第 31 卷第 10 期 强 激 光 与 粒 子 束 Vol. 31, No. 10
2019 年 10 月 HIGH POWER LASER AND PARTICLE BEAMS Oct., 2019

网电对抗下的复杂电磁环境再认识*

唐朝京

(国防科技大学 电子科学学院, 长沙 410073)

摘 要: 分析了复杂电磁环境的主要因素,阐述了网电攻击造成的复杂电磁环境,深入分析了这种欺骗式复杂电磁环境可能对预警雷达造成的危害,并探讨了加强雷达预警系统网电安全的防护措施,提出了关于网电对抗下复杂电磁环境的三点思考。

关键词: 复杂电磁环境; 雷达预警系统; 网电对抗; 网电防护

中图分类号: TN97 **文献标志码:** A **doi:**10.11884/HPLPB201931.190248

Recognition of complex electromagnetic environment under cyberspace countermeasures

Tang Chaojing

(*College of Electronic Science and Technology, National University of Defense Technology, Changsha* 410073, *China*)

Abstract: This paper presents the characteristics of complex electromagnetic environment, introduces the more complex electromagnetic environment under cyberspace countermeasures, analyzes the attack on early warning radars by hazards deception jamming in complex electromagnetic environment in detail, and discusses the protective measures to strengthen cyberspace security of radar warning system. In addition, it puts forward three points of view about relations of cyberspace countermeasures and complex electromagnetic environment.

Key words: complex electromagnetic environment; radar early warning system; network electric countermeasure; net electric protection

PACS: 84.40.Xb; 84.40.Ua

1 复杂电磁环境概述

复杂电磁环境是指在一定的时空和频段范围内,多种电磁信号密集、拥挤、交叠,强度动态变化,对抗特征突出,可对信息化设备、电子信息系统和信息化行动产生严重影响的电磁环境[1-6]。从其定义可较好地解释复杂电磁环境的特点和可能对电子设备、电子信息系统造成的影响。但从更宽的角度看还存在两点不足:(1)未强调欺骗干扰,传统理解的对抗就是压制式干扰;(2)未强调电磁信号中所包含的目标信息。

电磁环境看不见、摸不着,首先需要感知到。电磁环境的感知需要借助于频谱仪、场强计等电子测量仪器,雷达也是一种特殊的电磁环境感知器。电磁环境感知的过程中若受到网电攻击,感知到的就有可能是虚假的电磁环境,例如 20 世纪 90 年代出现在华东地区的不明空情。1994 年 10 月,我国东部地区的许多警戒雷达屏幕上突然出现大批高度逼真的空中目标回波,引起高层的极大关注,事后分析判明是某国航母上放飞的无人机发出的精确电子干扰。这是电磁环境感知过程中被人做了加法。

电磁环境感知还可以被做减法。例如发生在中东地区的"果园行动":2007 年 9 月 7 日凌晨,以色列空军 69 中队深入叙利亚腹地几百 km,轰炸了叙利亚的疑似核设施,完事后扬长而去,而叙防空雷达对此竟然毫无察觉。这次行动引起了全世界的高度关注,纷纷猜测以色列使用美国研发的网电对抗武器"舒特系统"对叙利亚的预警雷达实施了网电攻击。

舒特系统是美军在网络中心战思想指导下研发的侦察/打击一体化的作战网络,目标是将情报、监视、侦察与进攻性信息作战、进攻性防空作战横向一体化集成。舒特系统从 2003 年开始研发,迄今已发展了六代,其中第二代舒特系统具备控制敌方网络、操控敌方雷达的功能,正好符合以色列"果园行动"的作战场景。

* **收稿日期:**2019-06-29; **修订日期:**2019-07-17
作者简介:唐朝京(1962—),男,教授,博导,从事电磁信息安全、电对抗方面研究; tangchaojing@nudt.edu.cn。

因此，可以对“果园行动”现象做出这样的合理解释：第一，以色列网络战部队事先入侵了叙利亚防空雷达网，在叙雷达计算机中预埋了攻击程序；第二，空中突防时以色列的机载舒特 II 系统对叙利亚防空警戒雷达实施无线注入，发出攻击启动命令；第三，隐藏在叙雷达计算机中的攻击程序接收到攻击启动命令后，将飞机回波消隐，致使雷达对入侵目标视而不见，帮助以战机实现无感突防。

