

# 电子战综述

杜 辉

(中国电子科技集团公司第54研究所 石家庄 050002)

**【摘 要】**介绍了电子战的定义及内涵、分类、应用领域及发展趋势。电子战也称电子对抗,是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。电子战包括电子侦察、电子攻击和电子防护三个方面。电子战的应用领域包括平时期的电子战、危机时期的电子战、冲突时期的电子战、主战武器平台自卫用的电子战等四个方面。未来信息战中,电子战的地位将越来越突出。可以预测未来电子战技术的发展趋势是:电子战作战效能增大、发展电子战硬杀伤手段、电子战力量构成会改变、电子战将成为独立的战役行动、电子战双方将争夺外层空间。

**【关键词】** 电子战 电子侦察 电子攻击 电子防护

## 1 电子战的定义

电子战也称电子对抗,是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。电子战包括电子侦察、电子攻击和电子防护三个方面。

电子侦察是用电子侦察装备对敌方军事电子设备辐射的电磁信号进行截获、检测、分析、识别、定位,以便查清敌方军事电子设备及其相关平台的性能和配置,从而可以帮助了解敌方的作战意图、兵力部署和军事电子装备的技术性能,以便为己方指挥决策和电子战装备设计提供情报支援。

电子攻击是以削弱、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。

电子防护是为保护人员、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)密切相关的,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。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。

## 2 电子战的分类

按前面电子战的定义,电子战包含三大部分:电子侦察、电子攻击和电子防护。

### 2.1 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。

### 2.2 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

定稿日期:2005-03-16

的电磁信息。它包含电子伪装、模拟欺骗、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。

### 2.3 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、自适应天线调零、跳频、扩谱等等,用以减小或降低电子干扰对己方电子设备的影响。

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很多,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。

## 3 电子战的应用领域

电子战的应用领域包括以下几个方面。

### 3.1 和平时期的电子战

和平时期的电子战包含电子侦察、电子骚扰两个部分。

和平时期的电子侦察,是应用电子侦察卫星、电子侦察飞机、电子侦察船和电子侦察站(车)不断监视和收集其他国家和地区的电磁辐射信号,进行分析、识别、定位,获取对方电子兵器及其相关平台的性能、部署、调动态势,为高层领导决策提供情报依据,并为更新电子战目标数据库提供数据,以便设计和研制针对性强的电子对抗装备。

和平时期的电子骚扰,是应用电子战手段在他国上空制造异常空情,造成不明目标侵入纵深腹地的景象,以探测其防空能力,制造紧张和不安,同时获取情报。

### 3.2 危机时期的电子战

在危机时期,敌意国家利用电子战手段在危机地区制造大批

飞机入侵的景象,同时利用广播、电视、传单等心理战工具,制造紧张局势,达到加剧危机和非武装干涉的目的。

### 3.3 冲突时期的电子战

冲突时期的电子战包括战争时期的电子侦察、进攻作战中的电子战、防御作战中的电子战三个部分。

#### (1) 战争时期的电子侦察

在战争时期,陆、海、空、天电子侦察装备实时收集战区电子和通信情报,经过分析、处理形成敌方的战场态势,为作战指挥决策提供准确的情报依据。在各作战平台上的战斗威胁告警设备和测向设备向驾驶员提供实时的电磁威胁信息,并在操作人员的干预下直接控制、引导电子干扰设备和电子攻击武器,实施电子战作战活动。

#### (2) 进攻作战中的电子战

在进攻作战中,远距离支援干扰飞机、随队掩护干扰飞机、反辐射导弹攻击飞机、定向能武器、电子对抗无人机和地面、海面的电子干扰站在战场指挥官的统一控制和管理下,应用多种电子战手段,协调一致地干扰和攻击敌方的预警探测网、指挥通信网和武器拦截网,削弱和降低敌防御体系的综合作战能力,支援攻击机群、攻击舰队和攻击部队的进攻。

#### (3) 防御作战中的电子战

在防御作战中,电子干扰飞机、反辐射武器、定向能武器、地面干扰站、点目标电磁防护系统等在战场指挥官的协调指挥下,对敌进攻体系的目标探测、通信导航、精确制导各个环节实施综合电子战作战活动,以最大限度瓦解敌攻击能力,削弱和降低其攻击效能。

### 3.4 主战武器平台自卫用的电子战

对于高价值的作战飞机、舰艇、坦克,其主要威胁来自精确武器的攻击。因此对于精确制导武器的威胁进行告警,并运用雷达干扰、光电干扰等综合性电子战手段,以压制、诱骗敌精确制导武器的攻击,保障作战平台的安全。因此主战平台自卫用的电子战系统是提高其生存能力,保障其作战效能发挥的关键。

## 4 电子战的发展趋势

未来的战争将是信息化战争,电子战作为信息战主要的作战样式之一,在战争中的地位越来越突出。根据电子战在第二次世界大战、越南战争、贝卡谷地、海湾战争和科索沃战争中的运用、发展轨迹,可以预测未来电子战技术的发展趋势。

### 4.1 电子战作战效能增大

未来信息战中,电子战攻击的主要目标不仅仅是敌方的各种信息系统和装备,甚至还包括作战人员,强大的电子战威力足以对敌人心理或生理造成极大震慑,以影响人的意识或造成人员身体不适。现代战争实践表明,仅仅使用电子战,就可以使敌人侦察无能、信息中断、雷达迷盲、武器失控、指挥瘫痪。

