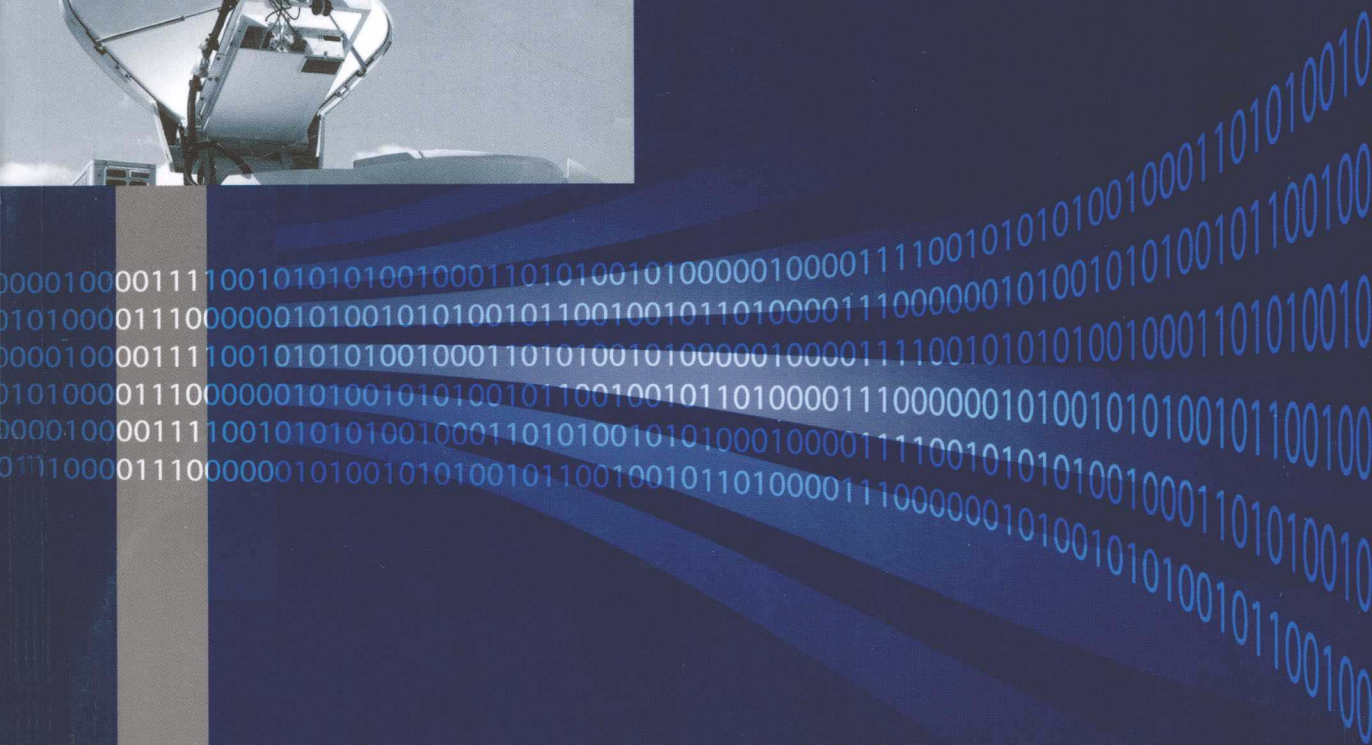
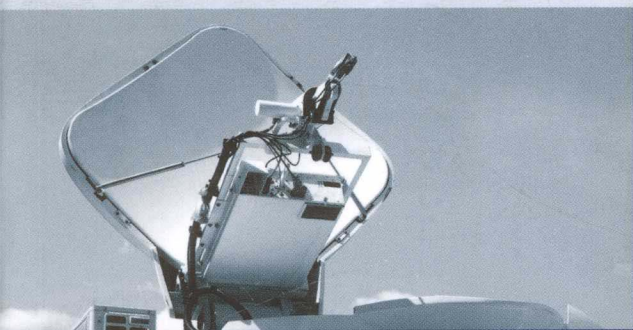


现代 电子战导论

(上)

司锡才 司伟建◎编著



哈尔滨工程大学出版社
Harbin Engineering University Press

现代电子战导论

(上册)

司锡才 司伟建 编著

哈尔滨工程大学出版社

内 容 简 介

本书论述了电子战的新概念、内涵、定义、主要内容以及原理、数学公式推导、计算方法、实现的技术措施与方法。电子战包括电子进攻、电子防护、电子支援;电子进攻包括反辐射武器攻击、定向能攻击、电磁欺骗、电磁干扰;电子防护包括对敌方电子进攻时,己方的电子防护,又包括己方、友方在使用电子进攻时,己方的电子防护;电子支援包括对敌方辐射源的探测、信号分析、识别、参数提取、定位和报警。与以前的同类书相比,本书增加了反辐射武器与定向能武器及其攻击;增加了己方与友方进行电子攻击时,己方的电子防护;增加了数字信道化测频、数字接收机测向以及信号细微特征(“指纹”)分析、识别与提取、无源定位等新理论、新方法、新技术。

本书可作为各阶段信息对抗专业学生的教材使用,包括本科生,硕士及博士研究生,亦可供从事相关专业的研究人员参考使用。

图书在版编目(CIP)数据

现代电子战导论/司锡才,司伟建编著. —哈尔滨:
哈尔滨工程大学出版社,2012. 11

ISBN 978 - 7 - 5661 - 0457 - 1

I. ①现… II. ①司…②司… III. ①电子对抗
IV. ①TN97

中国版本图书馆 CIP 数据核字(2012)第 241980 号

出版发行 哈尔滨工程大学出版社
社 址 哈尔滨市南岗区东大直街 124 号
邮政编码 150001
发行电话 0451 - 82519328
传 真 0451 - 82519699
经 销 新华书店
印 刷 哈尔滨市石桥印务有限公司
开 本 787mm × 1 092mm 1/16
印 张 29.25
字 数 762 千字
版 次 2012 年 10 月第 1 版
印 次 2012 年 10 月第 1 次印刷
定 价 53.00 元
<http://press.hrbeu.edu.cn>
E-mail: heupress@hrbeu.edu.cn

