doi:10.3969/j.issn.1001 - 893x.2013.09.024

网电空间下的数据链对抗技术及发展趋势*

霍元杰**

(中国西南电子技术研究所,成都 610036)

摘　要:针对美军网电空间战略构想中提出的作战空间和作战模式的变化,提出了发展数据链对抗技术的必要性,介绍了美军对抗技术的发展现状,分析了数据链对抗系统的组成,探讨了数据链对抗的发展趋势和涉及的主要关键技术。相关研究对提升部队未来对抗能力有重要意义。

关键词:网电空间;数据链对抗;网络攻防

中图分类号:TN97　　**文献标志码**:A　　**文章编号**:1001 - 893X(2013)09 - 1243 - 04

Technology and Developing Trend of Datalink Countermeasure in Cyberspace

HUO Yuan-jie

(Southwest China Institute of Electronic Technology, Chengdu 610036, China)

Abstract: According to the change of U.S. Army's operation pattern caused by Cyberspace strategy, the necessity of datalink countermeasure technology is provided. Then current situation of communication countermeasure is introduced. And the composition of datalink countermeasure system is analyzed. Finally the developing trend and key technology are provided. The research in this paper is meaningful for improving future countermeasure ability of military forces.

Key words: cyberspace; datalink countermeasure; network attack-defense

1　引　言

随着美军网电空间作战概念的提出,产生了许多新的作战理念和新的作战对抗方法。近年来美军已发布了《网电空间作战国家军事战略》和《美国空军网电空间司令部战略构想》等发展构想和作战条令[1-2]。在 IEEE 2012 军事通信(MILCOM 2012)会议上,涉及网电空间对抗及安全性的主题数量最多,可见网电空间对抗将是未来军事作战中的重要发展趋势。美军在网电空间对抗中明确涵盖了数据链系统。数据链系统在实现战场指挥控制、态势感知、武器协同等方面具有重要的作用,各作战平台及装备对数据链系统的依赖性越来越强。可以预见,在未来的信息化作战中,增强对战场网络的"制网络权"是体系化作战中的重要任务,数据链系统也必然成为攻防双方对抗的焦点。

2　需求分析

现代战争将是以信息优势为基础,夺取信息优势已成为现代战争中取得决策优势、军事优势和赢得战争胜利的关键,所以各国无不都在大力研制、开发用于信息战的装备,以便阻止或破坏敌对方获取和利用信息的能力。

美军 C4ISR 信息化系统实现了从单平台独立作战到多平台协同作战以及从各军兵种独立作战到多军兵种联合作战的转变。数据链系统是 C4ISR 系统的主要通信传输方式,通过数据链可以实现从传感器到作战平台、再到武器系统之间的信息流动,实现

* 收稿日期:2013 - 08 - 02;修回日期:2013 - 08 - 31　Received date:2013 - 08 - 02;Revised date:2013 - 08 - 31
** 通讯作者:acuteleopard@qq.com　Corresponding author: acuteleopard@qq.com

作战全过程、全要素的无缝连接。自 20 世纪 50 年代开始,针对战争样式的变化,美军为了满足其作战需求,发展了一系列专用和通用的数据链,主要包括指控数据链(Link-11、Link-16 和 Link-22 等)、武器协同数据链(IFDL、MADL、TTNT 等)和宽带数据链(CDL 系列)。数据链系统已成为 C4ISR 系统赖以存在和发挥效能的关键,但又是 C4ISR 系统中最易暴露的薄弱环节。因此,研究数据链对抗技术是实现 C4ISR 体系对抗的重要组成[3]。

目前国内已经开展了部分针对数据链对抗的研究,但主要采用的还是传统的功率压制的方式进行干扰。通过功率压制进行数据链对抗,干扰效率低、干扰功率分散。若采用宽带阻塞式干扰,还存在己方数据链通信也会受到干扰等问题。同时,由于美军在设计数据链系统时充分考虑了其抗干扰能力,数据链装备的抗干扰性、信号抗截获能力等战技指标得到了不断的改善。如 Link16 系统采用了高速跳频、直接序列扩频、MSK 调制的组合调制体制,而且采用了 RS 编码、交织等多层纠检错编码体系,使系统具有很强的抗干扰性能。TTNT 主要采用了跳频跳时技术,使用了一种将扩频、编码、调制相结合的高维网格编码,接收端所需的信噪比较低,并且兼具纠删和纠错功能。同时,TTNT 为了增强抗干扰能力,还采用了频谱感知技术,能够剔除掉被干扰的频点,因此仅在信号层对数据链系统进行干扰还无法满足未来的作战效能要求[4]。