这一过程综合采用了电子战、网络战和情报战手段，看似很神奇，但从原理上讲是完全可能的。

2 雷达可能遭受的网电攻击

2.1 雷达预警系统的一般结构

图 1 为雷达预警系统一般结构图。雷达预警系统的工作过程是：预警雷达探测到空中目标后将目标方位、距离、高度、航迹等信息显示在雷达屏幕上，同时将探测数据经由网络上传到雷达情报融合中心，情报中心经过融合处理后得到整个区域的目标雷达情报态势，并报告上级指挥所。其中雷达情报网络历经几代发展，现已形成以光纤/微波为主要传输媒介的 IP 化的物理隔离网络，再加上传输加密、入侵检测等防护措施，构成了一个具有很强安全防护能力的军事信息网络。

攻击方为了进行无线攻击而预先入侵防护严密的雷达情报网是否有必要呢？回答是：绝对必要！无线注入本质上是一个通信问题，有发还要有收，而且收发两端还需使用统一的协议，否则接收方无法理解无线注入信号的含义。

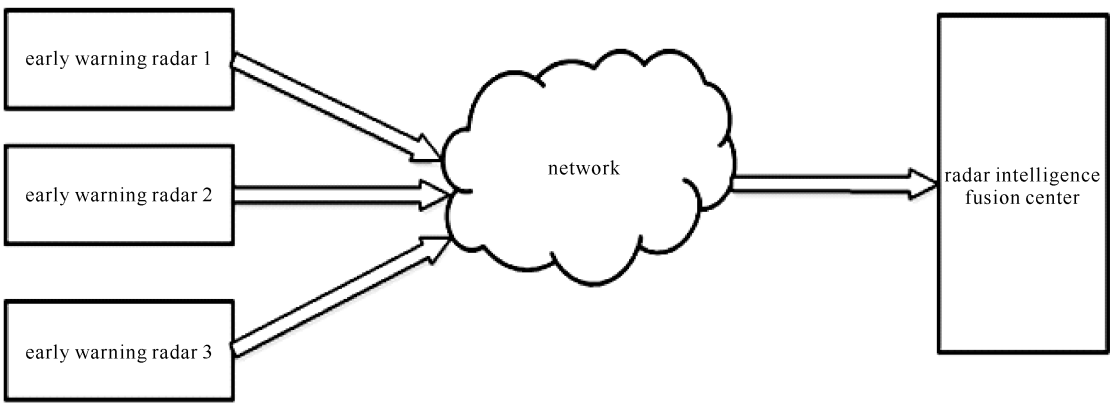

Fig. 1 Structure diagram of radar early-warning system

图 1 雷达预警系统一般结构图

预警雷达接收系统的一般结构如图 2 所示。其中天线射频单元负责接收雷达回波并作相应的频率变换；主控计算机负责管理雷达信号处理等实时过程；显控计算机通过内部局域网联到主控计算机和雷达情报网，负责显示目标回波和航迹、操控雷达系统，并上传目标雷达数据。

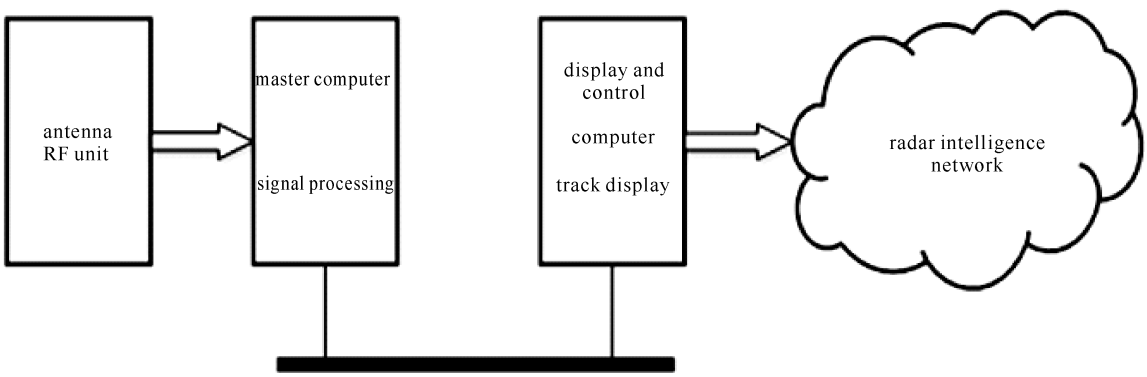

Fig. 2 Structure diagram of early warning radar receiving system

图 2 预警雷达接收系统一般结构图

2.2 对预警雷达的网电攻击过程

对预警雷达系统的网电攻击原则上可分为如下三步。第一步：入侵雷达情报网，攻占雷达计算机，预埋攻击程序；第二步：突防飞机按约定进行无线注入，发出攻击开始命令；第三步：预埋的攻击程序对雷达实施目标

