“舒特”计划对指挥控制系统的影响及对策研究

刘建强[1]，郭诗军[2]，孙德军[3]，刘养科[1]，倪发军[1]

（1.防空兵学院 郑州 450052；2.71521 部队信息化处 453000；3.信息工程大学 450001）

摘要：“舒特”计划是美军高度机密的“庞大旅行者计划”的一部分。本文介绍了“舒特”系统的构成及可能的攻击原理，分析了其对指挥控制系统的影响，并提出了相应的对策。

关键词：指挥控制系统　对策　“舒特”计划

0 引言

“舒特”计划是美军高度机密的“庞大旅行者计划”的一部分，是网络中心战的组成部分，近期是发展机载网络攻击系统，远期是发展美国空军的网络攻击系统[1]。近期的机载网络攻击系统，由BAE系统公司负责研发，目标是入侵敌方通信网络、雷达网络以及计算机系统，尤其是那些与联合防空系统有关的系统[2]。美军“舒特”攻击系统发展至今，已有“舒特I”、“舒特Ⅱ”、“舒特Ⅲ”、“舒特Ⅳ”和“舒特Ⅴ”5代，并在2000年、2002年、2004年和2008年的两年一度的“联合远征部队试验”(JEFX)中进行了技术能力演示[3，4]。本文在分析该系统可能的攻击原理基础上，对指挥控制系统的威胁和对策进行了研究。

1 典型“舒特”系统的构成及攻击原理

（一）典型“舒特”系统构成[5]

典型的“舒特”机载网络攻击系统由 RC-135U/V/W 电子侦察飞机、EC-130H 专用电子战飞机或 EA-6B 等普通电子干扰飞机和 F-16CJ 战斗机组成。其中电子侦察飞机负责信息获取，电子战飞机主要负责对敌方信息系统进行软打击，包括电子干扰和恶意信息输入等，而战斗机则负责对敌方信息系统进行硬打击，从实体上进行摧毁。

（二）“舒特”系统攻击原理[6]

军事网络中大量无线技术的使用，使得薄弱环节越来越多，渗入敌防空系统网络就有通过无线传感器、无线通信系统、无线通信链路、无线中继链路等途径进入信息处理设备和网络节点。“舒特”系统正是以敌方电子信息系统中薄弱的雷达、通信系统的天线为入口，渗透进入敌方的防空网，实施网络攻击。

装备“舒特”系统的飞机至少要加装“长矛”吊舱和“豹穴”软件。其中，“长矛”吊舱是一种功率强大的专用辐射源阵列，“豹穴”则是一种实施网络入侵的算法／程序。这样，实施攻击时，就能通过“长矛”吊舱发射大功率信号，渗透进敌方网络，然后根据具体攻击战术，采取以下措施：产生假目标；引导雷达在错误方向上搜索；用假目标或信息“淹没”其系统；迫使其系统转换工作模式；植入算法软件包，控制其网络并操纵其雷达转动。

由于美国军方对“舒特”系统严加保密，其攻击过程只能进行推理如下：

第一步,对目标实施电子侦察,主要是通过使用 RC-135U/V/W 电子侦察飞机在敌防空区外进行信号和信息侦察，及时掌握敌方防空体系的无线电联络内容并进行实时破译。如果发现不能实时破译的密码，立即通过全球信息系统送到美国国家安全局，对收到的各类信号参数和信息进行分析、识别、处理，然后将破译后的有关信息传递给地面指控中心。

第二步，地面指控中心根据作战目的选择攻击方式。如果是要对目标实施软打击，则通过数据链路将目标信息传递给 EA-6B、EA-18G 等电子战飞机后，由其对预定目标实施电子干扰；如果要对目标实施硬打击，则通过数据链路将目标信息传递给 F-16CJ 或其他战斗机，由其对预定目标实施精确火力打击；如果要接管敌方网络，则通过数据链路将目标信息传递给 EC-130H 专用电子战飞机，由其对预定目标实施网络战攻击。

第三步，实施网络攻击。当地面指控中心决定实施网络攻击时，首先由 RC-135U/V/W 电子侦察飞机通过网络中心目标瞄准系统，对敌方辐射源进行高精度定位，然后由 EC-130H 专用电子战飞机向敌方雷达或通信系统的天线发射电子脉冲信号。与传统的电子干扰或电磁脉冲攻击不同的是，这些电子脉冲流不是使用过载的“噪音”或能量淹没敌电子设备，而是向敌人脆弱的处理节点植入定制的信号，包括专业算法和恶意程序，巧妙渗入敌方防空雷达网络，或窥测敌方雷达屏幕信息，或实施干扰和欺骗，或冒充敌方网络管理员身份接管系统，操纵雷达天线转向，使其无法发现来袭目标。