前言

目前,我们正处于高技术战争时代,不久的将来(2030~2050)我们将进入信息化战争时代,无论是高技术战争,还是信息化战争,电子战是战争的主要内容,是战争的主要手段。电子战的概念、内涵、内容随着时代的变化而变化,但电子战是战争永恒的话题。

信息化战争是扩大了的电子战,电子战是信息化战争的主要内容和技術支撐。信息化战争是电子战发展的必然。因此,要驾驭信息化战争,就必须掌握电子战理论、技术与方法。

本书按照电子战的新概念,注入了新内容:电子进攻中的反辐射武器攻击与定向能攻击;电子防护不仅是敌人在电子进攻时己方要进行电子防护,而且己方或友方对敌实施电子进攻,己方也要进行电子防护。电子支援除了过去采用的模拟手段实现侦察与报警,本书还增加了数字接收机、宽频数字信道化、信号细微特征(“指纹”)分析、识别与提取,超分辨高精度空间谱估计测向,立体基线测向以及虚拟基线与立体基线解超宽频带测向解模糊,单站无源定位等一系列先进理论、技术与方法。

本书的内容丰富,知识面广,选用其中的部分内容可以作为信息对抗专业本科生的教材;还可以选用其中的部分内容作为硕士研究生的教材;本书与《信息化战争导论》结合在一起,选用相关的内容可作为博士生教材。

论述电子战的新概念、新内容、新技术、新方法是本书的特点,既可作为各层次学生的教材或参考书,也可以作为信息对抗或电子战专业人员的参考用书。

本书在编写过程中参考借鉴了国内外一些专家学者的论著,在此表示衷心的感谢!

由于作者水平所限,书上错漏或不妥之处在所难免,欢迎广大读者批评指正。

编著者

2009年10月

目 录

第1章 信息化战争	1
1.1 电子战的概念	1
1.2 电子战的作战思想	5
1.3 电子战信号环境	10
1.4 电子战的发展	15
1.5 电子战体系	30
1.6 信息化条件下的电子战	41
1.7 美国电子战及相关术语的演变	45
1.8 电子战是现代高技术战争与信息化战争的“杀手锏”	54
1.9 21 世纪电子战装备发展趋势	64
1.10 美军转型中的电子战	67
第2章 电子进攻概述与反辐射武器	78
2.1 概述	78
2.2 反辐射武器	78
第3章 定向能武器	100
3.1 新概念武器	100
3.2 动能武器——电磁导轨炮	106
3.3 基因武器	112
3.4 计算机病毒武器	115
3.5 地球物理武器及其发展趋势	122
3.6 定向能武器(Direction Energy Weapon)	128
3.7 激光武器(Laser Wepon)	181
3.8 粒子束武器	212
3.9 等离子体武器	215
第4章 电子干扰(Electronic Interference)	218
4.1 概述	218
4.2 遮盖性干扰	225
4.3 射频噪声干扰	234
4.4 噪声调频干扰	243
4.5 雷达有源干扰方程	274

4.6	欺骗性干扰	310
4.7	无源箔条干扰及干扰方法	350
第5章	电子防护 (Electronic Protection)	380
5.1	概述	380
5.2	电子战隐身技术	382
第6章	雷达隐身技术	393
6.1	外形隐身	393
6.2	涂层	393
第7章	箔条(干扰丝/带)干扰	400
7.1	箔条干扰的一般特性	400
7.2	箔条的有效反射面积	401
第8章	无源假目标——反射器	411
8.1	角反射器	411
8.2	龙伯透镜反射器	417
8.3	万-阿塔反射阵	419
第9章	雷达抗反辐射导弹	420
9.1	概述	420
9.2	雷达诱饵抗反辐射导弹	426
参考文献		459

第 1 章 信息化战争

电子战是信息化战争的主要内容也是信息化战争的技术支撑,信息化战争是扩大了电子战。因此,电子战是现代高技术战争乃至信息化战争的主要组成部分,电子战是战争永恒的主题。

现代电子控制、引导及指令控制武器的激增带动了一个科学领域的迅猛发展,这就是电子战。电子战的基本理论是在整个电磁频谱范围内,利用敌方的电磁发射,提供有关敌方战斗序列、作战意图和作战能力的情报,采用对抗措施和硬摧毁,阻止敌方有效地运用通信和武器系统,并同时保护己方有效地使用同一频谱。一条已被普遍接受的军事原则是,任何一场未来战争的胜利,将属于能最有效地控制电磁频谱的一方。

电子战是一个动态变化的领域,它必须对不断变化的威胁作出响应。这一点在它从第二次世界大战中的早期应用到现在的演变中反映了出来。这里,我们将详细论述现代电子战理论,它是军事战略不可缺少的基本要素,当与其他军事设施协同使用时,它将提供一种削弱敌方力量(战斗力倍减效应)而同时加强己方力量(战斗力倍增效应)的方法。

依据现代战争理论,电子战是整个军事战略的重要组成部分,它集中力量压制敌方指挥和控制系统(即 C^3I 系统、 C^4ISR 或 C^4I^2WSR),同时保持己方(即 C^3I 系统、 C^4ISR 或 C^4I^2WSR)系统的工作能力。为了理解这一战略,在此我们先离开主题,简单说明一下指挥和控制系统的必要性及其功能。基本理论是,仅干扰或摧毁一部雷达或一个通信系统,也许对敌方武器系统的工作不会产生多大影响,尤其是当被干扰或被摧毁的对象是备用网的组成部分时,影响更小。因此,有必要摧毁敌方武器系统的一个节点,为完成此项任务,仅靠电子战本身也许不是最佳方式。

