国防电子信息技术丛书

EW 104: EW Against a New Generation of Threats

EW104

应对新一代威胁的电子战

[美] David L. Adamy 著

朱 松 王 燕 常晋聃 王晓东 译

姜道安 何 涛 审校

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

国防电子信息技术丛书

EW104

应对新一代威胁的电子战

EW104: EW Against a New Generation of Threats

[美] David L. Adamy 著

朱 松 王 燕 常晋聃 王晓东 译

姜道安 何 涛 审校

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

内 容 简 介

本书重点介绍了当前电子战面临的新威胁以及采用的新型对抗技术。全书共 11 章，第 1 章简单介绍了本书的写作目的和背景；第 2 章探讨了电磁频谱作战域的特点以及与其他作战域的关系，阐述了与电磁频谱作战域相关的基本概念和用语；第 3 章介绍了传统的威胁雷达及雷达干扰技术；第 4 章概述了新型威胁雷达的技术改进，以及威胁的变化给电子战带来的影响；第 5 章全面论述了数字通信理论；第 6 章主要讲述了无线电传播的基本原理及其在通信电子战中的应用；第 7 章讲述了通信威胁的巨大进步以及给电子战带来的新挑战；第 8 章讲述了数字射频存储器的工作原理及其在电子战中的应用；第 9 章讲述了与红外武器和传感器以及红外对抗相关的原理、技术、发展现状；第 10 章讲述了雷达诱饵的作战任务、工作原理及部署方式等；第 11 章讨论了电子支援系统与信号情报系统之间的差异。

全书综述了威胁及其对抗措施的最新发展，内容全面、新颖，是近年来电子战领域不可多得的一本教科书式技术专著，适合电子战、雷达、通信等领域的工程技术、作战及管理人员阅读，并可作为高等院校或培训的教材或参考资料。

图书在版编目(CIP)数据

EW104：应对新一代威胁的电子战 /（美）戴维·阿达米(David L. Adamy)著；朱松等译.
北京：电子工业出版社，2017.9
（国防电子信息技术丛书）
书名原文：EW 104: EW Against a New Generation of Threats
ISBN 978-7-121-32560-1

I. ①E… II. ①戴… ②朱… III. ①电子对抗 IV. ①E866

中国版本图书馆 CIP 数据核字(2017)第 206224 号

策划编辑：竺南直
责任编辑：竺南直
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
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：787×1092　1/16　　印张：17.5　字数：470 千字
版　　次：2017 年 9 月第 1 版
印　　次：2017 年 9 月第 1 次印刷
定　　价：49.80 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：davidzhu@phei.com.cn。

谨以此书献给身着戎装的青年们！

你们将深入险境，应用电子战之科技，展现电子战之艺术。

直面新威胁，尽你们所能，于危险中保护世人之安全。

作者简介

戴维·阿达米（David L. Adamy）是一位国际公认的电子战专家，在电子战领域从业50多年，先后在军方和工业部门工作，曾担任“老乌鸦”协会主席和董事会成员，在业界享有很高的声望。作为系统工程师、技术负责人或项目经理，阿达米直接参与或管理过大量陆海空天平台的电子战项目，具有丰富的实践工程经验。

阿达米先生先后毕业于亚利桑那州立大学和圣克拉拉大学，拥有电子工程学士和硕士学位，理论基础扎实，学术造诣深厚，在电子战及相关领域发表了大量技术文章，在“老乌鸦”协会会刊《电子防御杂志》上撰写EW101技术专栏已超过20年，出版专著14本。所著的EW100系列（《EW101：电子战基础》、《EW102：电子战进阶》和《EW103：通信电子战》）名列“老乌鸦”协会公布的“十大最受欢迎的专业读物”之首，赢得业界广泛好评。

目前，阿达米先生在多个军方机构和电子战公司担任顾问，负责提供战略和业务咨询，并在全球范围内举办电子战讲座，传授电子战知识。

译 者 序

随着电磁频谱在现代战争中的作用和地位日益重要和突出，电磁频谱正逐步演进成为独立的作战域，电子战也加速向电磁频谱战转型发展。在电子信息技术日新月异的时代背景中，电子战作为一门对抗性的学科，其发展充满了新的机遇，更面临着巨大的挑战。以往对传统威胁行之有效的电子战技术在面对新的威胁时有可能不再有效，亟需开发新的对抗技术和作战模式。如何尽快找到新的对抗措施，开发出有效甚至是颠覆性的新技术，已成为全球电子战界密切关注的焦点，也是电子战技术人员面临的最重要的课题。

