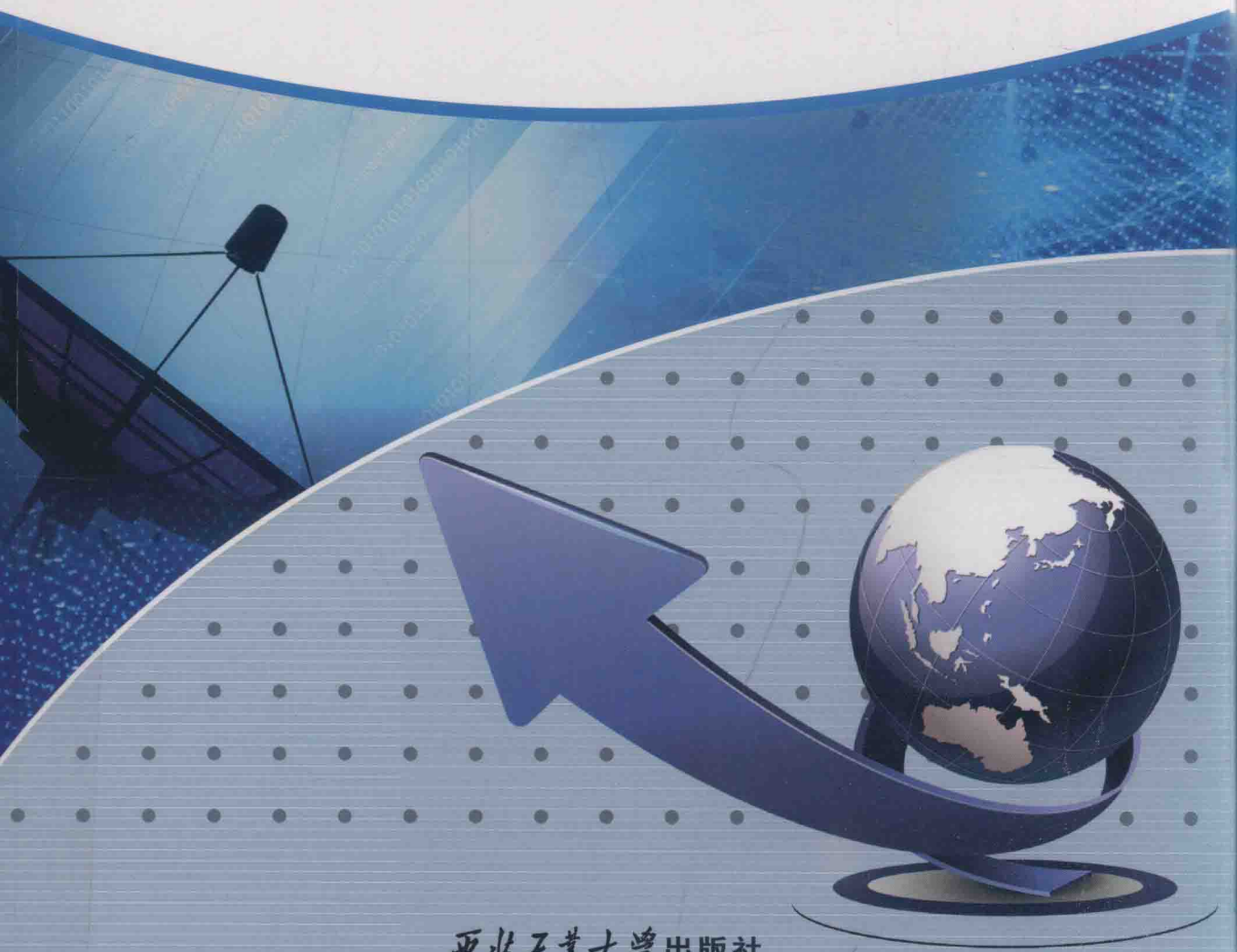


高等学校“十三五”规划教材·电子信息类专业教材

雷达电子对抗

张永顺 童宁宁 龙戈农 郭艺夺 编著



西北工业大学出版社

雷达电子对抗

张永顺 童宁宁 龙戈农 郭艺夺 编著

西北工业大学出版社

西安

【内容简介】 雷达电子对抗(亦称雷达电子战)作为指挥控制战和信息战的关键要素和手段,在现代信息化战争中具有重要的作用和地位。随着电子技术的发展,雷达电子对抗的内容和作战方式发生了重大的变化,出现了隐身技术、反辐射导弹、低空突防等新的技术和新的作战方式。本书从攻防对抗的角度介绍雷达相关的电子对抗技术和战术,主要包括电子战基本概念、雷达侦察与反侦察、雷达干扰与抗干扰、雷达隐身与反隐身、对雷达的硬杀伤攻击与防护以及对雷达的低空突防与反突防等。

本书涉及雷达电子对抗的多个方面,内容较全面,既有经典的基本理论和技术,又有最新发展的雷达电子对抗领域的先进技术,可供高等学校雷达、电子对抗工程等任职教育及专科相关专业作为教材使用,也可供雷达电子对抗领域的科技人员参考使用。