对指挥和控制系统的需求是随着现代战争的发展而出现的,并由于武器平台的机动性、武器的射程和杀伤力的发展而不断增加。现代战争的发展速度和现状,要求运用电子战手段来控制武器的运用,评价它们的效果,并统管整个武器系统的战斗使用。这样,连接各种传感器、作战指挥所和通信中心的总体结构便组成了指挥和控制系统。指挥官就通过这样一种结构去指挥他的部队,完成指定的作战任务。通信线路、指挥所、传感器和情报、传感器协调中心都是“反指挥和控制系统”作战行动的主要目标。

1.1 电子战的概念

电子战是现代高技术战争和未来信息化战争的重要组成部分,而且发展非常迅猛。由于电子战将直接影响战争的作战能力和效果,国内外非常重视电子战技术和战术研究。

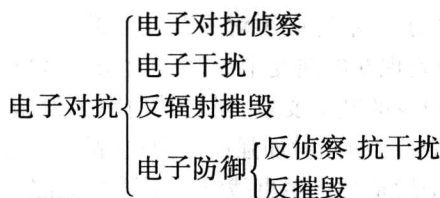
电子战在学科上的定义包括两个相互竞争的方面,即电子对抗和电子反对抗(Electronic - Counter Measures, ECM, Electronic - Counter - Counter - Measures, ECCM)。在军事科学上则包括电子进攻、电子防御和电子支援(Electronic Attack, EA; Electronic Protection, EP; Electronic Support, ES)。

1.1.1 我国电子对抗的定义与发展

1982年出版的《中国人民解放军军语》中将电子对抗定义为:敌对双方利用电子设备或器材进行的电磁斗争。即利用专门的无线电电子设备或器材,对敌方无线电电子设备进行的斗争,用以阻止敌方无线电电子设备获得电磁信息,减弱和破坏敌武器系统的效能和威力,同时保护自己的无线电电子设备及武器系统在敌方干扰条件下仍能正常发挥效能和威力。

1994年出版的《中国军事百科全书》上对电子对抗的定义是:“军事上为削弱破坏敌方电子设备的使用效能,同时保护己方电子设备正常发挥效能而采取的综合措施”。这个“综合措施”就涵盖了所有电子对抗手段,其中包括“软”、“硬”两个领域。可以说这在揭示电子对抗内在本质的规律性上有很大提高。

由我国军标《电子对抗术语》可知电子对抗就是电子战,其内容包括电子对抗侦察、电子干扰、反辐射摧毁和电子防御。按照军标,在我国无“反电子对抗”一词,我国的电子对抗的内容为:



我国的电子对抗也包含电子对抗支援、电子进攻和电子防御的内容,但无电子进攻一词。电子对抗设备包括电子侦察(告警)设备、电子干扰设备、摧毁武器(如反辐射导弹)。电子防御设备包括雷达、通信、导航和C⁴ISR系统等电子设备。综上所述,各国的电子对抗或电子战的概念基本是一致的,都包含作战双方的电磁竞争。

1.1.2 俄、美电子战定义

前苏联军队把电子对抗(电子战)称为“无线电电子斗争”,定义为“对敌方无线电电子器材和系统实施侦察,并随之进行无线电电子压制,以及对己方无线电电子器材和系统进行无线电电子防御的综合措施”。无线电电子斗争包含无线电电子压制、无线电电子防护和电子斗争保障措施,包含电子进攻性和电子防御性两方面。

美国的电子战定义为:“利用电磁能和定向能以控制电磁频谱或攻击敌人的任何军事行动”。其中包括电子进攻、电子防御和电子支援。

电子战(EW)——使用电磁能和定向能控制电磁频谱或攻击敌军的任何军事行动。电子战包括三个主要部分,即电子攻击、电子防护和电子战支援。

电子攻击(EA)——以削弱、抵消或摧毁敌方战斗能力为目的,使用电磁能或定向能攻击其人员、设施或装备。

电子防护(EP)——为保护人员、设施和装备在己方实施电子战或敌方运用电子战削弱、抵消或摧毁己方战斗能力时不受任何影响而采取的各种行动。

电子战支援(ES)——由作战指挥官分派或在其直接控制下,为搜索、截获、识别和定位有意或无意电磁辐射源,以达立即辨认威胁之目的而实施的各种行动。

最新定义电子战具有下列几个特点:

(1)更加强调了电子战的进攻性,不仅把反辐射武器,而且把定向能武器也列入了电子

攻击手段的范畴;

(2) 电子攻击的目的不仅是降低敌方电子装备的性能,而且是削弱、抵消或摧毁敌方的战斗力;电子攻击的目标不仅是设施或装备,而且还包括操纵这些设施和装备的人员;

(3) 电子防护不仅包括防护敌方电子战活动对己方装备、人员的影响,而且包括防护己方电子战活动对己方装备、人员的影响。

由此可见,最新定义的电子战大大扩展了其内涵和作用范畴。

美国对电子战的定义仅局限于作战使用过程,实际上电子战不仅在战争时期进行,在战争后及平时时期仍然广泛应用,其内容更广,范畴更大。为此,在本书中应用“电子侦察”来代替美军电子战定义中的“电子战支援”,以便把信号情报也包括在内。

电子战内涵和定义的几经变迁,总是与电子战作战活动的发展(第一次世界大战:通信对抗;第二次世界大战:预警雷达对抗;越南战争:制导雷达对抗;中东战争:反辐射攻击;海湾战争:综合电子战)密切相关,而且总是电子战技术、装备和使用战术的发展推动了电子战定义的更新和扩展。随着电子战范畴越来越广,电子战的目的已不仅是干扰和阻断敌方的通信,干扰和破坏敌方雷达等简单的目标,而且还逐步扩展到攻击敌方的决策能力,同时阻止敌方攻击己方的决策能力。因此,应该用“信息战”这个术语来表达这一新的发展概念。同时,最近国内外正在兴起的信息战概念研究和实践,也必将会在新的条件下推动电子战内涵的发展。

