



国防电子信息技术丛书

EW 104: EW Against a New Generation of Threats

应对新一代 威胁的电子战

[美] David L. Adamy 著

朱松 王燕 常晋聘 王晓东 译

姜道安 何涛 审校



中国工信出版集团



电子工业出版社
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 常晋聘 王晓东 译

姜道安 何涛 审校



电子工业出版社

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。

Authorized translation from English Language Edition entitled EW014: EW Against a New Generation of Threats, by David L. Adamy, ISBN-13: 978-1-60807-869-1, published by Artech House, Copyright ©2015 Artech House

Simplified Chinese Edition Copyright © 2017 by Publishing House of Electronics Industry.

All rights reserved.

本书中文翻译版专有出版权由 Artech House, Inc. 授予电子工业出版社,专有出版权受法律保护。
版权贸易合同登记号图字: 01-2015-7330

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。

2017年6月

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下，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	1	2.10.3 纠错与带宽	22
第 2 章 频谱战	3	2.11 电磁频谱战实践	22
2.1 战争的变化	3	2.11.1 作战域	23
2.2 与传播相关的特定问题	4	2.12 密写	24
2.3 连通	4	2.12.1 密写与加密	24
2.3.1 最基本的连通	5	2.12.2 早期的密写技术	25
2.3.2 连通需求	5	2.12.3 数字技术	25
2.3.3 远程信息传输	6	2.12.4 密写与电磁频谱战的 关系	26
2.3.4 信息保真度	7	2.12.5 如何对密写进行探测	26
2.4 干扰抑制	9	2.13 链路干扰	26
2.4.1 扩展发射频谱	9	2.13.1 通信干扰	26
2.4.2 商用调频广播	9	2.13.2 干扰数字信号所需的 干信比	27
2.4.3 军用扩频信号	10	2.13.3 对链路干扰的防护	27
2.5 信息传递的带宽需求	12	2.13.4 链路干扰的效应	28
2.5.1 无链路的数据传递	12	第 3 章 传统雷达	30
2.5.2 链路数据传输	13	3.1 威胁参数	30
2.5.3 软件的位置	13	3.1.1 典型的传统地空导弹	31
2.6 分布式军事能力	13	3.1.2 典型的传统截获雷达	32
2.6.1 网络中心战	14	3.1.3 典型的高炮	32
2.7 传输安全与信息安全	14	3.2 电子战技术	33
2.7.1 传输安全与传输带宽	16	3.3 雷达干扰	33
2.7.2 带宽限制	16	3.3.1 干信比	34
2.8 赛博与电子战	17	3.3.2 自卫干扰	34
2.8.1 赛博战	17	3.3.3 远距离干扰	35
2.8.2 赛博攻击	17	3.3.4 烧穿距离	37
2.8.3 赛博与电子战之间的 相似之处	18	3.4 雷达干扰技术	39
2.8.4 赛博战与电子战之间的 区别	19	3.4.1 压制干扰	39
2.9 带宽折中	19	3.4.2 阻塞干扰	39
2.9.1 对误码敏感的应用场景	20	3.4.3 瞄准式干扰	39
2.10 纠错方法	20	3.4.4 扫频瞄准式干扰	40
2.10.1 检错码与纠错码	21	3.4.5 欺骗干扰	40
2.10.2 分组码的例子	22	3.4.6 距离欺骗技术	40