图书在版编目(CIP)数据

雷达电子对抗/张永顺等编著. —西安:西北工业大学出版社,2019.4

ISBN 978-7-5612-6471-3

I. ①雷… II. ①张… III. ①雷达电子对抗 IV. ①TN974

中国版本图书馆 CIP 数据核字(2019)第 061767 号

LEIDA DIANZI DUIKANG

雷 达 电 子 对 抗

责任编辑:何格夫

责任校对:孙倩

出版发行:西北工业大学出版社

通信地址:西安市友谊西路127号

电 话:(029)88491757, 88493844

网 址:www.nwpu.com

印 刷 者:兴平市博闻印务有限公司

开 本:787 mm×1 092 mm

印 张:15.875

字 数:417千字

版 次:2019年4月第1版

定 价:49.80元

策划编辑:杨军

装帧设计:李飞

邮编:710072

1/16

2019年4月第1次印刷

如有印装问题请与出版社联系调换

前 言

在现代高技术战争中,雷达已成为必不可少的军事装备,是远程预警、制导武器的核心,针对雷达展开的电子战已成为现代信息化战争的重要内容。电子战作为指挥控制战和信息战的关键要素和手段,已渗透到信息作战的各个方面,成为掌握信息控制权、赢得战场主动权和获取战争制胜权的关键,已经成为继陆、海、空、天战之后的第五维战场。自从第二次世界大战以来,围绕雷达、通信系统展开的电子战成为了现代战争的序幕与先导,并贯穿于战争的全过程,能够决定战争的进程和结局。

随着军事电子技术的发展,新技术和新装备不断涌现,性能水平不断提高,促使电子战的作战领域和作战方式发生了重大的变化。电子战已经从防御性、掩护性的行动发展为既有防御又有进攻的电子作战行动,从只有软杀伤手段发展到既有软杀伤手段又有硬杀伤手段,从单个系统的对抗发展到系统对抗和体系对抗,电子战已成为决定战争胜负的重要因素。从发展角度来看,世界各国对电子战更新换代十分重视,F-117 隐身飞机退役后,F-22 和 F-35 闪亮登场;EA-6B 电子战飞机逐步退役的同时,EA-18G 电子战飞机成为新的威胁;AGM-88 哈姆反辐射导弹成为主力后,又发展了新型 AGM-88E 反辐射导弹;等等。近期美国在军事转型中提出了网络中心电子战和联合电子战,作为一种信息化武器,电子战成为作战武器组合中密不可分的一部分。

电子战是指使用电磁能或定向能控制电磁频谱或攻击敌军的任何行动。从技术上来看,电子战可以分为三个主要组成部分:电子攻击(EA)、电子防护(EP)和电子战支援(ES)。从敌我对抗双方来看,虽然都有电子战的三个部分,但处于相互对抗的两个方面,当敌方对我方实施电子攻击如电子干扰时,我方就要实施电子防护即电子反干扰;当我方对敌方实施电子攻击如电子干扰时,敌方就要实施电子防护即电子反干扰;当敌方对我方实施电子支援如电子侦察时,我方就要实施电子防护即电子反侦察;当我方对敌方实施电子支援如电子侦察时,敌方就要实施电子防护即电子反侦察;等等。对抗是军事科学的一种形式,其目的是阻遏敌军实际或预期的电磁频谱优势,同时确保己方无阻碍地获取信息环境的电磁频谱资源。从雷达攻防对抗主要矛盾的角度来看,雷达电子战是由敌我双方矛盾对立面组成的,主要包括雷达侦察与反侦察的对抗、雷达干扰与反干扰的对抗、雷达隐身与反隐身的对抗、反辐射导弹攻击与抗反辐射导弹的对抗、雷达低空突防与反低空突防的对抗等等。

本书从雷达电子战的主要矛盾展开讨论,主要包括 7 章内容。第 1 章绪论,主要介绍电子战的基本概念、电子战作战模式新发展、雷达对抗中的主要矛盾、电子对抗实例;第 2 章雷达侦察与反侦察,主要介绍侦察的基本内容与特点、侦察作用距离、对雷达信号频率的侦察基本技术、对雷达方向侦察的测量技术、对雷达定位的基本方法、雷达侦察信号处理基本过程、雷达低截获概念、雷达反侦察技术和战术等;第 3 章雷达干扰,主要介绍雷达干扰分类、干扰方程、有效干扰空间、对雷达有源干扰和无源干扰主要技术;第 4 章雷达抗干扰,主要介绍天线域抗干扰技术、能量域抗干扰技术、频率域抗干扰技术、速度域抗干扰技术、时间域抗干扰技术和战术抗干扰措施等;第 5 章对雷达的隐身与反隐身,主要介绍雷达隐身技术、隐身技术实例和雷达

反隐身的主要途径与技术;第6章对雷达的硬杀伤攻击与防护,主要介绍反辐射导弹的技术与发展、雷达对抗反辐射导弹的技术和原理、定向能武器、对定向能武器的防护等;第7章对雷达的低空突防与反突防,主要介绍低空突防的概念和技术、低空突防对雷达系统的影响、雷达反低空突防的技术和战术等。

本书主要是为高等学校雷达、电子对抗工程等相关专业的任职教育或专科教育而编写的,基本涵盖了雷达电子对抗的主要领域,内容较全面,突出了对抗性和实用性。本书由冯存前教授审阅,在此表示衷心的感谢;同时,对本书所参考资料的作者表示衷心的感谢!