表 1.1 电子战的分类表

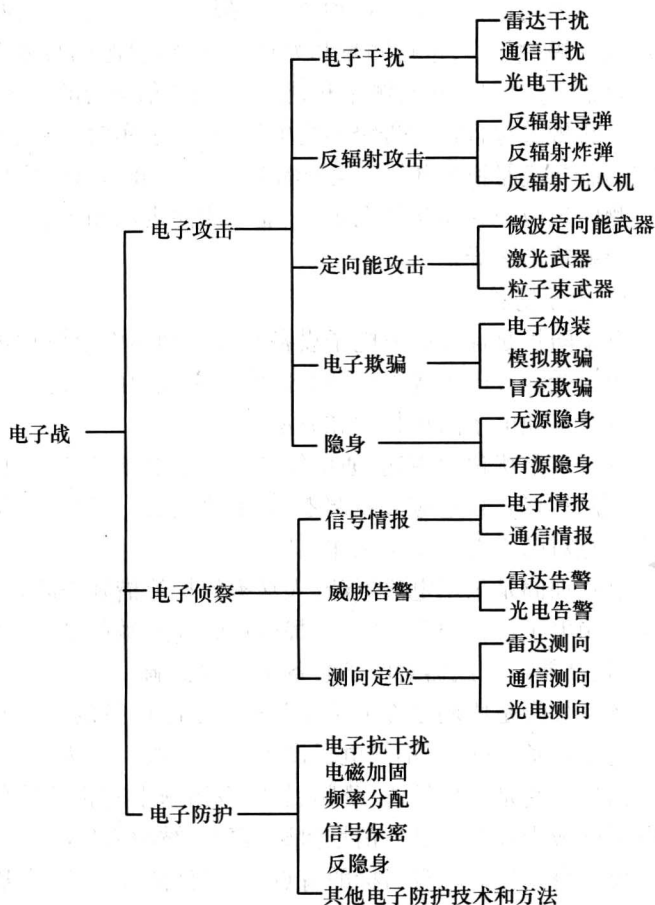
1.1.3 电子战的分类

根据电子战的最新定义,列出电子战的分类如表 1.1 所示。

电子战包含三大部分:电子攻击、电子侦察和电子防护(表 1.1),分述如下。

1. 电子攻击

电子攻击是电子战的进攻性部分,用于阻止敌方有效地利用电磁频谱,使敌方不能有效地获取、传输和利用电子信息,影响、延缓或破坏其指挥决策过程和精确制导武器的运用。电子攻击包含自卫性电子战和进攻性电子战两大部分。自卫性电子战防卫是应用自卫电子干扰、电子欺骗和隐身技术,保护作战平台或军事目标免遭敌精确制导武器的攻击,进攻性电子战是应用支援电子干扰、反辐射武器和定向能武器,攻击敌方的防御



体系,以保证己方的安全突防。

电子干扰用于发射或反射特定的电子信号,以扰乱或破坏敌方军用电子设备的工作,它包含雷达干扰、通信干扰、光电干扰和对其他电子装备的干扰措施(如计算机病毒干扰、导航干扰、引信干扰、敌我识别干扰等)。

反辐射武器用于截获、跟踪、摧毁电磁辐射源目标,它包含反辐射导弹、反辐射炸弹、反辐射无人机以及它们的攻击引导设备。

定向能武器应用定向辐射的大功率能量流(微波、激光、粒子束),在远距离使高灵敏的电磁传感器致盲、致眩,在近距离使武器平台因过热而烧损,它包含微波定向能武器、激光武器、粒子束武器等。

电子欺骗用于辐射或反射特定的电磁信号,向敌方传送错误的电磁信息。它包含电子伪装、模拟欺骗和冒充欺骗。

隐身用于减小目标的可检测性,降低雷达、红外探测器的作用距离。它包含无源隐身和有源隐身。

2. 电子侦察

电子侦察用于获取战略、战术电磁情报和战斗情报,它是实施电子攻击和电子防护的基础和前提,并为指挥员提供战场态势分析所需的情报支援。它包含信号情报、威胁告警和测向定位三部分。

信号情报包含电子情报和通信情报两部分。电子情报用于收集除通信、核爆炸以外的敌方电磁辐射信号,进行测量和处理,获得辐射源的技术参数及方向、位置信息。通信情报用于收集通信信号,进行测量和处理,获取通信电台的技术参数、方向、位置及通信信息内容。

威胁告警包含雷达告警和光电告警,用于实时收集、测量、处理对作战平台有直接威胁的雷达制导武器和光电制导武器辐射的信号,并向驾驶员发出威胁警报,以便采取对抗措施。

测向定位包含雷达测向定位、通信测向定位和光电测向,用于支援电子干扰的角度引导和反辐射攻击引导。

3. 电子防护

电子防护是保证己方电子设备有效地利用电磁频谱的行动,以保障己方作战指挥和武器运用不受敌方电子攻击活动的影响。它包含电子抗干扰、电磁加固、频率分配、信号保密、反隐身及其他电子防护技术和方法。

电子抗干扰包含雷达、通信等各类军事电子设备专用的抗干扰技术和方法,如超低副瓣天线、旁瓣对消、自适应天线调零、频率捷变、直接序列扩谱等等,用以减小或降低各类电子干扰措施对己方电子设备工作的影响。

电磁加固是采用电磁屏蔽,大功率保护等措施来防止高能微波脉冲、高能激光信号等耦合至军用电子设备内部,产生干扰或烧毁高灵敏的芯片,以防止或削弱超级干扰机、高能微波武器、高能激光武器对电子装备工作的影响。

频率分配是协调己方电子设备和电子战设备的工作频率,以防止己方电子战设备干扰己方电子设备,并防止不同电子设备之间的相互干扰。

信号保密是应用扩谱、跳频、加密等措施来防止传输信号被敌方侦收、分析、解密,并应用电磁屏蔽措施防止己方信号泄漏、辐射,被敌方侦收。

反隐身是针对隐身目标的特点,采用低波段雷达、多基地雷达、无源探测、大功率微波武器等多种手段,探测隐身目标,或烧蚀其吸波材料。

其他电子防护技术和方法,如应用雷达诱饵吸引反辐射武器攻击,保护真雷达的安全;应用无线电静默措施反侦察;应用组网技术反点源干扰;隐蔽关键电子设备,战时突发工作等战术、技术措施。

