文章编号:1007-5321(2020)05-0001-08 DOI:10.13190/j.jbupt.2020-037

美俄电子战对抗的现状与分析

陆 震[1], 黄用华[2]

(1.北京航空航天大学 自动化学院, 北京 100083; 2.桂林电子科技大学 机电工程学院, 桂林 541004)

摘要: 电子战和电磁频谱作战在现代战争中具有威慑作用,是决定战争胜负的首要因素,这在一系列局部战争和冲突中得到了充分证实. 冷战结束以来,美国和俄罗斯在该领域展开了激烈的竞争和对抗,新型电子战武器层出不穷. 梳理了近年来美俄两国在电子战武器发展方面的现状和趋势,以作为我国电子战武器研究的借鉴.

关 键 词: 电子战; 电磁频谱; 电磁频谱管理; 电子攻击; 电子防御; 电子战支援

中图分类号: TN97 **文献标志码**: A

Electronic Warfare Confrontation between the United States and Russia

LU Zhen[1], HUANG Yong-hua[2]

(1. School of Automation Science, Beihang University, Beijing 100083, China;
2. School of Mechanical and Electrical Engineering, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: Electronic warfare and electromagnetic spectrum warfare play a deterrent role in modern warfare, which is the primary factor determining the victory or failure of a war. It has been fully confirmed in the recent series of local wars and conflicts. Since the end of the cold war, the United States and Russia have launched fierce competition and confrontation in this field, and new types of electronic warfare weapons emerge in endlessly. It is summarized that current situation and trend of the development of electronic warfare weapons in the two countries in recent years, which can be used as a reference for the development of electronic warfare weapons in China.

Key words: electronic warfare; electromagnetic spectrum; electromagnetic spectrum management; electronic attack; electronic protect; electronic support; electronic warfare

电磁频谱已经成为现代战争中继陆、海、空、天、网络(赛博)之后的第 6 个作战域. 电磁频谱是指从频率为零到无穷大范围(红外线、光、紫外线、伽马射线和宇宙射线等)的电磁波频谱(见图 1). 在电磁频谱领域中的军事对抗就是电子战. 目前对电磁频谱的日益依赖突显了电子战在信息作战中的重要性和挑战性. 信息作战是指将信息技术运用到军事对抗中,是现代战争的发展趋势. 掌握信息控制权,就能在战争中取得主动. 美国和俄罗斯在电磁频谱领域展开了激烈的电子博弈,电子战已经从单一的无线电通信对抗发展为雷达对抗、定向能和光电对抗、隐身与反隐身对抗. 电子战不仅限于一般的射频或雷达频率以及电磁频谱的红外、可见光、紫外线和其他不常用部分,还包括以定向能量控制电磁频谱和攻击敌人的行动[1]. 随着时间的推移,主要的电子战已经发展到能利用电磁能物理学中所有的成果. 根据摩尔定律,每一年半 IC 的集成度翻倍,随着计算机技术和网络的广泛应用,电子战的智能化

收稿日期: 2020-03-26

作者简介: 陆 震(1942—), 男, 教授, E-mail: zhenluh@buaa.edu.cn.

程度大大提高,已经成为一种独立的作战方式,是战争中具有信息威慑作用的一种手段,它不仅是战争的先导,同时也贯穿于战争的全过程. 电子作战已成为信息作战不可分割的部分.