由于雷达电子战涉及多个学科领域,其技术发展日新月异,许多新理论、新技术正在研究和发

编著者

2018年9月

目 录

第 1 章 绪论	1
1.1 电子战定义与分类	1
1.2 信息战、指挥控制战与电子战关系.....	4
1.3 电子战作战模式新发展	7
1.4 雷达对抗中的主要矛盾.....	11
1.5 电子对抗实例简介.....	13
第 2 章 雷达侦察与反侦察	18
2.1 概述.....	18
2.2 侦察作用距离.....	24
2.3 雷达信号频率的测量.....	32
2.4 雷达方向的测量技术.....	45
2.5 雷达定位方法和原理.....	57
2.6 雷达侦察中的信号处理.....	61
2.7 雷达反侦察.....	66
第 3 章 雷达干扰	70
3.1 概述.....	70
3.2 干扰方程及有效干扰空间.....	72
3.3 有源干扰.....	80
3.4 无源干扰	115
第 4 章 雷达抗干扰	128
4.1 概述	128
4.2 天线域抗干扰技术	129
4.3 能量域抗干扰技术	137
4.4 频率域抗干扰技术	152
4.5 速度域抗干扰技术	161
4.6 时间域抗干扰技术	174
4.7 战术抗干扰措施	179

第 5 章 对雷达的隐身与反隐身	181
5.1 概述	181
5.2 雷达隐身原理	184
5.3 雷达反隐身技术	193
第 6 章 对雷达的硬杀伤攻击与防护	202
6.1 概述	202
6.2 反辐射导弹	202
6.3 雷达对抗反辐射导弹技术	211
6.4 定向能武器	221
6.5 雷达对定向能武器的防护技术	226
第 7 章 对雷达的低空突防与反突防	230
7.1 概述	230
7.2 低空/超低空突防技术原理.....	235
7.3 雷达反低空突防探测技术	237
7.4 雷达反低空突防战术	243
参考文献	246

第 1 章 绪 论

雷达是发射无线电波、利用目标对电波的反射特性、接收回波信号并进行信号处理来发现目标并测定目标距离、角度、速度等信息的电子装备。由于雷达具有探测距离远、测定目标坐标速度快、定位精度高、不受天气影响等特点,在军事上具有非常重要的应用价值,被广泛用于侦察、警戒、引导、武器控制、航行保障、气象观测和敌我识别等方面。不论是在今天的陆战、空战、海战还是在未来的太空战争中,雷达都是不可缺少的信息化兵器。如何观察战场、如何传递信息、如何利用精制导武器打击目标将成为信息化战争的重点。

战略和战术武器普遍应用无线电探测、控制、通信等电子技术,必然推动电子战技术的迅猛发展。未来战争是信息主导的现代化战争,电磁环境变得越来越复杂,夺取电磁频谱的控制权与使用权变得越来越重要。迄今,电子战已经成为现代战争必不可少的重要组成部分,成为夺取“制信息权”的关键。从本质上看,电子战是敌对双方在电磁频谱领域中广泛进行的一种对抗性军事行动。现代战争中,电磁频谱的应用深入到整个战争的各个领域,频谱从声波开始一直延伸到无线电波、红外、可见光波,直到紫外和更短波长的全部频段;作战范围从海、陆、空直到太空的广大空域,应用于军兵种武器的各种作战平台。

雷达对抗是发展最早、技术更新最快、对抗频段分布最宽、综合技术发展最受重视的一个电子战专业领域,对整个作战胜负具有重要的影响。历次局部战争表明,在电磁频谱的对抗中,敌对双方综合电子对抗实力特别是雷达电子战的实力已成为影响战争全局的关键因素之一。在现代高科技战争中,处于电子战弱势的一方,将失去制电磁谱权,失去制电磁谱权即意味着失去整个战争的指挥权,丧失制空权和制海权。在这种情况下,性能再先进的兵器也难以发挥作用,难以在整体上组织起有效的军事行动,将处于被动挨打的地位。因此,深入研究雷达电子对抗理论,掌握电子对抗知识,正确运用电子对抗技术和战术,对于取得未来战场上的胜利具有重要的意义。

本章主要介绍电子战的一些基本概念、信息战及指挥控制战与电子战关系、电子战作战模式新发展、雷达对抗中的主要矛盾、电子对抗实例等。

1.1 电子战定义与分类

1.1.1 电子战定义

由于电子战技术不断地发展,电子战概念有一个不断演变和发展的过程。

1. 美军的定义

1969年美军政策备忘录中对电子战是这样定义的:使用电磁能量去测定、利用、削弱或阻止敌方使用电磁频谱,并保护己方使用电磁频谱,包括电子对抗措施(ECM)、反电子对抗措施(ECCM)和电子支援措施(ESM)。

1990年美军政策备忘录中对电子战是这样定义的:使用电磁能量去测定、利用、削弱或以破坏、摧毁、扰乱手段阻止敌方运用电磁频谱,同时保证己方运用电磁频谱的军事行动,也包括电子对抗措施、反电子对抗措施和电子支援措施。上述两种传统电子战定义在实践中都有一定的局限性。1993年美军总参谋部修订了政策备忘录中传统的电子战定义。

新定义电子战(Electronic Warfare, EW)是指任何包括使用电磁能和定向能武器来控制电磁频谱或攻击敌方的军事行动,它包括三个方面:电子攻击(Electronic Attack, EA)、电子防护(Electronic Protection, EP)和电子支援(Electronic warfare Support, ES, 即电子战支援),如图 1.1.1 所示。