随着数据链通信技术的快速发展,数据链对抗装备必须有革命性的变化,传统信号层功率压制的干扰方式已不能满足未来发展要求,需要从仅进行信号层对抗向信号层、链路层、网络层和信息层综合对抗发展,因此有必要在传统通信对抗的技术基础上,针对外军数据链发展现状,发展专业化的数据链系统对抗装备。

3 美军对抗能力现状

数据链对抗技术是伴随着数据链技术的发展而出现的,由于数据链系统主要特点是通过无线信道实时传输和处理格式化战术信息数据,因此美军数据链对抗是在传统的通信对抗基础上发展而来,并在不断研究和探索在网络、信息的层面实现数据链对抗。

3.1 美军通信对抗概况

美军的通信对抗装备主要朝着大功率、宽频带,以及多平台、一体化的方向发展,归纳起来通信对抗技术装备的发展有如下两个特点。

(1)通信侦察动态范围大,精度高,情报共享能力强

美军通信侦察测向系统具有大动态范围、高灵敏度、低相位噪声和宽瞬时带宽的特点,能在密集的信号环境下实现对通信信号的截获、情报收集分析、测向定位和报告等功能。目前美军具备通信侦察频率为 0.5 ~ 2 000 MHz,测向频率为 0.1 ~ 2 000 MHz,测向精度一般为 1°,甚至更高。灵敏度一般在 - 80 ~ - 110 dBm,能接收多种调制方式的通信信号。RC-135 系列飞机是典型的美空军信号侦察飞机,其任务是电子信号和通信信号情报搜集,为战区和国家级用户提供近实时的情报搜集、分析和分发能力。RC-135 飞机侦收和测向设备的工作频段为20 MHz ~ 40 GHz,能够探测、定位和监视低功率通信信号,在10 km高度可侦测到 600 ~ 800 km距离内的电台信号。经过 RC-135 处理的情报数据可以通过战术数字信息链 TADAL-A 或战术信息广播业务(TIBS)传给战区内的 AWACS、Joint STARS 或其他飞机,也可以将获取的信息传给地面防空或其他指挥部门。

(2)通信干扰样式多,功率大

通信干扰装备普遍采用大功率、宽频带干扰机,具有可编程可配置功能,可同时干扰多个目标的能力。采用数字化处理和计算机控制,可全自动工作,能及时对付新出现的威胁目标。美军目前通信干扰系统的频率范围是 2.0 ~ 2 500 MHz,可上扩到 8.4 GHz,几乎覆盖了现役通信装备的全部工作频段。EC-130H 是美空军的大功率通信干扰飞机,主要用来干扰军事通信设施装备,其干扰系统工作频段 20 ~ 1 000 MHz,干扰功率 5 ~ 10 kW,波瓣宽度为方位角 20°、俯仰角 60° ~ 90°。

3.2 美军网络对抗概况

美军近年来非常重视发展网络侦察对抗能力,利用天基、空基、陆基、海基等多种侦察平台,形成网电一体的侦测体系,大幅度提高了目标精确指示能力,具备了精确对抗能力和网电一体战能力。

美军提出的新概念侦察设备“网电飞行器(Cybercraft)”,可发现、定位、跟踪、监视网电空间中潜在的目标。舒特系统是目前美军报道的典型网络对抗系统,它是一种机载网络攻击系统,通过 NCCT 实现网络战能力。舒特将 ISR 平台(RC-135V/W“联合铆钉”飞机)、进攻性反信息作战平台(EC-130H“罗盘呼叫”飞机)和进攻性防空作战平台(F-16CJ 飞机)进

行横向一体化集成,利用电磁频谱域和网络域的综合攻击能力,结合情报信息攻击敌方信息网络,能够入侵敌防空雷达网和通信网络[5]。

舒特机载网络攻击系统首先由 RC-135U/V/W 侦察飞机通过 NCCT 系统,对敌方辐射源进行信号和信息侦察和高精度定位,对侦收到的各类信号参数和信息进行分析、识别、处理,然后将有关信息传递给地面指控中心。同时通过 NCCT 将目标信息传递给 EC-130H,由 EC-130H 向敌方雷达或通信系统的天线发射电子脉冲信号。这些电子脉冲信号没有采用压制性的“噪声”干扰敌方的通信设备,而是向敌方脆弱的通信节点植入定制的信号和数据,包括虚构目标信息、专业算法和恶意程序等[6]。