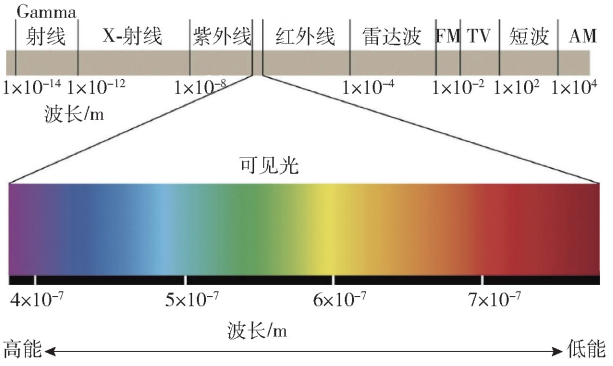


图1 电磁频谱图

1 电子战的历史和组成

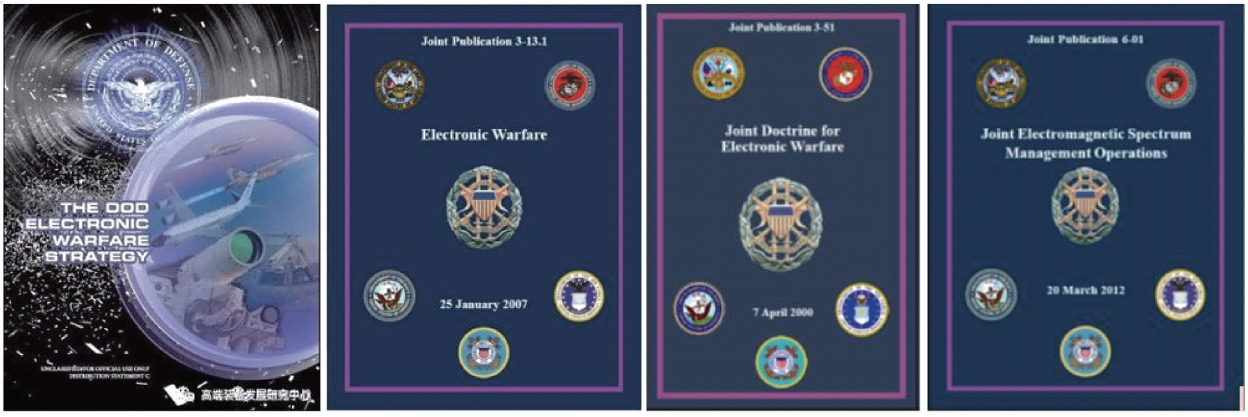
电子战的历史应该追溯到20世纪初. 在1904—1905年日俄战争期间,俄罗斯成功地干扰了日本海军通信信号,并校正了旅顺炮台俄海军的炮火[2]. 在第二次世界大战期间,盟国和轴心国都广泛使用了电子战,导航雷达已用于将轰炸机引导至目标并返回其基地. 电子战在第二次世界大战中的第1个应用是干扰导航雷达,在此期间,箔条也被引入,用来迷惑和扰乱导航雷达系统. 越南战争期间,电子战在许多军事行动中发挥了重要作用,美军综合采用多种对雷达的电子对抗措施,曾一度使地空导弹的命中率下降到2%. 海湾战争中,美军出动数千架次F 117A隐身轰炸机对防空火力最强地区进行轰炸,在强大的电子干扰掩护下,无一损失[3]. 2007年的"盒外行动"(或称"果园行动")中,以色列军队使用电子战系统使叙利亚防空系统瘫痪,以色列空军的10架F-15战机毫无阻拦地穿越了叙利亚的大半个领空,成功地摧毁了一座疑似在幼发拉底河附近的据称由伊朗提供资金建造的核反应堆,完成袭击任务后,这10架战机毫发未损地回到基地. 这是一个成功利用电磁频谱进行突防的典型战例[4].

电子战包括电子攻击、电子防御和电子战支援3个部分. 电子攻击(也称为电子对抗措施)是指使用电磁能量、定向能量或抗射频的武器攻击敌方人员、设施或设备,目的是压制、拒止或击毁敌方作战能力. 在电磁能量参与下,这类行动包括干扰,可针对通信系统(射频干扰)或雷达系统(雷达干扰和雷达欺骗)进行干扰. 电子攻击除了可以拒止或压制敌人使用电磁频谱的能力,还能使用电磁能量或定向能量作为杀伤武器,毁伤敌方的设施和有生力量,并具备进攻性自我防护功能. 电子防御(也称为电子防御措施或电子反对抗措施)是指为保护己方和友军(人员、设施和设备)免受友军或敌军使用电磁频谱的任何不利影响而采取的行动,可使用电磁频谱来保护人员、设施和设备. 例如,机载电子对抗和其他保护措施,诸如使用投放物(照明物和主动诱饵)、干扰器、拖曳诱饵、定向红外线反制措施和联合无线电控制的简易爆炸装置等各种对抗措施. 电子战支援是电子战的第3部分,是在作战指挥官授权或直接控制下,为了快速识别威胁,锁定目标,规划和引导后续行动而进行的搜索、拦截、识别和对有意和无意的电磁能辐射源定位,以便规划和进行未来作战. 电子战支援提供了电子战作战和其他战术行动(规避威胁、瞄准和寻的)决策所需的信息. 电子战支援数据可用于产生信号情报,为电子攻击和其他战术进攻行动提供目标,并产生测量和信号情报. 信号情报还可以提供战斗损伤评估和对总体作战计划效果的反馈. 传统意义上的信号情报和电子战支援不同,虽然二者都需要探测和感知外部发射信号,其技术和装备有所重叠,但是信号情报侧重于监听敌方通信,而电子战支援的目的是阻断信号.