3.4.7 角度欺骗干扰	41	4.3 地空导弹升级	68
3.4.8 频率波门拖离	43	4.3.1 S-300 系列	69
3.4.9 干扰单脉冲雷达	44	4.3.2 SA-10 及其改型	69
3.4.10 编队干扰	45	4.3.3 SA-12 及其改型	71
3.4.11 距离抑制编队干扰	45	4.3.4 SA-6 升级	71
3.4.12 闪烁	46	4.3.5 SA-8 升级	71
3.4.13 地形弹射	46	4.3.6 MANPADS 改型	72
3.4.14 交叉极化干扰	47	4.4 SAM 截获雷达改型	72
3.4.15 交叉眼干扰	47	4.5 AAA 改型	72
参考文献	49	4.6 对电子战的影响	73
第 4 章 下一代威胁雷达	50	4.6.1 增大杀伤距离	73
4.1 威胁雷达升级	50	4.6.2 超低旁瓣	73
4.2 雷达电子防护技术	51	4.6.3 相干旁瓣对消	74
4.2.1 推荐资料	51	4.6.4 旁瓣消隐	74
4.2.2 超低旁瓣	51	4.6.5 抗交叉极化	74
4.2.3 降低旁瓣电平对电子战的 影响	52	4.6.6 脉冲压缩	74
4.2.4 旁瓣对消	53	4.6.7 单脉冲雷达	74
4.2.5 旁瓣消隐	54	4.6.8 脉冲多普勒雷达	74
4.2.6 单脉冲雷达	55	4.6.9 前沿跟踪	75
4.2.7 交叉极化干扰	55	4.6.10 宽限窄电路	75
4.2.8 抗交叉极化	56	4.6.11 烧穿模式	75
4.2.9 线性调频雷达	56	4.6.12 频率捷变	75
4.2.10 巴克码	58	4.6.13 PRF 抖动	75
4.2.11 距离波门拖离	59	4.6.14 干扰寻的能力	76
4.2.12 AGC 干扰	60	4.6.15 改进型 MANPADS	76
4.2.13 噪声干扰质量	61	4.6.16 改进型 AAA	76
4.2.14 脉冲多普勒雷达的电子 防护特性	61	参考文献	76
4.2.15 脉冲多普勒雷达构成	61	第 5 章 数字通信	77
4.2.16 分离的目标	62	5.1 引言	77
4.2.17 相干干扰	63	5.2 传输比特流	77
4.2.18 PD 雷达中的模糊	63	5.2.1 传输比特率和信息比特率	77
4.2.19 低、高、中 PRF 脉冲 多普勒雷达	65	5.2.2 同步	78
4.2.20 干扰检测	66	5.2.3 带宽需求	79
4.2.21 频率分集	66	5.2.4 奇偶校验和检错纠错	80
4.2.22 PRF 抖动	66	5.3 内容保真	80
4.2.23 干扰寻的	68	5.3.1 基本的保真技术	80
		5.3.2 奇偶校验比特	82
		5.3.3 EDC	82
		5.3.4 交织	83