随着反辐射武器、电磁脉冲武器等高性能电子战武器的应用以及天基电子战力量的发展,电子战的威力将逐渐增大。通过电子战,使数个战场网络乃至整个国家或军队的信息作战力量瘫痪

已不是神话。

#### 4.2 发展电子战硬杀伤手段

电子战不仅能对敌方各种信息系统实施软杀伤,而且可以实现对敌方信息系统的硬摧毁。这样不仅可使敌方电子信息系统短期瘫痪,而且可使其永久失效。

随着电子战技术的发展,各种硬杀伤手段将大大拓展电子战的作战领域。再加上各种精确制导武器的硬摧毁,未来电子战必将真正形成“软硬兼施”的一体化打击力量。另外,电子设备、光电设备的发展和广泛应用,使信息化武器装备命中目标的精度进一步提高,杀伤力进一步增强,这也为电子战硬杀伤手段的发展创造了有利条件。

#### 4.3 电子战力量构成会改变

作战力量是构成战役的物质基础和最基本的要求。在电子战中,电子侦察、电子攻击、电子防护是电子战力量的主要构成要素。信息作战中的信息对抗是作战双方信息系统之间的全方位对抗,电磁频谱的迅速扩展,电子战空间的大大拓展,电子战设备种类不断增多,使得电子战力量构成发生变化。

从未来电子战的特殊地位和作用来看,电子战力量将从现在的陆、海、空各军兵种中分离出来,形成独立的电子战军种,同时还会作为独立兵种分布在各军兵种之中。另外,电子战力量还将与其它作战力量相互渗透、融为一体,成为既相对独立,又与其它力量相互渗透的一体化作战力量。

#### 4.4 电子战将成为独立的战役行动

信息作战中的电子战力量已经从初级阶段的通信、雷达、光电等单个设备的对抗,发展成为中级阶段的陆、海、空、天结合并软硬兼施的多种力量综合的系统对抗,形成了一支重要的作战力量。

从近年来几场局部战争来看,无论海湾战争还是科索沃战争,电子战力量还不能独立达到战役目的或形成独立的战役阶段。但随着电子信息系统在武器装备中的运用以及其作用的日趋增大,电子战战役目标体系将会发生巨大变化。信息作战中,夺取制电磁权已经形成和战略性空袭阶段相对独立的阶段,它完成对敌指挥系统的打击,并和其它战役目标一样,并列构成战役目标体系。

从电子战的未来发展趋势来看,一方面,电子战力量作为“软杀伤”力量,将与信息战其它作战手段更加紧密结合,并贯穿于战争全过程,共同达成一定的战役目的;另一方面,电子战自身软硬杀伤手段的结合,将导致以电子战力量运用为核心的独立的夺取制电磁权的战役的产生,这也为电子战力量独立达成战役目标创造了必要条件。可以看出,电子战在战争中的地位和作用越来越突出,并逐步形成相对独立的作战行动。

#### 4.5 电子战双方将争夺外层空间

由于技术水平的限制,目前电子战的主要战场还是集中在空中、地面、海上。但外层空间能够提供更加巨大的指挥、控制和通信能力的作战,使用外层空间的电子战技术成为现代各国竞相发展的重点。随着信息技术、空间技术的发展,电子战势必率先登上信息战角逐的最高场所——太空。空间电子战技术的不断发展,空间电子战能力的进一步提高,必将使大气层外层空间成为电子战角逐的主要场所。

#### 参考文献

- [1] 侯印鸣等.综合电子战[M].北京:国防工业出版社,2000.
- [2] 孙德海.国外电子战发展综述及对我国电子战研究的思考.中国科技发展精典文库,2004卷;(上):第八部分.

(上接第47页)

优点,提高了系统性能指标。

交换机根据需要可以组成链状或星形等多种网络。针对无线传输特点的信令类型和路由选择方式使交换机的适应性大大增强。交换机与其他网络连接时通过E1接口连接,支持中国1号信令和7号信令,可以实现本系统与公用自动电话网等其他网络的互连互通。

## 5 结束语

窄带多功能交换机提出了一种窄带中继条件下,实现多业务交换的解决方案。通过采用低速语音压缩编码和多交换模式的融合技术,满足特殊环境下的业务接入和语音、数据的交换功能。适应边远地区和复杂环境条件下的通讯需求,同时可以完成一定规模的组网应用。

#### 参考文献

- [1] 张文冬.程控数字交换技术原理[M].北京:北京邮电大学出版社,2000.
- [2] 王新梅.纠错码与差错控制[M].北京:人民邮电出版社,1989.

(上接第49页)

相应的操作。

DSP驱动模块是硬件驱动中的关键模块,它的功能包括对CSMV6芯片的初始化,在收到语音数据时进行语音编解码和各种信号音的检测和产生。因为该模块将直接完成对语音的打包操作,必须要求高效率,所以该模块的任务优先级较高。

## 5 结论

该系统实现了一种针对中小容量电话用户交换机的嵌入式企业级VoIP网关,对现有的用户交换机提供了一种新的功能,满足了大量H20-20企业用户的需求。

#### 参考文献

- [1] 电话网关设备技术要求.中华人民共和国通信行业标准[S].
- [2] MPC8260 PowerQUICC II User's Manual.
- [3] RL56CSMV/6 User's Manual.
- [4] Harris 20-20 TELEPHONY BUS SPECIFICATION.
- [5] ITU-T Recommendation H.323 Control-Version 2 (February 1998) -Packet-Based Multimedia Communication Systems.