2 美俄电子战的博弈

面对俄罗斯和中国日益强大的军事实力和国防科技水平的提高,美国感到其军事霸主的地位受到威胁,近年来将俄罗斯和中国作为美军的主要战略目标. 2017年1月,美国国防部发布了《电子战战略》[5]. 2018年1月,美国发布了新版《国防战略》[6],明确将美军的战略重点从打击恐怖主义转移到针对俄罗斯和中国这样势均力敌的对手上. 2018年8月,美国总统签署发布了《2019年国防授权法案》[7],进一步将中国作为主要的战略对手. 大国对抗成为美国未来争夺电子频谱优势的目标,五角大楼提出了电磁频谱战的新概念,从作战理论到电子战武器装备进行深入探讨和更新. 美军分析了

目前电子战组织结构分散零碎的现状，建立了电子战执行委员会等高层管理机构，制定并发布了电磁频谱战略和电子战战略，把电子战和电磁频谱管理提高到联合作战的高度，从 2007 年开始就不断发布一系列和联合电子作战有关的军事条令（见图 2），如美军 JP 3-13.1、JP 6-01、FM 6-02.70、FM 3-36 和 FM 3-12 等. 其实早在 2000 年，美军在其联合出版物 Joint Publication 3-51《电子战联合条令》（Joint Doctrine for Electronic Warfare）中就指出了电磁频谱在联合作战中的重要性.



(a) 图防部电子战战略　(b) 电子战　(c) 电子战联合条令　(d) 联合电子频谱管理行动

图 2　联合作战中关于电子战和电磁频谱的条令

美军参谋长联席会议在 2007 年发布的联合出版物 JP 3-13.1《电子战》（Electronic Warfare）和 2012 年发布的 JP 6-01《联合电磁频谱管理行动》（Joint Electromagnetic Spectrum Management Operations）中给出了联合电磁频谱作战的定义. 美国陆军 2010 年发布的 FM 6-02.70《美国陆军电磁频谱作战》（Army Electromagnetic Spectrum Operations）条令、2012 年发布的 FM 3-36《电子战》（Electronic Warfare）条令、2014 年发布的 FM 3-38《赛博电磁行动》（Cyber Electromagnetic Activities）条令以及 2017 年发布的野战指南 FM 3-12《赛博与电子战作战》（Cyberspace and Electronic Warfare Operations）条令中也都有电磁频谱作战的定义. 2019 年 7 月 30 日，美国空军发布新的电子战条令，用新的条令附录 3-51《电磁战与电磁频谱作战》替代了 2014 年 10 月发布的条令附录 3-51《电子战》[8]，它是空军对应联合条令 JP 3-13.1《电子战》的军种电子战条令.

在这些条令和文件指导下，美国陆军把电子战、赛博战和信号情报整合成一种全新的数字化战争，实现未来的多域作战. 美国陆军综合电子战系统中的具有主动攻击功能的模块——多功能电子战系统于 2023 年才会初步具备作战能力，而在乌克兰、叙利亚冲突之后，美国陆军深感电子战能力缺乏，为了解决 2023 年前电子战能力不足的问题，自 2015 年起美国陆军着手建立军以下战术性赛博电磁行动分队，建设快速反应能力装备和快速采购电子战装备的机制. 美国陆军没有采取俄罗斯在乌克兰、叙利亚的电子作战模式，即用大功率武器来干扰 GPS、雷达和无线电设备. 他们认为大功率干扰器极易暴露其位置，成为远程精确打击的目标. 他们采用了一种不易被目标察觉的方式干扰、欺骗和阻断对方的电子设备，除了能应对无线电遥控简易炸弹威胁外，还具备了应对无人机威胁的能力，图 3 和图 4 所示即是这样的电子战装备[9]. 美国陆军计划投入机载和陆基电子战项目研发经费，期望比对手更具竞争力. 这项投入包括建立一个新的专门从事电子战任务的部队，设法实现长续航时、无人的机载电子战系统和部队训练. 2017 年 5 月，美国陆军在南加州欧