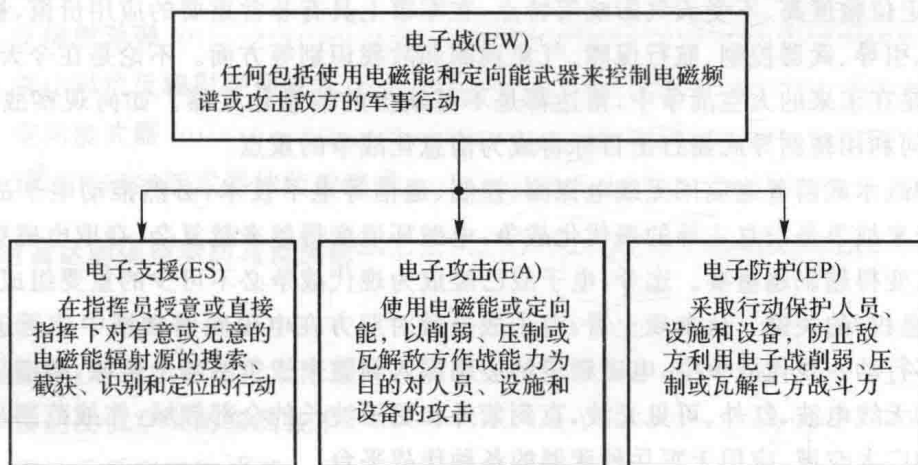


图 1.1.1 电子战定义

美军电子战的新定义是在原来的电子战定义的基础上发展而来的。显然,该定义增强了电子攻击能力,即使用激光、微波辐射、粒子束等定向能武器、反辐射导弹和电磁脉冲来摧毁敌方的电子设备。此外,扩大了电子防护的使用范围,电子防护不仅包括保护单个电子设备(ECCM),而且还包含采用如电磁控制、电磁加固、电子战频谱管理和通信保密等措施。因此,所有使用电磁波的设备(如雷达、通信、C³I系统、导航、敌我识别、精确制导、无线电引信、计算机和光电武器等)都是电子战的作战对象。

电子战的一般组成如图 1.1.2 所示。

(1)电子攻击是使用电磁能或定向能,以削弱、压制或瓦解敌方作战能力为目的对人员、设施和设备的攻击,主要包括电子干扰、反辐射攻击、定向能攻击、电子欺骗和隐身等。电子攻击是电子战的一个组成部分,因而被认为是一种新的“火力形式”。

(2)电子防护是保护人员、设施和设备,防止敌方利用电子战削弱、压制或瓦解己方战斗力的任何行动,主要包括电子抗干扰、电磁加固、频率协调、信号保密、反隐身及其他电子防护技术和方法等。

(3)电子支援是在指挥员授意或直接指挥下,对有意或无意的电磁能辐射源的搜索、截获、识别和定位的行动,主要包括信号情报、战斗告警和战斗测向等。

2. 俄罗斯的定义

俄罗斯将电子战称作“无线电电子战斗”,定义为用于探测、侦察和随后进行的无线电压制、摧毁敌人的指挥控制系统和武器系统的一类综合方法,以及对己方部队无线电电子资源及

系统的保护。俄罗斯电子战的内涵主要是干扰破坏敌电子设备之间的无线电通信、反干扰以及对干扰和反干扰行动的保障(主要指建立必要的兵力和兵器、阵地区域电子设备和电子战的信息保障以及隐蔽己方电子设备的重点信息等内容),其本质就是瘫痪敌指挥、控制和通信系统。



图 1.1.2 电子战的一般组成

3. 我国的定义

电子对抗亦称电子战,指使用电磁能、定向能和声能等技术手段控制电磁频谱,削弱、破坏敌方电子信息设备、系统、网络及相关武器系统或人员的作战效能,同时保护己方电子信息设备、系统、网络及相关武器系统或人员作战效能正常发挥的作战行动(包括电子对抗侦察、电子进攻和电子防御)。电子战分为雷达对抗、通信对抗、光电对抗、无线电导航对抗、水声对抗以及反辐射攻击等,是信息作战的主要形式。

1.1.2 电子战的分类

电子战包含了使用电磁频谱进行对抗的各个领域,内容十分丰富,有多种分类方法。按照具体的无线电电子设备或器材来分,电子战可分为雷达电子战、通信电子战、光电电子战、引信电子战、敌我识别系统电子战、C³I(通信、指挥、控制和情报)系统电子战、声呐电子战等。按照空间来分,电子战可分为空中电子战、太空电子战、陆地电子战、海上电子战、水下电子战等。