由上可看出,由于数据链无线通信的开放性,使得对数据链系统的攻击比对有线通信系统的接入和攻击更容易。美军对数据链的攻击方式,从连续阻塞干扰攻击转向精确灵巧攻击,从噪声压制向信息篡改和诱骗发展,从“监网”到“瘫网”、“骗网”甚至到“控网”,数据链对抗方式发生了重要转变。

4　数据链对抗系统分析

数据链对抗的基本任务是通过陆、海、空各种平台的侦察系统,搜索截获、检测处理、测向定位、分析识别和记录储存相关数据链目标的信号情报,能够对数据链目标进行干扰和网络攻击,破坏敌方通过数据链对信息的传输、交换和利用,降低其作战能力。

4.1　数据链侦察技术

数据链侦察技术是指截获、分析、识别敌方数据链信号的能力。截获目标信号是进行测量、分析、识别的基础,在设计数据链侦收系统时,需要考虑天线方向、极化形式、频率覆盖范围、灵敏度等因素。数据链信号分析与识别主要是通过测量提取目标信号的外部特征参数,识别出目标信号,并判断其属性、威胁等级等信息,提供给对抗系统。侦察系统多采用全向高增益天线、宽带接收机和高速信号处理器件,具有强大的截获与分析处理能力。

4.2　数据链对抗技术

数据链对抗技术是指根据侦察获取信息,干扰、攻击敌方数据链网络。若采用干扰方式则与干扰功率、干扰方式、干扰天线增益、干扰/通信距离比等因素有关;若采用网络攻击方式,则与传输体制、组网协议、消息格式等有关。目前主要干扰方式有全频带干扰、跟踪瞄准式干扰、单音干扰等。随着功率合成技术、定向干扰天线等新技术与器件的发展,干扰设备的干扰能力也不断提高。网络攻击方式需要更多的对抗参数信息,需要平时的情报侦察支持和对数据链技术体制的充分掌握,分析敌方所采用的传输波形、组网协议,针对其存在的薄弱环节进行网络攻击。

4.3　数据链对抗方式

传统的通信对抗采用点对点的信号对抗方式,随着数据技术的不断发展,数据链系统已经形成了网络体系。因此,数据链对抗不仅面对链路的点对点通信系统,而且将主要面对多节点、多路由、多链路、多频段的数据链通信网络,只对个别或部分通信设备的干扰并不能使数据链网络体系瘫痪。数据链对抗系统除了传统通信对抗中的针对链路的信号对抗外,还将越来越多的承担破坏敌方信息网络体系的职责,提供基于网络的对抗方式,这也是数据链对抗区别于传统通信对抗的重要标志。

5　发展趋势探讨

5.1　数据链对抗是未来高技术战争中体系对抗的重要环节

在现代战争中,信息化网络系统日趋成熟,使体系对抗成为现代高技术战争的基本特征。体系对抗的核心就是保障己方的信息化系统发挥正常效能,破坏或干扰对方的信息化系统。数据链作为重要的信息化系统,针对数据链的攻防对抗将是体系对抗的重要环节。随着外军数据链技术的不断发展,开展数据链对抗技术的研究成为必然趋势。

5.2　数据链系统的不断完善和发展促使需要专业化的数据链对抗装备

美军已装备的数据链混合利用了多种通信抗干扰技术,采用了跳频、直接序列扩频、跳时及混合式的抗干扰通信,使用了 TDMA、FDMA、SPMA 等组网方式,并采用了自适应调零天线、软件无线电及数字波束等新技术。目前的通信对抗手段很难对数据链实现有效的干扰,若采用传统的通信对抗手段,通信对抗装备不得不不断提高功率,导致对抗的代价不断增加。而专业化的数据链对抗装备的目标更加有针对性,通过分析目标数据链系统信号、波形、协议特征,采取综合化的对抗设计,具备更加灵巧和智能化的特点,对抗效能大幅提高。

5.3　网电一体化下的综合对抗模式将是数据链对抗的主要发展方向

综合化的对抗模式实施的是系统对抗,既注重

对通信链路的信号对抗,更着眼于破坏或削弱数据链网络化的通信能力,体现了网络对抗态势,基于波形、协议的一体化对抗模式将逐渐趋于主要地位。随着数据链通信网络化程度的不断提高,仅干扰掉部分链路,并不能使数据链网络失效,需要综合运用电子战和网络战两种手段,进行一体化作战,才能达到有效对抗的目的。网电一体战是从链路对抗向系统对抗、从系统对抗向体系对抗发展的重要方向。