5.3.5 保护内容的保真度	83	6.4.4 天线很低的情况	111
5.4 数字信号调制	83	6.4.5 菲涅耳区	111
5.4.1 每个波特携带一个比特的调制	83	6.4.6 复杂反射环境	112
5.4.2 误码率	85	6.4.7 峰刃绕射	112
5.4.3 m 元 PSK	86	6.4.8 KED 的计算	114
5.4.4 I&Q 调制	87	6.5 对敌方通信信号的截获	115
5.4.5 不同调制方式下 BER 与 E_b/N_0 的关系	87	6.5.1 对定向传输的截获	115
5.4.6 高效的比特转移调制	88	6.5.2 对非定向传输的截获	116
5.5 数字链路规范	89	6.5.3 机载截获系统	117
5.5.1 链路规范	89	6.5.4 非 LOS 截获	117
5.5.2 链路余量	89	6.5.5 强信号环境下对弱信号的截获	119
5.5.3 灵敏度	90	6.5.6 搜索通信辐射源	120
5.5.4 E_b/N_0 与 RFSNR	91	6.5.7 战场通信环境	121
5.5.5 最大通信距离	91	6.5.8 一种有用的搜索工具	121
5.5.6 最小通信距离	92	6.5.9 技术因素	122
5.5.7 数据率	92	6.5.10 数字调谐接收机	122
5.5.8 误码率	93	6.5.11 影响搜索速度的实际因素	124
5.5.9 角跟踪速度	93	6.5.12 窄带搜索举例	124
5.5.10 链路带宽和天线类型	93	6.5.13 增加接收机带宽	126
5.5.11 气象因素	94	6.5.14 增加测向仪	126
5.5.12 抗欺骗保护	96	6.5.15 用数字化接收机搜索	127
5.6 抗干扰余量	96	6.6 通信辐射源定位	128
5.7 链路余量的具体计算	97	6.6.1 三角定位	128
5.8 天线对准损耗	98	6.6.2 单站定位	130
5.9 数字化图像	98	6.6.3 其他定位方法	131
5.9.1 视频压缩	99	6.6.4 均方根误差	131
5.9.2 前向纠错	100	6.6.5 校准	132
5.10 码	100	6.6.6 圆概率误差	132
参考文献	103	6.6.7 椭圆概率误差	133
第 6 章 传统的通信威胁	104	6.6.8 站址和对北	134
6.1 引言	104	6.6.9 中等精度的辐射源定位方法	136
6.2 通信电子战	104	6.6.10 沃特森-瓦特测向方法	137
6.3 单向链路	104	6.6.11 多普勒测向方法	138
6.4 传播损耗模型	107	6.6.12 定位精度	139
6.4.1 视距传播	107	6.6.13 高精度的方法	140
6.4.2 双径传播	108	6.6.14 单基线干涉仪	140
6.4.3 双径传播的最小天线高度	110	6.6.15 多基线精确干涉仪	143

6.6.16 相关干涉仪	143	7.3.7 扫频干扰	170
6.6.17 精确的辐射源定位方法	144	7.3.8 跟踪式干扰机	170
6.6.18 TDOA	144	7.3.9 FFT 时间	171
6.6.19 等时线	146	7.3.10 跟踪干扰的传播延迟	172
6.6.20 FDOA	147	7.3.11 可用的干扰时间	172
6.6.21 频率差的测量	149	7.3.12 慢速跳频和快速跳频	173
6.6.22 TDOA 和 FDOA 的结合	149	7.4 线性调频信号	173
6.6.23 TDOA 和 FDOA 辐射源 定位系统的 CEP 计算	150	7.4.1 宽带线性扫描	173
6.6.24 TDOA 和 FDOA 精度的 闭定表达式	150	7.4.2 对每个比特进行线性调频	174
6.6.25 散点图	151	7.4.3 并行二进制通道	175
6.6.26 对 LPI 辐射源的精确定位	152	7.4.4 脉冲位置多样化的单通道	176
6.7 通信干扰	152	7.5 直接序列扩频信号	177
6.7.1 对接收机的干扰	153	7.5.1 对 DSSS 接收机进行干扰	178
6.7.2 对网络的干扰	153	7.5.2 压制干扰	178
6.7.3 干信比	154	7.5.3 脉冲干扰	179
6.7.4 传播模型	154	7.5.4 抵近干扰	179
6.7.5 地基通信干扰	155	7.6 DSSS 和跳频	179
6.7.6 公式简化	156	7.7 对己方的误伤	180
6.7.7 机载通信干扰	157	7.7.1 误伤链路	180
6.7.8 高空通信干扰机	157	7.7.2 误伤最小化	181
6.7.9 防区内干扰	158	7.8 对 LPI 发射机的精确定位	183
6.7.10 干扰微波频段的无人机 链路	159	7.9 对手机进行干扰	183
参考文献	161	7.9.1 手机系统	183
第 7 章 现代通信威胁	162	7.9.2 模拟系统	184
7.1 引言	162	7.9.3 GSM 系统	185
7.2 低截获概率通信信号	162	7.9.4 CDMA 系统	185
7.2.1 处理增益	163	7.9.5 对手机进行干扰	186
7.2.2 抗干扰优势	163	7.9.6 从地面对上行链路 进行干扰	186
7.2.3 LPI 信号必须是数字信号	164	7.9.7 从空中对上行链路 进行干扰	187
7.3 跳频信号	164	7.9.8 从地面对下行数据链 进行干扰	188
7.3.1 慢速跳频和快速跳频	165	7.9.9 从空中对下行链路 进行干扰	189
7.3.2 慢速跳频	166	参考文献	189
7.3.3 快速跳频	167	第 8 章 数字射频存储器	190
7.3.4 抗干扰优势	167	8.1 DRFM 结构框图	190
7.3.5 阻塞干扰	168	8.2 宽带 DRFM	191
7.3.6 部分带宽干扰	169		