图 3　VROD[9]

文堡国家训练中心举行的一场演习中,一支跟随假想敌部队参加演习的赛博电磁行动分队运用赛博和电子战装备对一支参训的坦克部队进行了攻击. 赛博诱骗和伏击使得该部队指挥系统部分失灵,而电子攻击则导致参训坦克部队的无线电通信失灵. 当坦克被迫停止行进,坦克部队指挥官还未弄清问题时,攻击方即刻实施的密集炮火打击,使该坦克部队直接退出了演习[10].

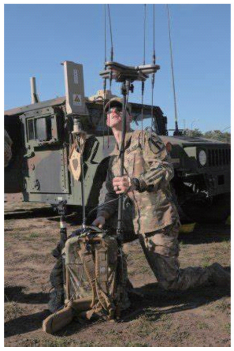


图4 VMAX[9]

美国空军方面,由于近20年来一直强调隐身,对机载电子战有所忽视. 目前这种状况正在改变,美国空军为研究下一代电子战,强调保持空中优势、多域指挥与控制能力和顺畅接入电磁频谱. 2018年1月,美国空军成立了一个“电子战/电磁频谱优势体系能力协同小组”的跨职能团队[11],以探索美国空军如何确保电磁频谱优势. 按照这些战略部署,美国空军和海军开展了机载和舰载电子战装备的研制. 美国空军主导了认知干扰机与大功率高效射频数模转换器项目[12]、频谱战评估技术工程[13]、反电子高功率微波先进导弹项目[14]等的研制. 其中的反电子高功率微波先进导弹系统采用了高功率射频技术,能够进入有争议的地区,使对手的电子系统失效(见图5).

美军开展了海上电子战改进(SEWIP-Block I/II/III,SLQ-32)舰载电子战系统[15]、舰船信号探测装备(SSEE, ship's signals exploitation equipment)[16]、电磁机动指挥与控制、下一代干扰机[17]等项目的研究. 其中,SSEE是一个信号探测系统,允许操作者监视和分析各种船舶级别上船舶探测空间内的有用信号. SSEE系统由AN/SSQ-80本地监控子系统和TRUMP系统演变而来,后者为系统提供了基本的密码分析能力. SSEE系统在地平线附近和地平线上方探测、识别和定位目标的能力不断

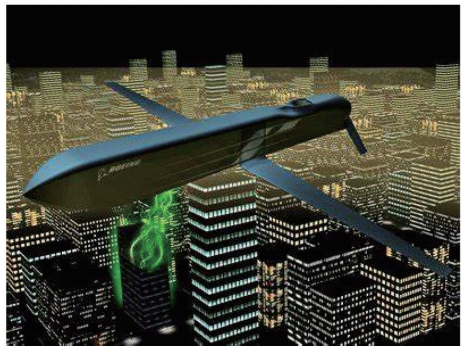


图5 反电子高功率微波先进导弹项目[14]

增强,对舰艇的指挥、控制和战斗能力具有重大贡献,并将成为舰艇信息战的作战中心.

美国国防部高级研究计划局开展了多项前沿电磁频谱作战项目的研究,如行为学习自适应电子战(BLADE, behaviour learning for adaptive electronic war)[18]、自适应雷达对抗(ARC, adaptive radar countermeasure)[19]、极端射频频谱条件下通信(CommEx, communication under extreme radio spectrum)[20]、近零功耗射频和传感器运行[21]等.

BLADE具有在战术环境中对抗新的动态无线通信威胁的能力[22],使电子战系统能够在战场上自主学习,以干扰新的通信威胁,目的是实时对抗敌方自适应无线设备和网络指挥、控制和通信以及遥控简易爆炸装置等带来的无线通信威胁.