相对于雷达、通信等领域的技术发展，电子战技术的发展更加隐秘，在公开的文献和讨论中，几乎看不到其工程应用研究报道，即使是理论性探讨也不多见，权威的经典电子战专著就更少。本书集中探讨了电子战面临的新威胁和对抗技术的新发展，弥足珍贵。

本书是EW100系列畅销书中的第4本(前3本分别是《EW101：电子战基础》、《EW102：电子战进阶》和《EW103：通信电子战》)。书中用大量篇幅对传统威胁进行了综述，探讨了本世纪以来雷达、通信和红外领域所出现的新威胁，以及对抗技术的新发展，是一本内容丰富的教科书式读物。本书内容全面、新颖，包括了频谱战、传统雷达威胁、新型雷达威胁、传统通信威胁、现代通信威胁、数字射频存储器、红外威胁及相应的对抗技术、雷达诱饵及电子支援与信号情报等，是近年来电子战领域不可多得的一本技术专著。通过本书，读者可以从技术的角度了解传统威胁的发展，同时能深刻地理解新一代威胁所带来的挑战。

本书的翻译出版，得到了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领导的大力支持，在此表示衷心感谢。在翻译过程中，也得到国内广大同行的关心和帮助，对此致以感谢。

本书覆盖面广，技术内容新，由于译者技术水平和翻译水平所限，对原著的一些意思把握不准，译著中难免存在错误，敬请读者指正。

译 者

2017年6月

前　言

这是 EW100 系列的第 4 本书。前两本书——《EW101：电子战基础》和《EW102：电子战进阶》讲述了电子战的基础知识。第 3 本书即《EW103：通信电子战》重点讲述通信电子战，主要是针对中东形势而写的。当时，地面电子战重新获得关注，《EW103：通信电子战》就是为了帮助地面部队应对敌方陆上通信，包括那些用于引爆简易爆炸装置的链路，而简易爆炸装置是造成美军伤亡的主要原因。

现在，整个电子战领域都在不断改变，出现了难以对付的新型威胁雷达和通信链路。在电子战界，最令人担忧的可能是，那些曾经有效的电子战功在很多方面将不再能发挥作用，需要采用新的方法。本书旨在帮助军内外的人士应对这种可能让他们付出生命代价的新现实。

与《EW101：电子战基础》、《EW102：电子战进阶》和《EW103：通信电子战》一样，本书是非涉密的，但涉及的某些话题要从保密渠道获取信息。为了不涉密，我们采取的处理方法就是，对天线增益、有效辐射功率（EPR）等进行合理估算。其数值可能不对，但这并不会影响分析结果。如果在公开文献中没有提供相关数值，我们就进行合理估值，并给出这样估计的逻辑。然后在公式中插入这些估值并举例说明来讨论问题。来源不同，给出的数值也会不同，所以其中一些必定是错的。我们不判断数值的对错，只选取一个值并用于解决实际问题，目的是提供使用信息的方式，如果以后在工作中要使用该信息，即可在获得授权的保密资料中查阅真实的数值，并将其插入我们所讨论的公式中。

戴维·阿达米

目　录

第1章 引 言

过去几年中，电子战的特点已经发生改变并正在加速变化中。本书旨在从技术角度阐述这些变化，书中采用的有关威胁信息均来自公开文献。本书并不准备全面介绍威胁的情况，而是使用合理的估计，讨论会对对抗措施产生什么影响。

电子战发生的重大变化包括：

- 电磁环境被认为是一个独特的战斗空间；
- 研制了新型和特别危险的电子制导武器；
- 涌现出影响武器精度和杀伤力的新技术。

本书将涉及以上所有这些领域，深度可能受所使用的开源情报的限制。不过，在新技术领域，开源信息是非常丰富的，足以支持对这些技术在新武器中的作用，以及对抗这些武器的电子战措施的效能展开讨论。

在电子战的语境中，我们把与威胁有关的无线电辐射称为“威胁”。其实这并不正确，威胁实际上是指以爆炸或其他某些方式造成破坏的东西。但是，我们会以这种方式来谈论信号。在本书中，我们将讨论雷达威胁和通信威胁。雷达威胁就是指与雷达控制武器相关的雷达信号，包括：