8.3	窄带 DRFM	192
8.4	DRFM 的功能	192
8.5	相干干扰	193
8.5.1	提升有效 J/S	193
8.5.2	箔条	194
8.5.3	距离门拖引干扰	194
8.5.4	雷达积累时间	195
8.5.5	连续波信号	195
8.6	对威胁信号的分析	196
8.6.1	频率多样性	196
8.6.2	脉间跳频	196
8.7	非相干干扰方法	197
8.8	跟随干扰	198
8.9	雷达分辨单元	198
8.9.1	脉冲压缩雷达	199
8.9.2	Chirp 调制	199
8.9.3	DRFM 的作用	200
8.9.4	Barker (巴克) 码调制	201
8.9.5	对 Barker 码雷达进行干扰	203
8.9.6	对干扰效率的影响	204
8.10	复杂假目标	204
8.10.1	雷达截面积	204
8.10.2	RCS 数据的生成	205
8.10.3	通过计算获得 RCS 数据	205
8.11	DRFM 使能技术	206
8.11.1	捕获复杂目标	206
8.11.2	DRFM 架构	207
8.12	干扰和雷达测试	208
8.13	DRFM 的反应时间	208
8.13.1	相同的脉冲	208
8.13.2	相同的 chirp 脉冲	208
8.13.3	相同的 Barker 码脉冲	209
8.13.4	脉间变化的脉冲	210
8.14	需要使用 DRFM 对抗措施的 雷达技术	211
8.14.1	相参雷达	211
8.14.2	前沿跟踪	212
8.14.3	跳频	212
8.14.4	脉冲压缩	212

8.14.5	距离变化率与多普勒 频移相关	213
8.14.6	RCS 分析	214
8.14.7	高占空比脉冲雷达	214
参考文献		214

第 9 章	红外威胁与对抗	215
9.1	电磁频谱	215
9.2	红外传播	216
9.2.1	传播损耗	216
9.2.2	大气衰减	216
9.3	黑体理论	217
9.4	红外制导导弹	218
9.4.1	红外导弹的构成	218
9.4.2	红外导引头	219
9.4.3	调制盘	219
9.4.4	红外传感器	220
9.5	其他类型的跟踪调制盘	221
9.5.1	辐条轮调制盘	221
9.5.2	多频调制盘	221
9.5.3	弯曲辐条调制盘	222
9.5.4	玫瑰型跟踪器	222
9.5.5	交叉线性阵列跟踪器	223
9.5.6	成像跟踪器	223
9.6	红外传感器	224
9.6.1	飞机的温度特征	224
9.7	大气窗口	225
9.8	传感器材料	225
9.9	单色与双色传感器	226
9.10	曳光弹	227
9.10.1	引诱	227
9.10.2	迷惑	227
9.10.3	冲淡	227
9.10.4	时机问题	228
9.10.5	频谱和温度问题	229
9.10.6	温度感应跟踪器	229
9.10.7	时间相关的防御手段	230
9.10.8	位置相关的防御手段	231
9.10.9	曳光弹的操作安全问题	232
9.10.10	曳光弹组合	234