消隐，或其他干扰。

2.2.1 攻占主控机后可能的无线注入方式

飞机向雷达发射特殊编码的信号，攻击程序通过实时分析雷达接收信号即可获知攻击启动，随即进行相应破坏。通过无线注入还可加载新的代码，及时更新攻击程序版本。

2.2.2 攻占显控机后可能的无线注入方式

攻击程序可获知雷达屏幕显示的内容，若突防飞机发出一特殊干扰图样，或做一特殊动作（如飞一个三角形），攻击程序通过屏幕显示即可获知攻击启动，随即进行相应破坏。

2.3 可能取得的攻击效果

对飞机回波和航迹进行消隐；控制天线转动方向；关闭雷达抗干扰模块；对雷达实施欺骗式干扰；向情报融合中心发送虚假雷达情报；控制雷达脉冲的通断；强迫雷达关机，等等。

2.4 网电攻击预警雷达所需要的条件

对预警雷达系统的网电攻击需要满足非常严苛的条件：1）能入侵严密防守、物理隔离的雷达情报网；2）能掌握雷达系统的详细技术情报；3）特殊的电子干扰技术；4）高效的网络攻击载荷。

上述四个条件都很苛刻，特别是前两项难度更大。但这些困难并不是不可克服的，相对于攻击所能取得的巨大效果，这些困难完全值得花大力气去克服！

3 雷达预警系统如何防护网电攻击

认识到雷达预警系统可能遭受的网电攻击威胁，防护问题就相对简单了。

3.1 监视雷达回波信号中的异常变化

若雷达受到无线注入攻击，接收信号必然会出现异常。防守方可对雷达接收信号进行实时检测，一旦发现异常立即报警。

3.2 监视雷达计算机活跃进程的异常行为

恶意程序侵入计算机后先要把自己隐藏在内存某个角落，再修改操作系统的自动加载项，以便每次开机都能被加载成为常驻内存的活跃进程，并实施相应破坏。防守方可通过检测雷达计算机进程的种种异常行为发现恶意程序，并加以清除。

3.3 沙箱检测网络流量中可能的漏洞利用代码

恶意程序一般都是利用软件漏洞入侵计算机系统的，防守方可以采用沙箱技术检测漏洞攻击。沙箱非实时地检测输入数据包对运行中的特定软件产生的影响，若发现程序控制权有异常变化，就表明可能发生了漏洞攻击。

3.4 雷达系统程序采取加密校验防篡改

恶意程序若要篡改雷达屏幕显示信息，就必须先更改雷达系统软件的代码或数据。防守方可对雷达系统进行加密校验，不掌握正确密钥就无法更改雷达软件，以此阻止恶意程序对雷达系统的篡改。

3.5 加强网络和主机的常规安全防护

恶意程序入侵网络往往都是利用防守方的一些疏忽趁虚而入的，加强常规安全检查可以尽可能地破坏攻击方的入侵机会。

3.6 采用自主可控芯片和基础软件杜绝后门

这是确保从源头上消除可能的系统后门危害。

3.7 强化防间保密工作

针对雷达预警系统的网电对抗需要掌握雷达的详细技术情报，因此做好防间保密工作尤为重要。

4 几点认识

4.1 网电对抗使复杂电磁环境更加复杂

电子干扰是导致电磁环境复杂的重要因素，可造成对抗性复杂电磁环境。按照传统的理解主要关注大功率、宽频带、压制式干扰造成的复杂电磁环境，实际上，欺骗式干扰同样是造成电磁环境复杂的重要因素。网电对抗可使复杂电磁环境笼罩上一团迷雾，在传统复杂性之上又增加了一层不确定性，使电磁环境从多和少的复杂性扩展到了真和假的复杂性。