- 搜索与截获雷达；
- 跟踪雷达；
- 雷达处理器与导弹之间用于制导和数据传输的无线电链路。

通信威胁包括：

- 指挥控制通信；
- 综合防空系统各组成部分之间的数据链；
- 连接无人机与控制站的指挥和数据链；
- 引爆简易爆炸装置的链路；
- 用于军事目的的蜂窝电话链路。

本书的重点是介绍这些信号的用途以及它们对武器和军事行动效果的影响，同时也将讨论在热寻的导弹以及挫败这些导弹的对抗措施方面的巨大进步。

简而言之，我们不能继续用以前的方式来实施电子战了，尽管在过去几十年中，这种方式取得了极大成功。世界已经改变，我们必须随之变化。

本书试图提供一些工具，以帮助实现这些转变。

本书其他部分的重点主要有三个：

（1）在第 2 章中将讨论新近确定的电磁战领域。除了熟悉的陆海空天之外，这是新出现的一个战斗空间。正如将要发现的，它与其他所有战斗空间很相似，电子战在其中发挥

着重要的作用。有一个相关的主题虽然并不是处处合适，但依然非常重要，那就是第 11 章将讲述的电子战支援（ES）与信号情报（SIGINT）在定义上的差别。

（2）涌现了很多对电子控制武器和电子战具有重大影响的新技术和新措施。所有这些领域都将在相应的章节中进行论述，其中第 5 章介绍数字通信原理，第 8 章讲述数字射频存储器（DRFM），第 10 章介绍雷达诱饵。

（3）对现代威胁进行了讨论。雷达威胁包括两章内容：第 3 章介绍传统威胁雷达，同时也包括了雷达威胁的截获方程和干扰方程；第 4 章讲述新型威胁雷达的特点。通信威胁也包括两章内容：第 6 章介绍传统通信威胁，包括用于截获和干扰的传播公式，同时也包括辐射源定位；第 9 章介绍红外威胁及其对抗。

第2章 频 谱 战

战争的特点就是不断变化。作战领域过去是陆地、海洋和天空，后来太空也加了进来，现在，又出现了第五个作战域：电磁频谱。本章将讨论这个新作战域的特点以及与其他 4 个域的关系，同时也将阐述与电磁频谱域作战相关的一些基本概念和用语。

2.1 战争的变化

通信能力的提升极大地改变着战争的方式。无线电通信始于一个多世纪前。在那之前，远程通信只能通过有线的方式进行。出于实际考虑，军用通信在四五十年前大多数还是采用有线方式。舰船、飞机和地面移动装备需要无线通信，所以对无线电通信进行了大量研发。在第二次世界大战（简称二战）开始时，大多数参战方都研制出了雷达，无线电通信变得更先进了。

从一开始，对频谱的使用和控制就是一个问题。当马可尼用火花隙发射机进行首次跨大西洋传输时，占用了大量频谱，但对于当时世界上唯一的无线电传输，频谱是足够的。此后不久，研制出了调谐发射机，不过无线电链路之间的互扰依然是一个很大的问题。截获无线电通信和雷达信号以及对辐射源进行定位，对军事行动产生了巨大影响。截获、干扰、辐射源定位、信息安全以及传输安全成为了战争的基础，此后就一直如此了。

战争中使用的基本摧毁能力并没有发生太大的改变（从事这方面研究的人士可能对此有争议）。但是，这些能力的应用方式通过使用电磁频谱（EMS）发生了很大变化。现在，我们通过各种方式使用电磁频谱将武器的破坏能量制导引向预定的目标。电子战行业的人员也使用电磁频谱来阻止这些武器攻击其预定目标或阻止敌方发现目标的位置。

破坏性能量（快速运动的导弹、超高压或热能）用于杀伤敌方或摧毁其作战或生活所需的物质。有时，摧毁敌方的通信能力本身就是一个目标。这样，以前只有纬度、经度、高度和时间四维的战斗空间现在成了五维：增加了频率（见图 2.1）。

随着对破坏能的控制越来越强，我们对摧毁的重点就更加小心。我们希望将所有的破坏力都放到预定目标上。附带毁伤是对军事能力的一种浪费，即使是那些不关心无辜百姓死活的家伙也会发现这样会激怒各方面。对希望避免平民伤亡的人而言，武器的攻击焦点就成为一个更加紧迫的问题。