ARC旨在使美国机载电子战系统能够在现场实时自动生成针对新的、未知的和自适应的雷达波的有效对抗措施,由BAE公司为主进行技术开发. ARC项目计划利用信号处理和机器学习方面的成果来开发智能算法,以检测和应对新出现的雷达威胁. CommEx是主要针对在遭受严重干扰压制的情况下,开发的一种具备高度自适应能力和灵活性的通信系统. 在Link16电台上对CommEx项目的自适应抗干扰系统进行了测试,并测试了其在飞行中的抗干扰性能. 雷神公司的新一代机载干扰机ALQ-239是一种先进的电子攻击系统(见图6),可以拒止、干扰和削弱敌人的作战能力,包括通信工具和防空系统[23].

波音EA-18G“咆哮者”(见图7)是一架美国舰载电子战飞机[17],是两座F/a-18F超级大黄蜂的专门版本. EA-18G取代了在美国海军服役的诺斯罗普·格鲁曼公司的EA-6B“徘徊者”. “咆哮者”的电子战能力主要由诺斯罗普·格鲁曼公司提供. EA-

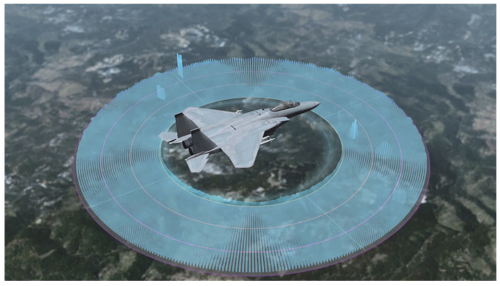


图 6　ALQ-239 数字电子战系统[23]

图 7　波音 EA-18G “咆哮者”[17]

18G 于 2007 年开始生产，2009 年底进入美国海军服役.

俄罗斯是最早使用电子战的国家，在 1904—1905 年间的日俄战争中就建立了无线电干扰和无线电通信保护系统，先后被黑海舰队和波罗的海舰队使用. 在苏联卫国战争爆发前的 1939 年，俄罗斯进行了首批无线电干扰台样机测试. 无线电特战营使用这些电台成功监听并压制了纳粹德国集团军-军团-师团链条的无线电通信[4].

近些年，俄罗斯为了对其潜在对手保持更加有效的威慑态势，更是将电子战视为对抗以美国为首的西方军队的“不对称”手段之一，不断加强自身电子战力量和电子战装备系统建设. 在战术层面，俄军具备了地面部队的电子战能力，建立了在旅/师级的电子战连，能够干扰通信，通过鲍里索格列布斯克-2（P-934Б/P-378Б/P-330B Мандат/Борисоглёбск-2）干扰无线电控制的火炮引信和精密武器所必需的全球定位系统信号（P-3303-житель/Борисоглебск-2）[24].

据美国《防务邮报》报道[25]，美国特种作战司令部司令雷蒙德·托马斯抱怨道：“叙利亚已成为地球上最富侵略性的电子战区域. 俄罗斯和叙利亚政权部队每天都在考验我们，破坏我们的通信，使我们的 EC-130 飞机瘫痪. ” 俄罗斯能够进行这种干扰的系统是“克拉苏哈-4（Krasukha-4）”（见图 8），它主要用于对抗攻击、侦察和无人飞机的雷达，据报道已经部署到叙利亚. 俄军在叙利亚赫迈米姆空军基地部署的“克拉苏哈-4”电子战系统甚至能够切断敌人在半径 250 km 内所有的地面电子战系统，是俄军极具代表性的先进战场电子战系统. 车载发射器不仅可以干扰雷达信号，还可以控制无人机的频道，使飞机变得“又盲又聋”，有效范围可达 300 km（185 mile）.

图 8　克拉苏哈-4[28]

洛克希德·马丁 EC-130 罗盘呼叫是美国最先进的电子战飞机. 该飞机以 C-130 大力神为平台，用于破坏敌方的通信、雷达和指挥行动，但在叙利亚空中却遭到了俄罗斯电子战武器的打击. 一名美国匿名军官告诉 NBC（national broadcasting company）：俄罗斯的电子战作战正在对美国的军力产生重大影响. 他说：“这些复杂的攻击甚至成功地针对加密信号和反干扰装置.” 俄罗斯军队在整个乌克兰东部的战斗中，用干扰器来破坏乌克兰的通信和禁用监视无人机，就连欧洲安全与合作组织的无人机也受到俄罗斯常规和电子武器共同作用的影响. 俄罗斯军队的军区、军、旅、营都建立了电子战系统和部队. 最初，电子战武器被用来保护俄罗斯军队和基地，减少了人员和物质损失. 2018 年 1 月，莫斯科展示了数架无人机，据称这些无人机是武装分子发射的，并在叙利亚的赫迈米姆空军基地附近通过电子干扰和拦截导弹的组合被击落. 叙利亚的冲突不断升级，为新式电子战武器提供了理想的试验场[26].