2“舒特”系统对指挥控制系统的主要影响

从“舒特”系统攻击原理可以看出，其主要利用无线电信道进行入侵，进而攻击敌方系统。其对防空指挥控制系统的影响主要有以下几个方面：

一是压制警戒雷达，制造警戒盲区，从而缩短预警时间。

根据“舒特”系统电子侦察得到的敌方目标准确的情报信息，采取高强度、宽频域的瞄准式、拦阻式等干扰样式对目标实施干扰压制，甚至直接实施反辐射攻击或精确的火力打击对目标进行摧毁，从而使敌方的警戒雷达功能减弱甚至失效，达成缩短预警时间的目的。

二是入侵网络系统，接管网络权限，扰乱指挥控制

“舒特”系统对指挥控制系统实施网络攻击时，主要以空间电磁波为载体，以敌方预警雷达、微波中继站、数据链地面站等电子信息系统的天线为入口，利用包括专门算法和恶意程序的特制信号，渗透进入其指挥控制系统，通过值入“木马”“蠕虫”病毒，发送虚假消息，修改系统参数等方式，取得控制权限或瘫痪其指挥控制系统，进而扰乱敌方防空雷达系统，达到突袭目的。。

三是打击重要节点，实体摧毁系统

“舒特”系统攻击效能的发挥，首先依赖高精度快速辐射源定位技术为空军提供攻击目标的详细信息。只有通过电子侦察手段摸清敌方指挥信息的组成以及具体分布情况，才能为“舒特”系统实施软、硬攻击提供目标指示。当软打击不足以达到效果，或者无法破译其相关信息时，可以对敌方相关重要节点实施硬打击，从实体上加以摧毁，从而使敌方的体系破解，大辐降低其体系战斗能力。

3 指挥控制系统应对“舒特”系统的主要对策

（一）加强系统网络安全防护技术能力

从“舒特”系统攻击方式来看，指挥控制系统将受到无线注入的网络攻击。提高指挥控制系统网络安全防护能力要从以下几个方面入手：一要深化对“舒特”攻击的认识，加强指挥控制系统保障人员的安全防护意识和能力。二要为指挥控制系统加装一体化的安防设备，打造指挥控制系统的安全防护体系。例如根据各个层次系统安全要求，为系统安装防火墙、漏洞扫描设备、入侵检测设备、防病毒软件等，并及时为软件升级，以提高网络的攻击检测能力、快速恢复能力等。三是要采取各种措施，提高指挥控制系统的无线接入点（如预警雷达、卫星天线、短波电台、数据链等）反“舒特”攻击能力。四要尽量采取安全性更高的联网技术，如有线联网采用光纤，无线联网采用移动自组网和加密技术。五要积极研制具有自主知识产权的计算机核心芯片和操作系统等。

（二）加强系统装备保密工作

在“舒特”系统攻击叙军的报道中称，美国给以军提供了大量的关于俄制防空武器的情报。可见，加强指挥控制系统装备的保密刻不容缓。一是平时要注重对指挥控制系统装备的部署位置、技术体制、工作原理、各种技战术指标的保密；二是在与外军联合军演时做好指挥控制系统装备的保密工作；三是对指挥控制系统装备所用频率进行严格管控，区别常用、备用、隐蔽、战时、平时，做到常、备、隐分离，平、战分离，真正达到管控严格，使用合理，最大限度地保护频谱资源。

（三）加强系统网络安全运用能力

“舒特”系统是建立在强大的信息获取和共享基础之上的。可以说，侦察力量是“舒特”系统发挥战斗力的信息之本。无线节点是进入敌方作战体系的关键，所以加强指挥控制系统无线传感器设备反侦察反干扰能力。一是通过假频率、假信号迷惑敌方电子侦察系统，在作战地域实施高效的电磁频谱管理，减少用频时间，以此减少被敌从分析网络脆弱节点的机会，提高反侦察能力；二是对无线接入点设备进行技术改造，专门研制发展与之相配套的攻击防护、报警告知、定位指示、快速杀毒等性能完备的防护软件，拒绝民用信息，从源头上减少被攻击的可能性。也可以探测到“舒特”系统工作后，对其具体实施网络攻击的单元发射大功率的强电磁脉冲，干扰、削弱、摧毁其远程无线入侵能力。

参考文献：

[l].李耐和.“舒特”-电子战先锋[J].航空知识．2008 (5)：15-17.

[2].张春磊．网络中心的战场网络战-Suter 计划[J].通信对抗，2009 (1)：11-17.

[3].姚红星．温柏华．美军网络战研究[M]．北京：国防大学出版社，2010.

[4].宋新彬．美军网络作战能力建设现状研究[J]．现代军事，2009 (12)：78—81.

[5].穆军林 朱国阳 王江涛. 美军“舒特”系统攻击方式及应对措施[J]. 装备制造技术，2009（9）：131-135

[6]. 赵敏. 网络中心战的网络攻击——Suter 计划[J].2011（6）：139-143