从频域上可以将电子战划分为三大类:射频电子战、光电电子战和声学电子战。图 1.1.3 给出了频段的划分图。

1. 射频电子战

射频电子战包括雷达、通信、导航、敌我识别、无线电引信和制导等领域的电子战,其设备工作频率范围为 3 MHz~300 GHz。

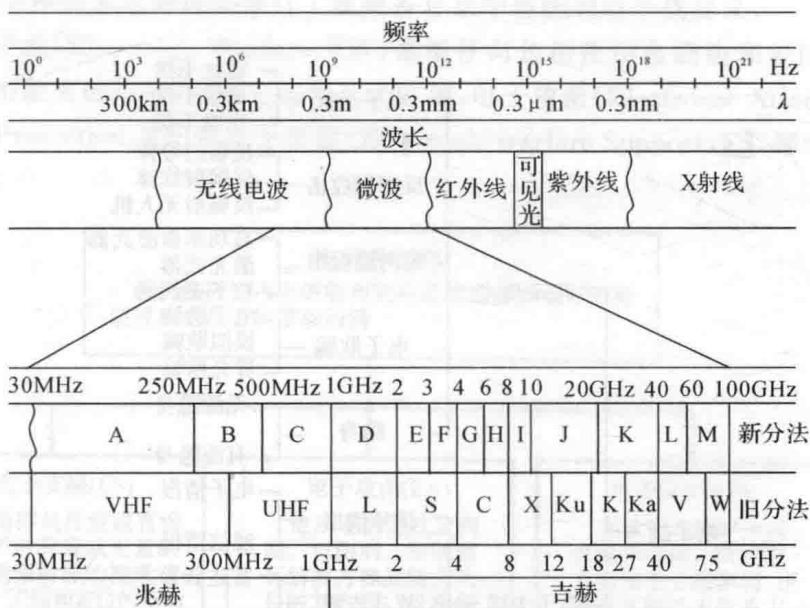


图 1.1.3 电磁频谱的划分

2. 光电电子战

光学波段可分为红外线、可见光和紫外线等子频段,是近距离精确制导武器和定向能武器工作的主要频段。

光电电子战是指作战双方在光学波段(频率范围在 300 GHz 以上)运用光学设备、器材和其他设施所进行的电磁斗争。其最显著的特点是,所使用的光电设备和光电武器的精度高、分辨力好且抗电磁干扰的能力强。

光电电子战可分为光电侦察和反侦察、光电干扰和反干扰、光电制导和反制导、光电摧毁和反摧毁等。

3. 声学电子战

声学电子战主要用于水下信息的对抗。其频段从次声波至超声波,是声呐、水下导航定位设备工作的主要频段。

1.2 信息战、指挥控制战与电子战关系

1.2.1 信息战与指挥控制战的关系

信息战亦称信息作战,是指综合运用电子战、网络战、心理战等形式打击或抗击敌方的行动。目的是在网络电磁空间干扰、破坏敌方的信息和信息系统,影响、削弱敌方信息获取、传输、处理、利用和决策能力,保证己方信息系统稳定运行、信息安全和正确决策。信息战主要包括信息作战侦察、信息进攻和信息防御。信息战按其性质可分为广义信息战和狭义信息战。

(1) 广义信息战是指敌对双方在政治、经济、科技和军事等各个领域,运用信息技术手段,为争夺信息优势而进行的对抗。内容包括:为了维护国家的安全利益,对于信息技术及其产品和系统所进行的研究、生产、装备、使用活动,以及对于敌对国家上述活动所进行的侦察、干扰、破坏等行动。它是在平时、危机时期或战时打击对方的社会、经济、政治、工业或军事电子信息系统所采取的秘密或公开的、有控制性、破坏性或毁灭性的行动。其目的是通过取得信息优势来影响对方行为,阻止或避免冲突的发生,或以最小的财力、物力和人员伤亡的代价,迅速彻底地赢得战争。

(2) 狭义信息战特指战场信息战,即军事领域的信息战,它主要发生在指挥控制、情报和信息系统等部分,是为获取军事行动范围内的信息优势而进行的斗争。内容包括:使用信息技术手段进行的探测、侦察、引导、指挥、控制、通信、信息处理、伪装欺骗和打击等作战行动,以及针对敌方上述活动所进行的侦察、干扰、破坏和反利用等作战行动。

反映在作战空间上,信息战是在陆、海、空、天、信息多维空间进行的作战行动,既是一种相对独立的作战形式,又渗透到多种作战形式之中;反映在行动性质上,它是以电子战、网络战为主的争夺制信息权的作战行动,既受联合战役的支配和约束,又对联合战役的胜败产生重大影响。

信息战的作战对象可概括为信息、信息系统、以信息为基础的处理过程、以计算机为基础的网络和决策人员等。信息战要达到的首要目标是压制、削弱、破坏和摧毁敌方的指挥、控制、通信、计算机与情报系统。

信息战作为一种崭新的战争形态,使得现代作战手段进一步增多,使作战速度更快。其主要特点:持久性——信息战贯穿于战争的全过程(包括战前和战后);多维性——不仅在同一时空坐标内与陆战、空战、海战相互渗透、融合,而且能综合运用政治、经济、技术和军事信息在五维战场进行特殊战争;透明性——各参战部队对战况都了如指掌,从散兵到最高指挥部,所有用户都可以通过无缝隙、多媒体通信联络和网络共享信息;一体性——各军兵种、各类作战系统、作战职能系统、武器平台和各作战单元连成一个有机的整体,信息的收集、管理、传递和拒绝也由信息系统连在一起;实时性——各级之间接近实时地分发情报信息,作战进程与决策时间几乎同步;精确性——目标发现就意味着打击,打击目标就意味着摧毁。

因此,在信息时代进行信息作战,首先要对敌方各级部队的决策机构进行信息攻击,通过切断或破坏敌人所有的信息媒介,使敌方指挥机关与部队脱节,从而使敌方部队失去活动方向和活动能力。同时,确保己方进行不间断的、严密的和多频谱的监视与侦察,完整地接收己方部队从远距离发来的传感数据,使信息的准确性与武器的精度相适应,并快速、全面、准确地进行战斗评估。其次,确保己方决策周期比敌人的更短、运行更快,信息提供者应保持高度的战备状态,确保能随时提供所需信息。

从目前的发展情况来看,信息战的作战样式主要分为指挥控制战(C^2W)、民间事务战、公共事务战和网络空间战等,其核心是指挥控制战,而指挥控制战的重要内容之一是电子战。

1.2.2 电子战与指挥控制战的关系

指挥控制战(C^2W)的定义为通过情报的相互支持与综合运用作战保密、军事欺骗、心理战、电子战和实体摧毁等手段,达到影响、削弱或破坏敌军的指挥控制能力,同时保护友军的指挥控制系统免受敌方此类攻击的行动。 C^2W 适用于任何作战行动及所有不同级别的军事冲突。