另一方面，在战役和战略层面，俄罗斯在陆军中建立了相当完善的电子战体系. 早在 2009 年就组建了直接隶属俄罗斯武装力量最高统帅部的第 15 独立电子战旅，而且俄军每个军区都有独立电子战旅，在电子战旅下设战略电子战营和战术电子战营，分别配备了“摩尔曼斯克-BN（Мурманск-БН）”通信压制站[27]，“摩尔曼斯克-BN”雷达系统可抑制敌

人在5 000 km以内的控制和通信系统. 目前,俄军共有5个独立电子战旅,每个旅兵力达1 200人,装备的干扰系统战场作用距离可达数百公里. 同时,俄军地面部队每个常规作战旅均编有电子战连,装备的干扰设备战场作用距离可达30 km.

俄海军北方舰队已换装新式电子战装备,除了“摩尔曼斯克-BN”和“克拉苏哈”等远程电子战系统,未来还将配备新式“季夫诺莫里耶”电子设备. 报道称,远东地区堪察加半岛部署“摩尔曼斯克-BN”电子战系统后,整个北方海航道都将被纳入电子战装备的严密监控之下. 这些装备可对非法侵犯俄罗斯边界的舰艇和飞机的通信、导航及指挥系统进行干扰.

俄罗斯空天军也为其各型战机配备了现代化的电子战装备和系统,其中包括配备在苏-34前线轰炸机上的“希比内”干扰系统和配备在米-8直升机上的“杠杆”干扰系统. 俄军在叙利亚部署的米-24、卡-52武装直升机和米-17运输直升机均装备有“维捷布斯克(Витебск)”和“总统(Президент)”单机保护系统. 这些电子战系统可以干扰敌方光学和红外制导弹头的导弹,诱使其偏离原来的飞行轨道. 在叙利亚战场上,这类系统曾成功干扰了叙利亚反对派用“Pin-1”式便携式防空导弹对米-17运输直升机的攻击. 同时,俄军还有以伊尔-18、伊尔-22等飞机为平台的机载电子干扰机. 俄军2018年列装了“季夫诺莫里耶(тивноМорье)”多用途移动电子战系统,对包括美国E-3和E-2预警机、E-8“联合星”指挥控制机等在内的多型飞机、直升机和无人机的雷达及其无线电电子系统进行压制.

近年来,俄军在克里米亚、乌克兰危机中以及叙利亚战场上展示出了强大的电子战能力. 2018年1月8日,俄罗斯国防部发布消息称,当地时间1月5日晚至6日清晨,俄罗斯在叙利亚境内的赫迈米姆空军基地和塔尔图斯海军基地成功抵御了大规模无人机袭击. 俄军防空部队共探测到13架无人机向俄军事基地靠近,俄军电子战部队成功截获并控制了6架无人机,其中3架降落在基地外受控区域,3架在触地时爆炸,其余7架被俄军的防空部队“铠甲-S”防空综合体摧毁. 此次事件在向世界表明,电子战是对抗无人机蜂群攻击这一新型空中打击形式有效手段的同时,更充分展示了俄军强大的战场电子对抗能力.

俄军的电子战实战能力给美国等潜在战略对手造成了极大的威慑. 特别是在克里米亚战争期间,2014年4月10日,一架俄军苏-34战斗机使用配备的“希比内”电子战系统,对敌空情雷达(警戒、引导雷达和目标指示雷达)厘米波段实施了噪声干扰或直接压制. 而在2017年4月,美军对叙利亚境内沙伊拉特空军基地发射的59枚“战斧”导弹中,疑有36枚是受到俄军米-8MTPR-1直升机装备的“杠杆-AV”电子战系统干扰而偏离目标.

2017年9月14—20日,在俄罗斯和白俄罗斯的“西方-2017”联合演习中,俄军释放的强大通信干扰甚至严重影响了拉脱维亚、挪威和瑞典等北约国家的通信. 为此,美国和北约国家均认为俄军的电子战力量已经对其构成巨大威胁,北约官员甚至感叹“北约电子战能力不如俄军的十分之一”.