4.2 网电对抗扰乱了对电磁环境的正确认知

网电对抗造成的欺骗式电磁环境影响的是人们对复杂电磁环境的正确认知。典型网电对抗的作用是从物理域到信息域再扩展到认知域;基于网电对抗的欺骗式复杂电磁环境直接从物理域影响到了认知域。作为对比,常规电子攻击则是通过破坏物理域来阻断信息域。

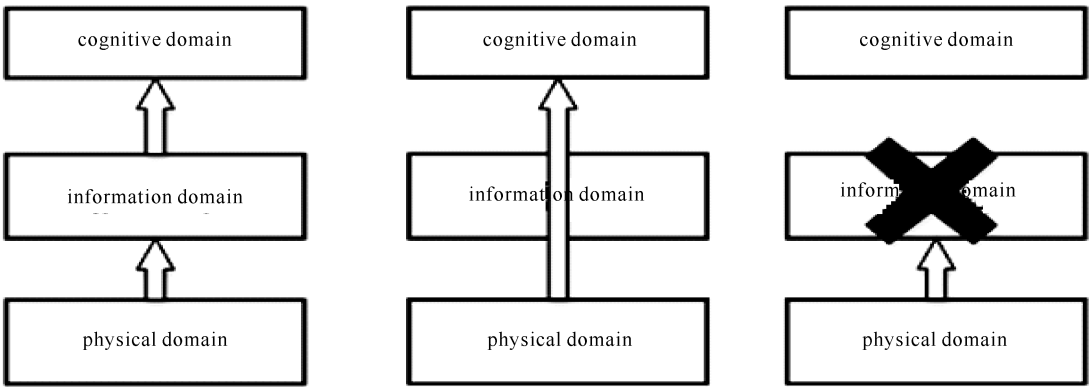

Fig. 3 Relations between network electrical countermeasure, electronic countermeasure and cognitive domain, information domain and physical domain

图 3 网电对抗、电子对抗与认知域、信息域和物理域之间的关系

4.3 破除复杂电磁环境迷雾要靠网电一体

在网电对抗条件下,欺骗式复杂电磁环境的危害性可能是难以估量的。只有采取网电一体的方法,从电磁和网络两个维度双管齐下,切实把住系统安全的网、电关口,才能驱除笼罩在电磁环境上的不确定性迷雾,保证我们的网电空间安全和国土安全。

参考文献:

[1] 刘尚合,孙国至. 复杂电磁环境内涵及效应分析[J]. 装备指挥技术学院学报, 2008, 19(1):1-5. (Liu Shanghe, Sun Guozhi. Analysis of the concept and effects of complex electromagnetic environment. Journal of the Academy of Equipment Command & Technology, 2008, 19(1): 1-5)

[2] 汪连栋,曾勇虎,申绪涧. 电子信息系统复杂电磁环境效应研究路线图 V1.0[M]. 北京:国防工业出版社, 2013. (Wang Liandong, Zeng Yonghu, Shen Xujian. Road map of complex electromagnetic environment effect research in electronic information system—V1.0. Beijing: National Defense Industry Press, 2013)

[3] 王洁. 面向服务的复杂电磁环境电磁态势可视化[D]. 南京:南京理工大学, 2015. (Wang Jie. Service-oriented visualization of electromagnetic situation in complex electromagnetic environment. Nanjing: Nanjing University of Science and Technology, 2015)

[4] 赵刚,郑生全,侯冬云,等. 应对复杂战场电磁环境的舰船防护设计[J]. 河北科技大学学报, 2011, 32:148-153. (Zhao Gang, Zheng Shengquan, Hou Dongyun, et al. Ship protection design for complex battlefield electromagnetic environment. Journal of Hebei University of Science and Technology, 2011, 32:148-153)

[5] 徐永成,罗日荣,陈循,等. 复杂电磁环境下装备损伤模式与保障问题研究[J]. 国防科技, 2008, 29(4):27-33. (Xu Yongcheng, Luo Rirong, Chen Xun, et al. A study on material damage mode and integrated support under complicated electromagnetic environment. National Defense Science & Technology, 2008, 29(4):27-33)

[6] 张良,祝欢,杨予昊,等. 机载预警雷达技术及信号处理方法综述[J]. 电子与信息学报, 2016, 38(12):3298-3306. (Zhang Liang, Zhu Huan, Yang Yuhao, et al. Overview on airborne early warning radar technology and signal processing methods. Journal of Electronics & Information Technology, 2016, 38(12):3298-3306)