电子战按技术领域分类,包括雷达对抗、通信对抗、光电对抗、计算机对抗等,以及雷达、通信、光电、计算机等装备的反对抗。其中雷达对抗、通信对抗、光电对抗等将在以下各章节详细介绍,本章重点介绍雷达电子战。

1.2 电子战的作战思想

1.2.1 概述

军队在许多应用方面依赖于电磁频谱,包括(但并不仅限于)通信、探测、识别和目标定位。在支援任务中,电子战的有效运用对于发现、确定、跟踪、瞄准并与对手交战的能力以及遏制对手的上述能力都是十分重要的。参与军队电子战的计划人员、操作人员、采办人员以及其他人员必须了解威胁系统的技术进展与延伸,以便运用电磁频谱保护己方军队。

若要使电子战发挥作用,必须运用控制、利用和增强三原则。电子战的三个要素(电子攻击、电子防御和电子战支援)都运用了这三个原则。正确运用这些要素能在不同程度上达到探测、阻止、扰乱、欺骗和摧毁敌人的目的,进一步保证整个任务的完成。

1.2.2 电子战原则

美国电子战原则可以概括为控制、利用和增强。

1. 控制

控制指直接或间接地控制电磁频谱,从而使己方部队能够使用电磁频谱,并利用其攻击敌军以保护己方频谱不被利用或遭受攻击。电子战通常具有进攻和防御两个方面,应当协同使用以支持任务的完成。如同空中优势可以使己方部队自由攻击、自由机动一样,电子战的合理协调运用可以使己方部队使用电磁频谱。例如,可以通过干扰攻击敌军指挥控制网络扰乱敌军部署部队的能力。合理运用电子防御可以使己方雷达即使在敌军干扰的情况下也能继续工作。

2. 利用

利用就是运用电磁频谱加强己方部队的优势。己方部队可通过不同程度的探测、阻止、扰乱、欺骗和摧毁手段阻碍敌军的决策环路。例如,可使用电磁欺骗发送误导敌军的信息,也可通过敌军的电磁辐射对其进行定位和识别。在第二次世界大战期间,美国就曾通过日本海军的无线电通信对其舰船进行跟踪。由于无线电报务员手法各不相同,所以,通过跟踪无线电通信,美国海军情报部门就能知道日本每艘舰船所处的位置。同样,己方飞机可以使用雷达告警接收机来定位和识别敌军的地空导弹威胁。

3. 增强

增强就是将电子战作为力量增强器。将电子战综合到航空航天行动中,可以在不同程度上探测、阻止、扰乱、欺骗或摧毁敌军部队,增强整个作战任务的效果。通过控制和利用电磁频谱,电子战具有力量增强器的作用,可提高任务成功的可能性。在“波斯尼亚”行动的

第一天夜晚,敌军的地空导弹系统因受机载干扰机和反辐射导弹的影响而不能发挥作用,致使北约飞机没有障碍地到达要打击的首要目标。

1.2.3 电子战要素

电子战的三个主要要素是电子攻击、电子防御和电子战支援,如图 1.1 所示。

1. 电子攻击

电子攻击包括防区外干扰、高速反辐射武器、箔条、曳光弹、自卫干扰和定向能武器等。

电子攻击是指利用电磁能、定向能或反辐射武器攻击敌军人员、设施或设备,以达到降低、削弱或摧毁敌军战斗力的目的。它还能阻止或削弱敌军使用电磁频谱。电子攻击通过探测、阻止、扰乱、欺骗和摧毁来实现,其中最主要的是探测。电子攻击包括用高速反辐射武器直接攻击和主动使用箔条、曳光弹、噪声干扰、欺骗干扰和一次性使用的小型干扰诱饵以及电磁能或定向能武器(激光、射频武器、粒子束等)。电子辐射控制和低可观测技术则属于电子攻击的被动运用。电子攻击以往称为电子对抗措施(ECM)。

电磁干扰和对敌防空压制(SEAD)也属电子攻击的范畴。

电磁干扰是以阻止或削弱敌军有效使用电磁频谱为目的的电磁能有意辐射、再辐射或反射,其意图是削弱或阻止敌军的战斗能力。早期的电子战工作主要是对敌军雷达进行电子干扰,以掩藏己方飞机的数量和位置,并降低敌军雷达控制武器的精度。而现在则是通过干扰敌军传感器来实现。

2. 电子防御

电子防御包括在敌军使用可以削弱、压制或摧毁己方战斗能力的电子战时,为确保己方有效地使用电磁频谱而采取的各种行动。电子防御包括无线电电台的频率捷变和改变雷达脉冲重复频率等。电子防御和其他安全措施的综合运用可以防止敌军对己方的探测、阻止、扰乱、欺骗或摧毁。电子防御是防御性信息对抗的组成部分,需要合理地纳入到信息作战行动中。己方部队对先进技术的依赖性需要电子防御安全措施。合理的频率管制是防止产生对己不利影响(如干扰己方部队等)的一个关键要素。许多成功的电子防御措施产生于装备的设计和采办期间。电子防御以往称为电子反对抗措施(ECCM)。

3. 电子战支援

电子战支援包括雷达告警接收机、通信情报和电子情报等。

电子战支援是指对有意和无意辐射源与电磁能进行搜索、截获、识别和定位,以进行威胁识别的各种活动。指挥官、机组成员和操作员可通过电子战支援提供近实时信息,以补充来自其他情报源的信息。电子战支援的信息可以同其他情报、监视与侦察的信息进行相关,从而更为准确地提供战场态势。这种信息可以成为态势感知的电子战斗序列(EOB),也可以用于研究新的对抗措施。电子战支援数据能够用于产生信号情报,包括通信情报和电子情报。因此,电子战支援能为有效阻止敌军使用电磁频谱,同时确保己方使用电磁频谱提供所需要的信息。电子战支援可对电子战作战行动和其他战术行动(如威胁规避、目标瞄准和寻的等)立即进行决策。它具有无源特点使其在和平时期可以得到有效的运用。电子战