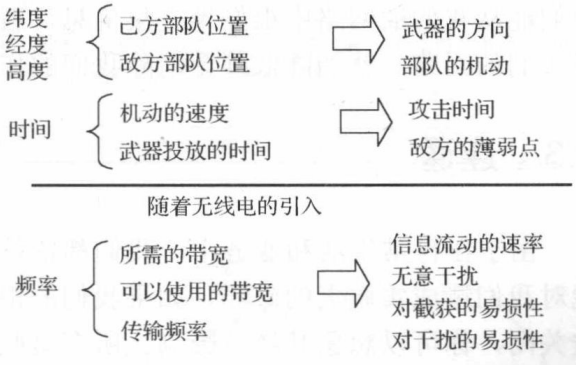

图 2.1 在无线电通信出现以前，战争在四维空间内进行。现在，频率成为另外增加的一维空间

2.2 与传播相关的特定问题

距离对无线电传播影响很大。根据不同的环境，接收到的信号强度是与发射机距离的平方或四次方相关的一个函数。这样，离接收机越近，接收到的信号就越好，通常就能更精确地定位发射机。如果我们具有多个接收机，距离敌方发射机最近的接收机所接收的信息最好（见图 2.2）。但是，为了利用这些信息，必须将其传送到制定决策的地方。这样，那些接收机必须成为网络的一部分。

一旦我们依赖来自多部接收机的输入，网络就会成为作战能力的关键。我们现在已经进入网络中心战。

然后考虑干扰敌方发射的问题。无论是通信干扰还是雷达干扰，必须形成足够高的干信比。通信干扰和雷达干扰两种干扰公式都包括从干扰机到被干扰的接收机之间距离的平方（或四次方）。如果我们有大量在地理上分布的干扰机，那么使用距目标最近的干扰机效果会最好。与之相关的一个问题就是它会对我们自己的电磁频谱设备形成干扰（即自扰）。如图 2.3 所示，距离目标接收机最近的干扰机能够用最低的功率进行干扰，这可以减小对己方通信或雷达的影响。

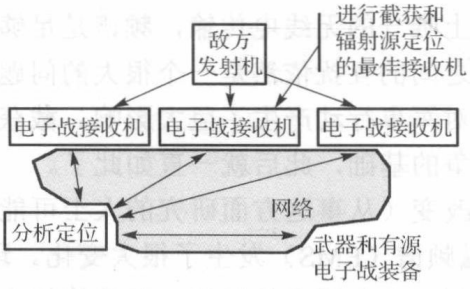

图 2.2 与敌方发射机的距离对截获和辐射源定位的性能有很大影响

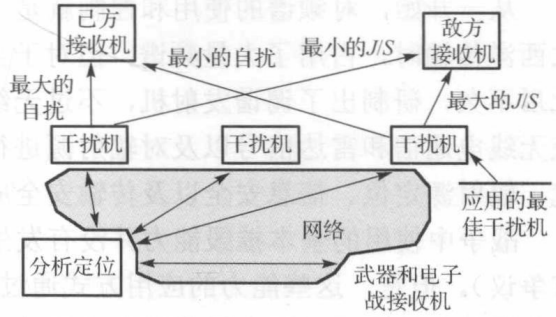

图 2.3 与敌方或己方接收机的距离对干扰效能和自扰有很大影响

同时，干扰机也必须是网络的一部分。当然，这个网络将成为敌方的重要目标。如果他们能从我们的网络中很好地搜集信息，就能很大程度确定我们的战术意图，如果能够摧毁我们的网路，就能降低甚至消除我们的作战能力。

2.3 连通

由于在日常生活和业务中，我们都依赖于互连互通，敌方通过对这种连通进行攻击就能对我们造成实质上的破坏。如果我们的银行交易系统、轨道基础设施或者航空运输系统被关闭，你可以想象其经济影响。所有这些系统以及我们的现代经济和军事能力的诸多方面都高度依赖连通，因此，一次射频或赛博攻击都可以导致重大的物理损坏，破坏其军事能力或严重扰乱其经济活动。在详细探讨对连通进行攻击之前，从技术角度讨论一下连通的特点将是有用的。

连通可以被认为是将信息从一个地方或一方转移至另一个地方或另一方的方式。其媒