3 结束语

电磁频谱空间已成为大国博弈的重要战场,电子战已成为具备战略威慑能力与战术进攻手段的新型作战力量. 我国在这场电磁频谱作战的博弈中正在迎头赶上,成为这个作战领域不可忽视的力量. 展望未来,电子战和赛博作战将涌现出更多颠覆性的新技术和新装备,呈现出更多新的应用,成为军事博弈的制胜力量. 目前美俄先进的电子战装备不断升级,在发展战略上,美国重视电子战条例的制定,以保证电子战装备的型谱化,不允许不同军种重复开发,同时重视单兵电子战的开发,极大地提高了单兵作战能力和大大减少作战人员的伤亡. 俄罗斯重点放在战略战术电子战装备的发展上,在某些领域已经超过美国同类电子战装备.

美俄在发展电子战和电子频谱战的装备方面各有所长,可供我国借鉴. 我国在这方面还有较大差距. 笔者认为装备的系列化和型谱化是非常重要的,不但要有战略性和战役性电子战攻防武器,也要发展用于单兵和连团级的战术电子战装备. 此外,机载电子战装备在未来战争中的作用也不容忽视.

参考文献:

[1] 陆震,冯向京. 空间武器的发展态势[J]. 兵器装备工程学报, 2017, 38(9):1-7.
Lu Zhen, Feng Xiangjing. The trend of space weapon's evolution[J]. Journal of Ordnance Equipment Engineer-

ing, 2017(9):1-7.

[2] Semenoff V. The Russo-Japanese war at sea 1904-5: volume 1-port arthur, the battles of the yellow sea[M]. 2014:1-296 .

[3] Fulghum D A, Robert W, Butler A. Israel shows electronic prowess [EB/OL]. 2010(2010-09-28) [2020-02-24]. https://warsclerotic.com/2010/09/28/israel-shows-electronic-prowess/.

[4] Spreckelsen von M. Electronic warfare: the forgotten discipline [EB/OL]. 2019 (2019-06-14) [2020-02-24]. https://www.japcc.org/electronic-warfare-the-forgotten-discipline/.

[5] Sean D C. EW: DOD releases electronic warfare strategy to stakeholders [EB/OL]. 2017 (2017-06-24) [2020-02-24]. https://toinformistoinfluence.com/2017/06/24/ew-dod-releases-electronic-warfare-strategy-to-stakeholders/.

[6] Zech A. The 2018 national defense strategy [EB/OL]. 2018(2018-01-22) [2020-02-24]. https://www.hsdl.org/c.

[7] Congress GOV. National defense authorization act for fiscal year 2019[EB/OL]. 2018(2018-05-15) [2020-02-24]. https://www.congress.gov/115/crpt/hrpt676/CRPT-115hrpt676.pdf.

[8] DoD of USA. ANNEX 3-51 electromagnetic warfare and electromagnetic spectrum [EB/OL]. 2019(2019-07-30) [2020-02-24]. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-51/3-51-D12-EW-EMSO-Planning.pdf.

[9] Pomerleau M. Outmatched, army begins long road to electronic warfare rollout[EB/OL]. 2017 (2017-10-02) [2020-02-24]. https://www.c4isrnet.com/electronic-warfare/2017/10/02/outmatched-army-begins-long-road-to-electronic-warfare-rollout/.

[10] Walsh S. In remote southern California desert, U.S. army tests advanced cyber weapons [EB/OL]. 2019 (2019-05-31) [2020-02-24]. https://www.npr.org/2017/05/31/530929908/in-remote-southern-california-desert-u-s-army-tests-advanced-cyber-weapons.

[11] Managing Editor. US air force launches enterprise capability collaboration team [EB/OL]. 2018(2018-02-21) [2020-02-24]. https://defensetechconnect.com/2018/02/21/us-air-force-launches-enterprise-capability-collaboration-team.

[12] Hill J. Raytheon wins DARPA HiPerdac research, demonstration award [EB/OL]. 2012(2012-04-11) [2020-02-24]. https://www.satellitetoday.com/government-military/2012/04/11/raytheon-wins-darpa-hiperdac-research-demonstration-award/.