图 1.1 电子战三要素

支援以往称为电子支援措施(ESM)。

1.2.4 电子战作用

电子战要通过探测、阻止、欺骗、扰乱和摧毁相结合的方式在整个电磁频谱中进行控制和使用。电子战的作战运用并不限于有人驾驶飞机,也适用于从地面到空间的无人驾驶飞行器。倘若能合理运用电子战以控制电磁频谱就可以获得优势,但如果未予以综合考虑而错误地使用电子战则会增加己方部队的危险。比如干扰时间选择不当可能会导致把注意力集中到另外一支不相干的部队上或妨碍己方部队使用频率。错误或不当的雷达告警接收机可能会导致采取不恰当的反应。只有灵活使用探测、阻止、欺骗、扰乱和摧毁等手段才是合理运用电子战。

1. 探测

探测是采用有源和无源手段对电磁环境(包括雷达/无线电频率、光电/激光和红外等)进行监测的行动,这是电子战的第一步。因为有效描述电磁环境对于确立准确的电子战斗序列是必不可少的。电子战斗序列对于电子战的决策和使用电磁频谱来满足任务目标是至关重要的。各种探测手段包括机载接收机、天基系统、无人航空器(LAV)、人工情报(HUMINT)和情报监视与侦察系统。探测能支持电子攻击、电子防御和电子战支援并规避已知敌对系统。无法规避时,阻止、欺骗、扰乱或摧毁敌军电子系统都要用到探测。

2. 阻止

阻止即控制敌军或敌方接收信息,防止敌军获取准确的己方信息。阻止可以通过传统的噪声干扰技术阻塞敌军通信系统信道或雷达显示来实现,也可以通过更为先进的电子欺骗技术或摧毁性措施来进行。

3. 欺骗

欺骗就是对敌军进行扰乱或误导。电子战的一个目标是通过电磁频谱切入敌军的决策环路,使其难以区分现实与已有感知。若敌军依赖电磁传感器收集情报,就可以向这些系统注入欺骗性的信息,使其产生误导或混乱。欺骗性干扰应尽可能多地模仿敌军信息源以达到理想的目的。多传感器欺骗可以增加敌军对那些感觉上“似是而非”的欺骗行动的信任度。电子欺骗行动由军事欺骗军官协调,在欺骗计划、信息作战行动计划和整个战役计划的全过程中都要考虑电子欺骗的问题。作战保密(OPSEC)对有效地欺骗计划极为关键。

电磁欺骗是采用某种方式有意辐射、再辐射、替换、压制、吸收、阻止、增强或反射电磁能,其意图是向敌军或敌军依赖电磁的武器传送错误信息,从而削弱或阻止敌军战斗能力。欺骗干扰机/发射机能在敌军雷达显示器上产生假目标,或引导敌军雷达错误地测量目标速度、距离或方位。这种干扰机/发射机的工作方式是接收到敌军雷达的能量脉冲,对其进行替换后再把替换信号传给敌军的雷达。

电磁欺骗的类型有伪装式电磁欺骗、模拟式电磁欺骗和冒充式电磁欺骗。

伪装式电磁欺骗是为避免暴露或向敌军传递可能为敌军所用的假信号而采取的行动。如通过发射模拟的敌军系统信号使敌军传感器接收这些模拟信号,并作为真实情况记录,从而误导敌军。低可观测技术是伪装式电磁欺骗的一种无源方式。通过无源伪装式电磁欺骗的一种无源方式。通过无源伪装或阻止威胁系统不能接收正确的回波脉冲,改变航空航天飞行器的可感知范围。电磁欺骗可以使用通信或非通信信号传递误导敌军的信息,使敌军的情报和电子战部队失去作用。伪装式电磁欺骗可误导敌军的电子战支援和电子攻击资

源,从而使己方通信几乎不出现问题。在这种应用场合,伪装式欺骗就是一种电子防御技术。

模拟式电磁欺骗即模拟友军和己军以误导敌军的行动。模拟式电磁欺骗包括采用箔条模拟假目标使敌军产生有大型攻击编队的印象,或采用干扰机发射欺骗干扰误导敌军目标跟踪雷达,使其不能发现目标的真实位置。

冒充式电磁欺骗是将电磁能引入敌军系统,冒充敌军的发射。敌军的任何接收机都可以作为冒充式电磁欺骗的目标。这种欺骗方式可用于掩护己方作战行动。如采用转发式干扰技术冒充敌军雷达脉冲,就是这种欺骗的一个例子。敌军跟踪雷达接收到这些脉冲以后,就会把错误的目标信息输入其系统。

该类欺骗的其他例子包括红外特征伪装欺骗和使用反射器、应答器或转发器再辐射的雷达欺骗,以及通过烟雾剂等伪装电磁频谱光区的光学欺骗。这些技术可以单独使用,也可以组合使用。一般情况下由电子战欺骗计划决定使用何种电磁手段来误导敌军,为己方创造优势。

4. 扰乱

扰乱就是削弱或干扰敌军指挥控制,从而限制敌军战斗能力。扰乱可以通过电子干扰、电子欺骗、电子入侵和摧毁来实现。这些手段将增强对敌军的攻击能力,发挥兵力增强器的作用。

5. 摧毁

摧毁在电子战领域里是指消除敌军一些或所有电子防御能力。摧毁是最为有效的对抗措施。目标跟踪雷达和指挥控制设施都是引人注目的目标,因为摧毁目标跟踪雷达和指挥控制设施可严重地阻止敌军的战斗效能。摧毁需要确定目标的准确位置,可以通过有效应用电子战支援措施来实现。机载接收机和测向设备可以确定目标的位置。敌军电磁系统可以通过各种武器和技术进行摧毁,包括从常规弹药的炸弹到强辐射和高能粒子束等。对敌军电磁设备的摧毁也许是阻止敌军使用电磁频谱最为有效的手段。压制的长度将取决于敌军维修和替换战斗资源的能力。电子战摧毁的一个例子就是采用高速反辐射导弹对付敌军雷达。

