通常是必要的，这样才能使用以上四个形式。

第 5 章探讨电子战系统是如何与网络中心作战（NCO）相互关联的。介绍电子战系统对现代战场的贡献，并特别关注它们为态势感知带来什么，还讨论电子战系统作战的基本流程图，包括电子支援、电子攻击、电子战目标分析和电子战情报分析。在讨论电子战系统提供的信息时，同时讨论电子战系统履行其任务所需要的信息。最后，综述数据和信息的融合。

构成有效的网络中心战的主要能力之一是多个战场设施间通信的能力。在第 6 章讨论组网的基础，并介绍移动自组织网络（MANET），然后给出几个现代MANET协议的例子并研究它们的一些基本特征。安全性已

经成为对 MANET 协议的主要挑战之一，所以对此重要话题有较多的讨论。最后，综述电子战对 MANET 的攻击。

电子战系统对网络中心战的主要作用之一是提供信息以进行态势评估，从而给出态势感知。在第 7 章讨论这些原则，并展现不同层次的数据融合如何嵌入态势评估的流程中。

第 8 章介绍电子战系统的体制，概述电子支援和电子攻击系统的组成，以及电子战系统是如何设计的。为其他章节的讨论提供所需的信息。

第 9 章介绍几种电子战系统体制的理论性能，分析的基础是香农信息论和现代多输入多输出（MIMO）天线系统的概念。接着介绍评估电子支援系统的基础 —— 对窃听信道的分析，以及评估电子攻击系统性能的基础 —— 任意变化信道（AVC）。本章还对窃听信道和 AVC 的组合进行评估和性能比较，并对协作与非协作的电子支援和电子攻击活动提出几点思考。

第 10 章给出部分电子战系统架构的计算机仿真结果。首先对多种架构进行工程（技术）仿真并给出结论，随后通过作战仿真以评估一些有代表性的电子战系统体制。既考虑复杂的电子战系统体制，也考虑简单的系统体制。考虑两种不同的场景：一种是在东北亚地区的情况；另一种是在城市地区，如在一个大城市的情况。对每个场景都分析复杂系统和简单系统的性能，讨论不同电子战系统架构的优点，并给出建议。

本书中的内容主要是从陆地机动部队（陆军和海军陆战队）的观点来看的。这是作者的偏好，也是作者的背景。但该内容是适用于其他场景的，主要原则适用于所有使用电子战系统的情况。

本书或多或少会有些许错误，虽然我们花费了相当大的努力尽量减少这种错误，但总归不会是完美无瑕的。如有纰漏，在任何情况下都愿意承担全部责任。我们欢迎建设性的反馈意见，不论是发现错误还是提供积极建议。

目录

第 1 章

电子战和信息战系统导论

1.1 引言

设计通信系统时，通常会考虑信道物理损伤（如接收机的热噪声或无线媒介的衰落和干扰）时它仍能确保信息的可靠传输。然而，许多非军事和几乎所有的战术军事通信场景都要求对信息加以保护，以抗衡电子战的行动。

然而，电子战行动，尤其是在战术层面上，可以用来降低敌方通信的有效性。

安全通信问题中，敌对方的行为基本上可归为两类：一类是对传输信息的被动拦截和窃听，它不产生任何拒止效应；另一类是主动地影响消息和传输介质。前者称为窃听，后者称为干扰。

考虑这样的一类消息保护问题，它同时需要考虑防窃听的机密性和防干扰的完整性，而不注重身份的区分。为了对电子战进行分析，要确定这些功能对特定的电子战措施到底有多脆弱。如图 1.1 所示，我们研究了在这样的要求下安全通信的基本极限，也就是窃听者可能窃听信道，而干扰者也可能干扰信道。在该假设中，双方独立行动，相互不协作。

为了应对敌对方数量无法控制的问题，将根据计算的复杂程度来运用信息论方法。用任意变化的窃听信道（AVWTC）对这样的场景建模。AVWTC 结合了来自窃听信道的模型和任意变化信道模型的元素，这两种信道模型将在第 9 章中进行讨论。该模型包含一系列的窃听信道，它们具有多个由干扰机以任意和时变方式（仅对通信链而言）选择的状态，而这些状态对于发射机和目标接收机是未知的。我们研究的目标是确定该信道

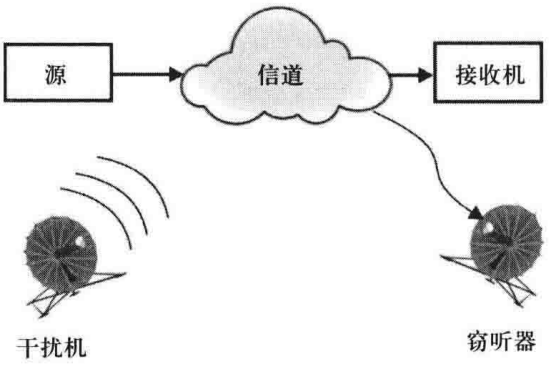


图 1.1 存在非协同的干扰和窃听时信息保护场景的总体框架

安全的容量，也就是合法用户在有干扰的情况下能够保证可靠通信并且能避免被窃听的最大私密速率。通过这样的研究，就可以搞清楚电子战方法的有效性。

在本书中，将着重考虑地面部队的电子战。然而这并不限制其基本规则适用于其他部队的电子战以及对非军事网络和信息交换/处理设施的电子战。

1.2 全球信息栅格

自 20 世纪 90 年代中期，美国军方就把其未来的部队定义在利用网络中心战（NCW）（在英国和其他地方也称为网络使能战）的原则打造更轻、更精、更有杀伤力的部队上，也称为网络中心作战（NCO）。通过利用信息技术（IT），将传感器、射手和决策者（DM）连接到一个共同的框架中，使军事力量可以快速同时发现敌方行动和部署[1]。该信息优势使得美军对任何敌对力量都拥有全谱优势。

但是，使今天的军事力量更轻便、更有杀伤力的信息优势，也增加了敌方基于商用网络的（相对于分级架构的）信息技术实施攻击的可能。

陆军旅战斗队（BCT）利用[3]："先进的网络架构实现前所未有的各层互通、态势感知和协同作战。"

国防部负责最大的网络中心战相关的项目，其核心是让网络自己组网——称为全球信息栅格（GIG）。全球信息栅格用来为网络中心战提供"入场券"，密集互连、超高带宽、高度可靠的信息基础设施，也就是联系多个网络中心战系统的"信息架构"[4]。然而，全球信息栅格主要集中于为军事