C²W 适用于作战的各个阶段,不仅在敌对状态期间可以运用,而且在敌对状态之前和敌对状态之后都可以运用。即使在一般性作战行动而非战争的情况下,C²W 也可以为军事指挥官提供致命性和非致命性杀伤手段,以完成上级部门交给的作战任务,达到遏制战争促进和平的目的。C²W 可延缓敌军的作战速度,扰乱其作战计划的制定,削弱其战斗力集中的能力,影响其对作战局势的估计。此外,C²W 能够将友军指挥控制系统的易毁性及各部队之间互相制约、相互牵制的程度降到最低。

指挥控制战的基础设施是完善的指挥、控制、通信和计算机(C⁴)信息系统,并与各级作战相关信息和情报支持系统结合在一起。指挥控制战的基本组成部分是作战保密、军事欺骗、心理作战、电子战和实体摧毁。电子战和实体摧毁是指挥控制战的关键和核心。

1. 作战保密

作战保密(OPSEC)定义为通过控制和保护与军事作战计划和军事行动有关的信息而使敌方无法获得己方能力和意图的过程。OPSEC 并非一个独立的过程,必须同精心制定的欺骗计划相结合。一个好的 OPSEC C²攻击计划将使敌方的情报系统收集不到情报,降低敌方指挥官有效控制部队的能力。OPSEC C²防卫的目的是用欺骗的手段将假信息反馈给敌方,而将己方的指挥和控制信息隐藏起来。

目前,作战保密计划和措施的制定,受到新兴的全球商业部门的严峻挑战。其中,诸如摄像、定位和网络系统等新技术和手段,可以使敌方对友军信息情报的获取达到新的水平。而且,在作战行动期间,不可避免出现的媒体新闻使得作战保密问题更趋复杂化。新闻媒体向全球听众传播实时信息的能力,可以成为敌军十分有利的信息来源。随着军队数字化程度的飞速发展和广泛应用,信息安全的重要性也日益增长。

2. 军事欺骗

军事欺骗是指对己方作战能力、作战意图及作战活动等方面的信息进行误导和示假,从而有意误导敌方军事决策人员做出错误判断,最终引起敌军采取有利于己方完成任务的错误军事行动。军事欺骗是影响敌军指挥官决策的基本手段,其一般方法是对己方的作战意图、位置、部署、作战能力、活动过程和作战力量进行误导、隐蔽和伪装等,使敌方做出与真实情况相反的判断。欺骗的目的是引诱敌指挥官按着有利于己方军事行动的方案行动,也就是人们常说的“牵着敌人的鼻子走”。

3. 心理作战

心理作战是一种将信息和指令传递给敌方的政府、组织及个人,以影响其情绪、意志、动机和客观的推理,直至最终影响其行为的作战形式。心理作战是以具体、事实和可信的信息为基础的。

美军的心理作战能够将分散的信息扩散到敌方的 C⁴I 收集系统之中,显示其强大的联合作战力量和先进的技术优势,从心理上给敌方以巨大的震撼,从精神、情感、意志上征服敌方。心理作战因素必须与其他指挥控制战要素、公共事务战略紧密结合、密切协同,以最大限度地发挥信息战争的优势。

心理作战在指挥控制防御战中的主要目的是将敌方在对抗己方力量方面的宣传和假情报的影响降到最小。

4. 电子战

在指挥控制战的框架之内,电子攻击主要支持 C²W 攻击,电子防护主要支持 C²W 防护,

而电子支援既向情报系统提供信息又支持电子攻击和电子防护。为支持电子攻击、电子防护、规避、目标瞄准和其他战术部署有关的快速决策,用电子支援来搜索、截获和定位电磁辐射源,以便准实时地识别威胁。电子支援数据还用来生成信号情报,经处理后,成为情报数据库的一部分。这些更新的情报可用于规划 C² 系统攻击行动和提供战场损伤评估,并反馈整个 C² W 计划的效能。

无论是干扰、电磁欺骗还是采用定向能武器或反辐射导弹摧毁 C² 系统的节点,电子攻击在作战环境中对几乎所有的 C² 系统攻击行动都具有重要作用。它还可用于保护己方 C² 系统免受敌方的攻击。电子防护在 C² 系统防卫中用来保护己方部队的信息安全,不被敌方电子支援行动所利用,是保障在 C² 系统攻击行动中己方部队顺利、不间断地应用电磁频谱的最好手段。

5. 实体摧毁

在 C² W 中,一项重要策略就是中断敌方 C² 系统的关键节点。摧毁只是能完成这一使命的一种方法。而且,摧毁行动仅仅在特定的时间范围内起作用,所以实施时间很重要。通常,只要有足够的时间和备份资源,敌方就可以从摧毁状态恢复过来。从军事观点来看,若要使敌方 C² 系统功能瘫痪,非常有必要采用实体摧毁。

针对 C² W 的指挥功能,摧毁的目标是指挥中心。针对 C² W 的控制功能,攻击的重点则是 C² 系统的通信、计算机或传感器网的关键节点。对辐射信号目标进行攻击时,常采用的方法是监视攻击前后信号的辐射情况。如果一个节点在被攻击前有辐射信号而在被攻击后即停止了辐射,那么可以假设摧毁行动至少取得了暂时的成功。摧毁过程得益于精确制导武器的发展,它可对敌方 C² 系统的各个部分进行外科手术式的打击。

反辐射导弹是摧毁性电子攻击的一种手段。反辐射导弹通过跟随关键传感器或通信链的辐射信号而被制导到辐射源上。这使得在可能遭受反辐射导弹攻击时,传感器或通信链只能停止工作。