[13] Economic Time. Air force research laboratory awards macaulay-brown a seven-year spectrum warfare evaluation and assessment technology engineering contract [EB/OL]. 2016(2016-01-25) [2020-02-24]. https://www.econotimes.com/Air-Force-Research-Lab-Awards-MacAulay-Brown-a-Seven-Year-Spectrum-Warfare-Evaluation-and-Assessment-Technology-Engineering-Contract-148951.

[14] Global Security. High powered microwave advanced missile project (CHAMP) [EB/OL]. 2018(2018-04-14) [2020-02-24]. https://www.globalsecurity.org/military/systems/munitions/champ.htm.

[15] Freedberg S J. Navy's new jammer passes critical design review: SEWIP block III [EB/OL]. 2016(2016-05-09) [2020-02-24]. https://breakingdefense.com/2016/05/navys-new-jammer-passes-critical-design-review-sewip-block-iii/ .

[16] Global Security. Ship's signals exploitation equipment (SSEE) [EB/OL]. 2013(2013-01-14) [2020-02-24]. https://www.globalsecurity.org/intell/systems/ssee.htm.

[17] NACAIR. Next generation jammer (NGJ) overview [EB/OL]. 2014 (2014-03-31) [2020-02-24]. https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2014/PSAR/Croxson.pdf.

[18] Defense Advanced Research Projects Agency. Behavioral learning for adaptive electronic warfare (BLADE) [EB/OL]. 2011 (2011-01-04) [2020-02-24]. https://www.darpa.mil/program/behavioral-learning-for-adaptive-electronic-warfare.

[19] Giangreco L. Adaptive radar countermeasures (ARC) [EB/OL]. 2016 (2016-11-09) [2020-02-24]. https://www.flightglobal.com/darpa-selects-bae-to-develop-new-counter-to-modern-radars/122242.article.

[20] BAE Systems. Communications under extreme RF spectrum conditions [EB/OL]. 2016 (2016-05-11) [2020-02-24]. https://www.baesystems.com/en-us/download-en-us/20160511234534/1434581048612.pdf.

[21] Olsson R H, Gordon C, Bogoslovov R. Zero and near zero power intelligent microsystems[J/OL]. Journal of Physics: Conference Series, 2019, 1407 (12042): 1-8 [2020-02-24]. https://iopscience.iop.org/article/10.1088/1742-6596/1407/1/012042/pdf. Doi: 10.1088/1742-6596/1407/1/012042.

[22] Sameer A. Cognitive electronic warfare system [EB/

OL]. 2016 (2016-10-31) [2020-02-24]. https://www.researchgate.net/publication/309292171_Cognitive_Electronic_Warfare_System.

[23] MilitaryLeak. ALQ-239 digital electronic warfare system (DEWS) [EB/OL]. 2020 (2020-03-24) [2020-05-21]. https://militaryleak.com/2020/05/24/alq-239-digital-electronic-warfare-system-dews/.

[24] Defense Security News. Russian army units of eastern district have received new borisoglebsk-2 electronic warfare vehicles[EB/OL]. 2015(2015-02-11) [2020-02-24]. https://www.armyrecognition.com/february_2015_global_defense_security_news_uk/russian_army_units_of_eastern_district_have_received_new_borisoglebsk-2_electronic_warfare_vehicles.html.

[25] Varfolomeeva A. Signaling strength: Russia's real Syria success is electronic warfare against the US[EB/OL]. 2018 (2018-05-01)[2020-02-24]. https://thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/.

[26] Brennan D. Russia is attacking US forces with electronic weapons in syria every day, general says[EB/OL]. 2018 (2018-05-31) [2020-02-24]. https://www.newsweek.com/russia-attacking-us-forces-electronic-weapons-syria-daily-general-says-900461.

[27] Комплекс РЭБ Мурманск-БН подавит системы управления и связи противника на дальности до 5000 км! [EB/OL]. 2016(2016-10-27) [2020-02-24]. https://nampuom-pycu.livejournal.com/193410.html.

[28] 张柏开, 朱卫纲. 对多功能相控阵雷达干扰决策方法综述[J]. 兵器装备工程学报, 2019, 40(9): 178-183.
Zhang B, Zhu W. Overview of jamming decision-making method for multi-functional phased array radar [J]. Journal of Ordnance Equipment Engineering, 2019, 40(9): 178-183.