1.2.5 其他因素

1. 电子战中的定向能

定向能是产生集中的电磁能、原子或亚原子粒子束相关的技术总称。定向能战(DEW)是指利用定向能武器、装置或对抗措施直接损伤或摧毁敌军装备、设施和人员,或通过损伤、扰乱及摧毁来确定、利用、削弱或阻止敌军使用电磁频谱的军事行动。定向能战还包括为保护己方装备、设施和人员及己方使用电磁频谱而采取的行动。定向能的应用包括激光、射频和粒子束。定向能可用于实施电子攻击、电子战支援或电子防御。例如,设计用来致盲或扰乱光学传感器的激光属电子攻击;设计用于探测和分析激光信号的告警接收机属电子战支援;设计用于对激光有害波长进行过滤的装置则为电子防御。

2. 敌军能力

指挥官必须了解己方的电子战能力和潜在敌军的电子战能力。任务计划的制订依赖于准确的信息。新技术武器系统的数量每年都在增加。潜在敌军认识到美国对电子化的通信和武器系统有极大的依赖性。为利用这一点,一些潜在敌军在组织上做好了攻击美军关键武器系统控制功能和相关通信节点的准备。许多国家已通过各种途径购买了能力强大的现

代武器系统,而恐怖分子也许获得了非常危险的高端武器。为了应对这种情况,指挥官及参谋人员应当熟悉所有潜在敌人这类武器的部署和电子战能力。

3. 作战要求

电子战参与的等级总是取决于任务的具体要求,应根据任务进行调整。作战目标、战术态势、作战系统的效能和可用性以及当前国内和国际政治气候,都决定着军事资源的合理运用。制订电子战计划并不是简单地某项任务自动增加干扰吊舱或护卫设备。为了达到预期目标,每项任务都可能对电子战提出特殊要求。指挥官及参谋人员必须将威胁和可用于支持电子战的资源都考虑进去。

4. 情报、监视与侦察

军事行动成功的关键在于军事指挥官通过对近实时信息与某一阶段收集的长期作战、科学和技术情报信息的汇总,透彻了解敌军的能力。必须了解敌军规划内的军事能力以避免措手不及。了解己方能力对有效地制订计划同样非常重要。判定敌军意图需要准确的情报,这种情报必须及时传递给用户。众多监视和侦察系统正在为各种电子数据库收集数据,这是有效运用电子战所必需的。人工介入管理监督的先进处理与运用系统可将数据转换成可用情报,而能经得住核袭击的通信栅格会把情报传给用户。电子战与所有军事行动一样,对情报要求的规定和管理至关重要。

5. 环境条件

自然环境也影响着电磁频谱的使用,并且在整个频谱上都会受到影响。云、湿度和灰尘可以降低工作在红外和光学波段内的各种系统的性能,大气条件可以使雷达信号畸变,导致跟踪误差,加大探测距离或在雷达覆盖范围内形成“无信号区”。大雨也会影响微波的传输。甚至太阳和大气层外的扰动都会在雷达和卫星链路中产生射频干扰。使用环境条件预测的计划人员可以利用或减轻这些影响,以形成己方对敌方的优势。

电子战可通过有效运用探测、阻止、欺骗、扰乱、摧毁和及时提供情报,并通过在关键时刻扰乱敌军使用电磁频谱增强己方的作战能力,同时确保己方对电磁频谱的持续使用。各种电子战技术的协同运用能够严重扰乱敌军的一体化防空系统、武器系统和指挥控制系统。干扰、箔条和诱饵能削弱敌军发现、确定、跟踪、瞄准和交战的能力,而幸存下来的雷达制导武器系统将在电子战环境下丧失部分效能。总之,合理运用电子战可以大大提高成功率。系统限制敌军获取己方兵力调动和部署的信息,引起敌军混乱。对敌指挥控制系统进行干扰可以削弱敌军的决策和部署过程。敌军集中控制与使用其兵力则为电子攻击提供了机会。

对敌防空压制(SEAD)是指利用摧毁性或扰乱性手段压制、摧毁或暂时降低敌军地基防空能力的活动。对敌防空压制作战行动的目的是为了使己方战术部队有效地执行其任务而为其提供一个不受敌防空系统电磁影响的环境。在联合出版物条令中,对敌防空压制并不属电子战中的一部分,它是一个涵盖面更宽泛,甚至包含电子战运用的术语。在空军条令中,对敌防空压制是反航空兵作战任务的一部分,并直接有利于夺取空中优势。对敌防空压制可包括使用电磁辐射来压制、削弱、扰乱、延缓或摧毁敌军一体化防空系统(IADS)中使用电磁频谱的那些部分。在敌对期间,敌军防空系统很可能对己方的空中作战行动构成挑战。这时就需要使用对敌防空压制武器系统对敌军的机载和地基辐射源进行定位、削弱、压制或摧毁。对敌防空压制的目标一般包括预警、地面控制截获、捕获、地空导弹和高炮威胁雷达。通过运用对敌防空压制作战行动可以加强空军的功能。

1.3 电子战信号环境

1.3.1 电子战的领域与扩大

电子战是一个技术分支很多、范围很广的技术领域。

从电子战的对象来分,有通信战、雷达战、导航战、制导战、计算机战、对敌我识别系统的对抗、对无线电引信的干扰以及对 C^2 系统的对抗等等。信息化战争概念出现之后,将导航战、制导战(导弹战)与计算机战归纳到信息化战中。 C^2 系统是20世纪90年代发展起来的指挥与控制结合在一起的新系统(C^2 ,指挥、控制二词英文缩写词头)。

从频域上分,有射频战、光学战和声学战三个领域,而且在每个领域上,电子战的范围都在扩展。

(1) 射频战 射频是通信、导航、雷达和制导等设备工作的主要频段,如图1.2所示。其中雷达工作频段跨米波、分米波、厘米波和毫米波四个波段。雷达工作的频段也是雷达战的频段。