定向能武器(DEW)是另一种摧毁性电子攻击手段。定向能武器采用激光、带电粒子或微波/射频波束,其吸引人之处是它们以光速进行攻击。目前,因功率受限,定向能武器在战术使用上还只能对电子设备进行破坏或烧毁。

1.3 电子战作战模式新发展

能够战胜未来任何潜在对手的军事能力基础就是在信息控制方面保持绝对优势。电子战能够直接用于压制敌方的军事信息系统和信息化武器系统,从整体上瓦解敌人的战斗力,进而决定战争的进程与结局。进入新世纪后,电子战在现代军事行动中的作用更加突出,近年来,电子战领域出现了一些新的概念和作战模式,主要有网络中心电子战、联合电子战、电磁频谱管控、电磁战斗管理等等。与电磁频谱管控相比,电磁战斗管理指向更具体,操作性更强,与电子战及整个作战行动结合更密切。

1.3.1 网络中心电子战

1. 含义

21 世纪初美军把网络中心战概念应用于电子战作战,发展和形成了网络中心电子战。网络中心电子战是电子战作战模式的创新与发展,它提供了一种协同、综合、多平台、以网络为中

心的电子战能力,实现了基于效果的作战目的,用以提高各种电子战资源的利用率,增大承担各种作战任务的灵活性,提高电子战资源的指挥控制能力,以便增强其对遂行各种作战任务的能力,从而控制电磁频谱,以夺取战斗空间的信息优势。

2. 特征

网络中心电子战系统具有精确电子战态势感知、目标截获和电子攻击能力。这种能力是并行的,集成了陆、海、空、天多平台的协同电子战能力。

网络中心电子战利用强大的计算机信息网络和电子战数据链,把各种电子战装备组成一个互相连接的自适应系统网络。即把具有不同频谱特性、不同功能、分散于不同位置的各种电子战装备作为一类特定权限的终端或节点接入电子信息网络。网络中的电子战装备承担履行的任务,接受网络管理、享受网络资源和服务,通过网络使各种电子战侦察系统、指挥控制中心、干扰系统、火力系统连接成整体进行作战,实现整个战场范围内的信息共享和资源优化,能有效控制和使用整个电磁频谱,达到不同平台上的设备如同在一个平台上的效果。该网络能够动态地适应不断变化的环境,进而提高各个系统的威胁响应能力和态势感知能力。

3. 网络中心电子战系统体系结构

网络中心电子战系统体系结构根据遂行任务的不同,可由网络中心电子战系统体系结构总框架派生出不同的系统体系结构。无论何种电子战装备都可作为一类特定权限的终端或节点,通过有线或无线通信方式(例如武器数据链),在理论上均可以构成服务于特定或整个战场需求的网络。当功能和规模扩大时,可与整个作战系统中所有与信息有关的装备相连,包括信息系统、指挥控制系统、武器系统,承担各种作战任务、接受网络管理、享受网络资源和服务,从而提高作战的整体效能。

网络中心电子战并不是以网络中心计算和通信为重点的,而是以信息流动、作战空间实体的本质和特征以及它们相互作用的方式为重点,其实质是作战。网络中心电子战反映并综合了在信息时代获得成功所必需具有的特征属性,即先于敌人了解战场空间,从而获得战场作战的灵活性和主动性,以便实施最优的电子战作战行动并对付突然出现的威胁。

1.3.2 联合电子战

在现代军事斗争中,电子战是一种十分复杂的作战行动,为了充分发挥其潜在能力,对达成作战目标作出贡献,电子战必须与其他作战行动完全综合为一体。联合电子战的发展,使电子战产生了新的作战特征,即可有效地支援多种形式的军事斗争。进行联合作战时,作为一种火力武器,电子战成为武器组合中密不可分的一部分。在对敌实施强大的电子攻击、迷惑或欺骗对手、在敌人发现之前进行突袭和穿越、自卫干扰、防区外干扰、防区内干扰和随队干扰等诸多方面,电子战可利用在陆、海、空、天领域的人工或者自动化系统,在联合作战中有效支持包括侦察、阻止、欺骗、破坏、削弱、防护和摧毁在内的多种形式的作战行动。因此,联合电子战是联合作战概念指导下电子战作战能力的有效集成,可产生最佳的作战效果。

为了满足联合作战的需要,电子战任务必须具有可融合性、可协调性、可重编程等新特性。

1. 融合性

在阿富汗和伊拉克的多国部队作战行动中,电子战率先成为联合作战的组成部分。美军指挥员将美国与联军和盟军的电子战能力纳入整体电子战作战方案,进而对联军和盟军提供电子支援,即进行识别威胁、威胁视避、指示目标和目标寻的等战术行动。像军事行动的其他

方面一样,联合作战中的电子战行动也是统一计划并分散实施的。因此,电子战行动经常融于各种作战行动之中,成为联合作战的重要组成部分。

2. 协调性

电子战作战协调是联合作战协调的重要组成部分,其协调的整体性强、协同层次高、协调专业性强。协调性主要包括以下几个方面:

(1) 电子战与情报的协调。

电子战与情报部门间的协调主要是确保电子攻击行动所需情报,确保电子攻击行动效果;电子战与情报部门要保持密切的协调,不断消除相互之间在干扰需求与情报需求上的冲突。

(2) 电子战与电磁频谱管理的协调。

电子战作战部门与频谱管理部门的协调,是要根据敌我双方电磁频谱使用情况,修改联合保护频率表,以便对禁止干扰频率、保护频率、干扰频率、监视频率进行联合监管,综合利用和控制电磁频谱,消除电磁频谱冲突。