5.4 数据链技术水平将是影响数据链对抗设计的关键因素

传统的通信对抗只需要获取目标的信号特征,而未来的数据链对抗除了需要获取目标信号特征外,还需要更多的对目标传输波形、组网协议等通信体制的了解。而这些信息密级程度高,通常很难获取,只能通过情报支持等获取部分参数,更多的是需要对其体制的分析,寻找对抗目标的薄弱环节,为数据链对抗手段的设计奠定基础。

6 关键技术分析

(1)数据链对抗系统的总体设计

数据链对抗系统性能首先取决于总体设计的优劣,因此首先应加强数据链对抗系统总体技术的研究,包括从需求出发,针对不同的对抗目标的特点,从总体角度出发综合考虑侦察、测向、信息情报处理、对抗方案设计等内容。根据目标特点和所掌握的技术资料,进行最有效的数据链对抗总体设计。

(2)非合作目标信号侦察和识别技术

数据链对抗的目标是非合作性目标,对其侦察和识别具有较大的技术难度。特别是对采用了跳频、扩频、跳时以及定向波束、功率控制等射频隐身等技术体制的信号,只有不断加强对数据链通信信号的研究,提升数据链通信信号侦察和识别能力,才能为数据链对抗奠定基础。

(3)数据链网络薄弱环节分析

数据链薄弱环节分析通过对特定数据链系统的传输体制、组网协议、拓扑结构、使用流程的分析,得到其存在的薄弱环节。数据链网络在逻辑功能上的相对稳定性,提供了从网络功能角度进行网络薄弱环节分析的可能性。目前,数据链系统主要采用了轮询、FDMA、TDMA、SPMA 等协议,针对不同网络协议的局限性,应深入挖掘组网协议、传输波形等存在的漏洞,针对性地找到数据链对抗的最佳方法。

(4)数据链网络攻击技术

根据目标信号的时域、频域或空域的多种特征参数以及波形、协议的设计原理,借助情报信息,研究针对不同数据链的网络攻击技术,破坏敌方数据链信息的传输、处理和网络管理过程,使其数据链网络无法协调运转,从而大大降低其整体作战能力。

7 结束语

网电空间将是未来一个新的作战领域,数据链系统是网电空间中重要的组成,数据链对抗将成为未来网电空间作战的重要样式。数据链系统对抗难度大、密级高,可参考的数据链对抗资料较少。国内也还处于初步研究阶段,需要进行不断探索研究。数据链对抗未来将越来越多地承担着侦察、干扰、攻击敌方作战信息网络体系的职责,因此在网电空间对抗环境中,持续深入地研究数据链对抗技术对提升部队未来体系对抗能力具有重要意义。

参考文献:

[1] Bush G W. The National Strategy to Secure Cyberspace[R]. Washington DC: The White House, 2003: 3 - 7.

[2] Chairman of the Joint Chief of Staff. National Military Strategy for Cyberspace Operations[EB/OL]. Washington DC: Chairman of the Joint Chief of Staff, 2006.

[3] 李子富. 全球信息栅格及其对抗策略[J]. 杭州电子科技大学学报, 2010, 30(5): 137 - 140.
LI Zi-fu. Global Information Grid and Its Countermeasure[J]. Journal of Hangzhou Dianzi University, 2010, 30(5): 137 - 140. (in Chinese)

[4] 翟利超,吕久明. 数据链及其对抗方法研究[J]. 舰船电子对抗, 2004, 27(6): 26 - 29.
ZHAI Li-chao, LU Jiu-ming. Study of Data Link and Its Countermeasure[J]. Shipboard Electronic Countermeasure, 2004, 27(6): 26 - 29. (in Chinese)

[5] Department of Defense. Report to Congress: NetworkCentric Warfare[R]. Washington DC: DoD, 2005.

[6] 赵敏. 网络中心战的网络攻击 - Suter 计划[J]. 现代防御技术, 2011, 39(6): 139 - 143.
ZHAO Min. Network Attack of Network Centric Warfare: Project Suter[J]. Modern Defence Technology, 2011, 39(6): 139 - 143. (in Chinese)

作者简介:

霍元杰(1970 -),男,湖北武汉人,高级工程师,主要研究方向为航空通信与电磁兼容。

HUO Yuan-jie was born in Wuhan, Hubei Province, in 1970. He is now a senior engineer. His research interests include aviation communication and electromagnetic compatibility.

Email: acuteleopard@qq.com