(2) 光电战 包括红外战、电视战和激光战等分支,主要用以对付红外探测、夜视设备和激光雷达,以及用红外、电视、激光制导的武器系统。

光波也是电磁波,从图1.2可知,光电战实质上是射频对抗向更高的电磁频段的发展。光电战是近年来发展最快的电子战领域。

(3) 声学战 或称水声战,它是指海下的电子战。在辽阔的海洋里,潜艇、舰船或新型鱼雷主要靠声学探测设备来发现目标和跟踪目标。水声战则是专门用来对声学探测设备(声呐)进行侦察和干扰的措施。声学战还包括对潜艇、舰船航行时所发出噪声的侦听和跟踪,以及对其航迹的探测。水声战是现代海军极其重要的电子战领域。

(4) 新概念武器的对抗 新概念武器包括远定向能高速动能武器、高超声速武器、计算机病毒、基因等武器。定向能中的高能激光与高能电磁波武器、计算机病毒已用于战场,并取得了良好的效果,新概念武器是现代高技术战争与未来的信息化战争的主要武器之一,是发展方向。

(5) 太空电子战 太空将是电子战的主要战场,是电子战制高点。

(6) 导航电子战 导航对抗属于太空电子战范畴,它以卫星导航战为主要内容。

从空间范围来看,电子战不仅在地面、海上、空中、水下经常性地大规模进行,而且随着卫星、反卫星、洲际导弹和反导弹的斗争,促使了空间电子战的迅速发展,发展成为太空电子战,太空是将来的主要战场。

目前,卫星已经广泛地担负着战略通信、精确导航和侦察任务,不仅是重要的军事情报来源,而且是今后战争中战略通信指挥和武器控制的重要手段。用卫星作为进攻性武器,如卫星轰炸系统等也在加紧研究。在反卫星的斗争中,电子对抗措施可以发挥重要的作用,如干扰卫星的发射,干扰其遥控遥测系统,使其失控、变轨、自爆,干扰卫星上的信息系统使之饱和或破坏其正常工作程序等。

对战略导弹突防过程中电子对抗技术的研究业已达到成熟阶段。例如减小载人体的雷达有效反射面积和改变其目标反射特性的研究,假目标、雷达诱饵及消极干扰丝投放技术的研究,以及在外层空间利用投掷式干扰机以掩护真弹头的技术研究等。

1.3.2 电子战的信号环境

电子战的频率范围非常广,从超低频 3 kHz 一直到紫外线,如图 1.2 所示。

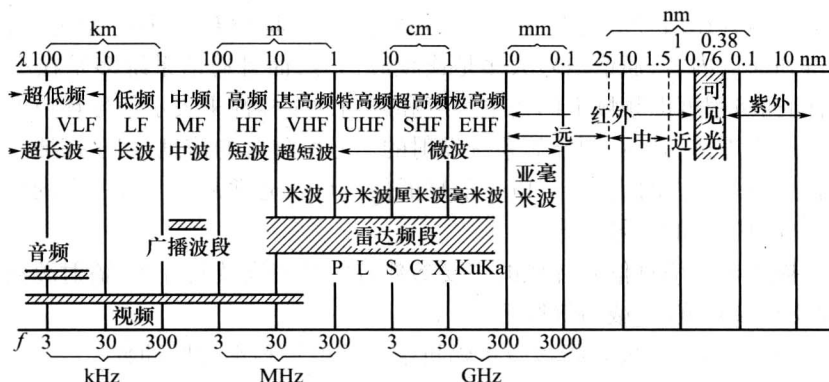


图 1.2 电磁波频谱图

1.3.3 现代电子战环境的特点

电子战的信号环境与雷达的信号环境不同。雷达的信号环境包括目标、环境回波和人为的有源及无源干扰所产生的信号。雷达是窄波束窄频带工作,它所收到的信号除目标回波外还有环境杂波(如地物杂波、海浪杂波等)、人为干扰以及同频率的雷达信号。雷达是在这些干扰背景下提取目标回波信号的。电子战的信号环境是由各种辐射源所形成的。电子战设备通常是在宽频带和宽空域工作,要随时截获各个辐射源的信号并进行分析和识别,进而判断所受到的威胁。所以,电子战信号环境随着辐射源数量日益增多而日趋复杂。

现代电子战信号环境与过去(20 世纪 50 年代及其以前)的电子战信号环境不同。那时,辐射源数量不多,工作频率不变或慢变,工作时间长而且信号波形及参数不变,雷达和通信、导航各在不同频段上工作,信号形式也有明显差异。这样,电子战接收机可以采用窄的波束、窄的频带进行宽范围的搜索,从而对各辐射源的信号进行分别的处理。

现代电子战信号环境的特点是:(1)辐射源的数量日益增多,飞机或军舰上的电子战设备可能受到数十甚至上百个辐射源的照射,因而信号密度大(可达百万脉冲数/秒);(2)辐射源的体制多变,波形复杂多变;(3)辐射源的工作频段在不断增宽,而且不同辐射源(如通信、导航、雷达、制导系统)的工作频段在越来越宽的范围上重叠;(4)基于以上原因,信号源在频域上拥挤,在时域上密集而且交叠在一起;(5)制导武器的大量使用,使得电子对抗信号环境里潜在的威胁,在数量上和严重性上日益增大,要求电子战系统必须快速、不间断、高可靠地进行信号处理,特别要实时地确定并测知威胁信号。

概括地说,现代电子战信号环境的特点是密集的、复杂的、交错的和多变的。面对这样的信号环境,电子战系统要对每个信号实现 100% 概率的截获,并将每个辐射源的信号分选出来进行分析和识别,的确是十分复杂而艰巨的任务。

1.3.4 电子战信号环境的定量描述和参数范围

设计电子战系统时,其性能指标需要根据现代电子战信号环境来确定;评价一部现有的侦察干扰设备的性能,能否适应今后电子战信号环境,都需要对信号环境作定量的描述,以