(3) 电子战与作战保密的协调。

电子战、网络战、情报和频谱管理部门通过监视敌我双方频谱使用情况来监视作战保密效果,如隐蔽频率是否暴露、网上是否泄露重要信息。电子战与作战保密部门要及时评估己方电磁辐射控制效果,提出改进保密手段及方式的建议。

(4) 电子战与军事欺骗的协调。

电子干扰部队有选择地干扰、扰乱敌方传感器,伪装部队模拟不同目标。由这些电子欺骗行动产生的“电特征”,与其他军事欺骗活动综合,欺骗敌方传感器,造成不同部队规模及行动的假象,并在较长时间内维持其可信度,以使敌方做出错误判断。

(5) 电子战与心理战的协调。

电子战采取电子攻击行动,对敌方广播、通信和网络进行压制时也要与心理战密切协同,消除两者在频率和网络资源使用上的冲突。利用电子战手段向敌方发送有关信息,产生心理战效果,同时,作战中将电子战收集到的敌方信息,应及时地通报心理战部队,使其掌握心理战的效果。

(6) 电子战与实体摧毁的协调。

电子战要及时与实体摧毁行动进行协调,以使电子战计划更全面。电子战情报部门绘制的电磁态势图,可以为其他武器攻击行动提供航路和规避参考。电子干扰和定向能武器攻击行动,与己方引信、遥控、遥测、制导活动有关,因此也应与实体摧毁行动密切协调,杜绝冲突。

3. 可重编程

随着战场环境的变化,电子战常需要重新规划与编制作战程序。包括改变自卫系统、进攻性武器系统和情报收集系统的程序,以保持和增强电子战和目标探测设备的作战效能。重编程主要用于威胁变化、任务修改和地理修改等特定情况。威胁变化,包括敌方威胁系统在作战时电磁信号特征的任何改变;任务修改,可提高系统对严重威胁做出反应的能力;地理修改,可对某个特定地区和区域实施作战。特别在联合作战期间,在敌情迅速变化的情况下,重编程工作的迅速判定和执行,可能成为生死攸关的问题。

1.3.3 电磁频谱管控

电磁环境对电子战作战效能发挥具有非常重要的作用,而频谱管理和控制是使电子战装

备有效使用的前提和保证。电磁频谱是重要的作战域,电子战是电磁频谱作战域的主要行动样式,电子攻击(EA)是频谱攻击部分,电子防护(EP)是频谱的防护部分,电子支援(ES)是频谱利用部分。电磁频谱控制采取的主要举措有:

1. 制定管理规则

为了维护电磁频谱的安全,应建立一整套完整的联合战役频谱管理体系,形成相应管理机制,同时要制定一系列管理条例、操作规程和技术标准,为全面管理电磁频谱提供统一的依据。

2. 制定电子战作战频谱管理计划

电子战电磁频谱管理计划包括:确定作战方案与需要保护的关键目标;进行情报评估;明确受保护的节点与网络并区分优先级;拟制、分发联合限制性频率表;拟制频谱使用计划。

3. 确定作战方案与需要保护的关键目标

各个作战阶段的作战方案由作战部门确定。对于每一阶段,作战部门根据联合部队作战方案明确被保护的不能被干扰压制和电子欺骗的己方重要目标,并在联合部队作战计划中就电子干扰优先于情报搜集或情报搜集优先于电子干扰的情况提出指导性建议。

4. 进行情报评估

根据作战部门的作战方案,情报部门确定情报支援需求,明确每一个作战阶段中需重点进行情报搜集的敌方电子系统目标和需要受频率限制的相关电子系统节点。

5. 明确受保护的节点与网络区分优先级

应明确区分对敌我双方作战有重大影响的特定节点和设备。为便于在实施电子攻击时对这些节点和网络进行保护,应将其提交给联合部队指挥部门。

6. 拟制、分发联合限制性频率表

根据性质的不同,将限制性频率分为监视性频率、保护频率和禁用频率,以此拟制、分发联合限制性频率表,供作战单位使用。

7. 拟制频谱使用计划

联合频率管理办公室根据部队部署情况、用频装备的数据,利用联合作战计划与实施系统中的数据,对联合部队进行用频需求分析,拟制频谱使用计划,进行频率分配,提出频率使用建议。频谱使用计划是联合部队作战计划的一部分。

8. 电子战频谱管理的实施

电子战电磁频谱管理实施的主要内容包括实时评估频谱管理计划、动态调整部队用频、及时查处用频冲突。

(1)实时评估频谱管理计划。随着作战过程中部队的重新部署和指挥与控制、监测、武器系统和其他用频设备的重新配置,这一电磁环境将会不断变化。因此,联合频率管理部门要对作战区域电磁环境进行不间断的评估,判断频谱管理计划的有效性,提出联合用频冲突解决方案,对可能出现的频谱管理问题提出建议。

(2)动态调整部队用频。按照联合限制频率表和辐射控制计划进行电磁环境监测;根据出现的频率冲突的要求,提出调整电磁频谱行动的建议;提出电子攻击运用的指导性意见和附加的交战规则建议,确保电子攻击计划与标准的交战规则相一致;制定确保通信网在有意干扰或无意干扰入侵时能有效工作的应急措施;指定干扰控制负责人,协调和解决电子攻击行动与其他电磁频谱应用之间的冲突。

(3)及时查处用频冲突。电子战计划人员检查电子攻击任务是否与联合限制性频率表有