9.11 成像跟踪器	234	10.4.2 天线隔离度	252
9.11.1 成像跟踪器的交战	235	10.4.3 机载迷惑式诱饵	252
9.11.2 目标截获	235	10.4.4 机载诱骗式诱饵	252
9.11.3 中段	235	10.5 舰船防护诱骗式诱饵	252
9.11.4 末段	236	10.5.1 舰船诱骗式诱饵的雷达截面积	252
9.12 红外干扰机	237	10.5.2 诱饵的部署	253
9.12.1 热砖干扰机	238	10.5.3 转移模式	254
9.12.2 对跟踪器的干扰效果	238	10.6 拖曳式诱饵	254
9.12.3 激光干扰机	239	10.6.1 分辨单元	255
9.12.4 激光干扰机的操作问题	240	10.6.2 应用实例	256
9.12.5 干扰波形	240		
第 10 章 雷达诱饵	242	第 11 章 电子支援与信号情报	257
10.1 简介	242	11.1 引言	257
10.1.1 诱饵的任务	242	11.2 SIGINT	257
10.1.2 无源与有源雷达诱饵	243	11.2.1 COMINT 和通信 ES	258
10.1.3 雷达诱饵的部署	244	11.2.2 ELINT 和雷达 ES	258
10.2 饱和式诱饵	244	11.3 天线和距离	259
10.2.1 饱和式诱饵保真度	245	11.4 天线	259
10.2.2 机载饱和式诱饵	245	11.5 截获距离	261
10.2.3 雷达分辨单元	247	11.6 接收机	262
10.2.4 舰载饱和式诱饵	247	11.7 频率搜索问题	264
10.2.5 探测式诱饵	248	11.8 处理问题	265
10.3 诱骗式诱饵	249	11.9 增加一台记录仪	267
10.4 投掷式诱饵	250	参考文献	267
10.4.1 飞行式诱饵	251		

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。

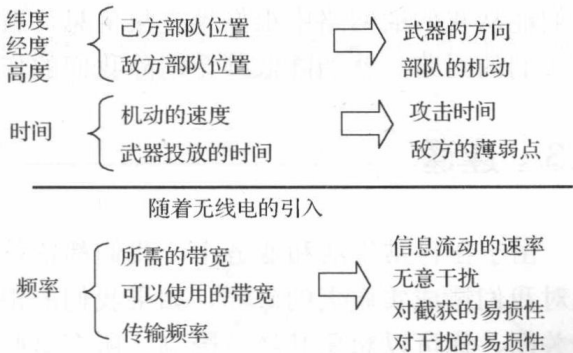


图 2.1 在无线电通信出现以前，战争在四维空间内进行。现在，频率成为另外增加的一维空间

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。

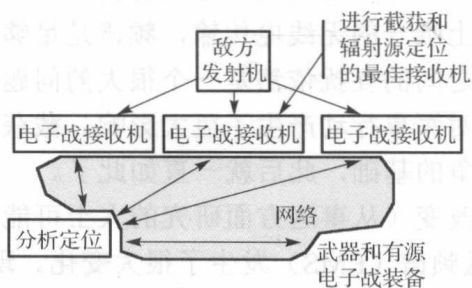


图 2.2 与敌方发射机的距离对截获和辐射源定位的性能有很大影响

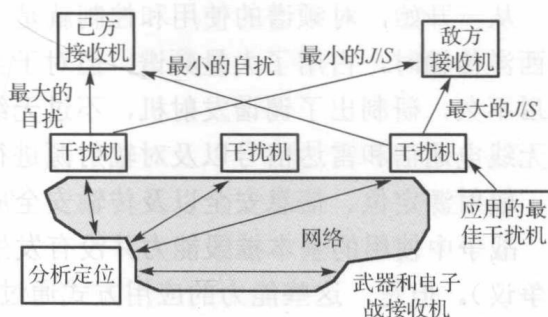


图 2.3 与敌方或己方接收机的距离对干扰效能和自扰有很大影响

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益的。

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