2007年9月6日傍晚，以色列空军第69战斗机中队18架F-16I战斗机，幽灵般地越过边界，沿着叙利亚的海岸线超低空飞行，成功躲过叙利亚军队苦心经营多年的防空体系，对叙方纵深100千米内的所谓“核设施”目标实施了毁灭性突击。此次以色列成功的军事行动举世瞩目，令叙利亚最高层大为震惊，也让俄罗斯颜面扫地，并对广泛购买装备俄制防空武器的国家产生了极大冲击和潜在影响。人们不禁要问，以军如何以F-16I等非隐身飞机突破“道尔”-M1等俄制先进防空武器系统的严密防护，对叙利亚“核设施”目标实施成功空袭的。据有关资料披露，以军制胜的秘诀在于使用了美军的“舒特”攻击系统。那么，“舒特”攻击系统到底是什么，近年来有哪些发展?它的攻击原理又是什么?对购买装备俄制防空武器的国家有哪些警示呢?

一、充满神秘色彩的“黑箱”

“舒特”的名字来自于大名鼎鼎的美国“红旗”演习创立者理查德•穆迪•舒特上校。“舒特”是美国高度机密的“庞大旅行者”计划的一部分，是美军用来攻击敌人网络系统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。

早在2000年1月6日，美空军向国会通报了发展“舒特”网络攻击计划的意向，意在建立一套将情报、监视和侦察(RC-135V／W“联合铆钉”电子侦察飞机)与进攻性反信息作战(EC-130H“罗盘呼叫”电子战飞机)和进攻性防空作战(F-16CJ)横向一体化集成的系统。

2001年7月27日，美国国防部呈交国会的《网络中心战》报告(附件)中首次正式披露了“舒特”计划的相关情况。它指出，“舒特”计划是美国空军实现从传感器到射击器的无缝一体化作战网络计划之一。其目的是实现情报、监视、侦察与进攻性电子压制和进攻性防空作战横向一体化集成。这样，执行侦察任务的传感器平台就通过指挥所与电子压制和打击武器平台连接成一体化的作战网络。一旦发现目标(如移动导弹发射架)，就可以迅速将目标信息传输给电子压制和打击武器平台。根据需要实施电子压制或实施火力打击，从而将信息优势转化为行动优势。

2002年11月4日，美国《航空周刊和空间技术》的一篇报道向世人揭示了“舒特”的存在。报道称，在最新的“舒特”能力演示中，EC-130飞机使用其最新改进的能力渗透到敌计算机系统中，对其进行控制，植入假目标，发布错误消息，甚至操作了敌人的传感器。同年，美国防部要求国会对EC-130“罗盘呼叫”飞机追加资金进行改装，以提高飞机的“舒特”能力，支持伊拉克“自由行动”，“舒特”计划正式曝光。由于“舒特”计划的高度机密性，迄今为止，“舒特”攻击能力的开发、使用和技术手段，对其他国家国防和政府机构仍是充满了神秘色彩的“黑箱”。但据外媒报道，“舒特”可以通过敌方雷达天线、微波中继站、网络处理节点侵入敌方防空网络系统，能够实时监视敌方雷达的探测结果(即攻击方操作员可以获得与敌方雷达探测系统一致的信息，后根据看到的敌方雷达屏幕图像评估其隐身系统或地形遮蔽战术的效能)，甚至能以系统管理员身份接管敌方网络，实现对传感器的控制，注入欺骗信息和处理算法，并能实现对敌时敏目标链路的控制能力。这个过程就好比特工将一座大楼的监控中心的信号源截断而给监视者以虚假的图象，然后把整个大楼掏空，这时的监视保安恐怕连二郎腿都没有放下来。“舒特”还可以控制敌人的雷达，想怎么转就怎么转，自己的飞机连隐身都不需要了。

二、持续升级的美军“舒特”攻击能力

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。联合远征部队试验是美空军进行的旨在探索和评估新的和即将出现的空中力量能力的一系列试验之一。联合远征部队试验在一个真实的作战想定中对所有能力进行验证，并将这些能力与空间作战中心结合在一起，确保所要验证的能力能够真正发挥作用。

JEFX-2000演习中，EC-130H专用电子战飞机、RC-135U／V／W电子侦察飞机和F-16CJ战斗机参加了对“舒特I”系统进行的技术演示。几个机种成功演示了信息平台与攻击平台在几个场景中一起完成了低空飞行，并对目标实施了硬摧毁。演示表明，“舒特I”可以实时监视敌方雷达探测结果，即攻击方操作员可以直接看到的敌方雷达屏幕图像，并据此评估己方作战飞机隐身或利用地形遮蔽的效果。

JEFX-2002演习中，“舒特Ⅱ”系统进行了技术演示。RC-135U／V／W电子侦察飞机在敌防空区外进行信号和信息的侦搜，并及时传递给EC-130H大功率电子干扰飞机实施进攻性信息战。演示表明，“舒特Ⅱ”可以使攻击方人员替代敌方系统操作员，直接控制敌方网络，操作其雷达等传感器设备。

JEFX-2004演习中。“舒特Ⅲ”系统进行演示的主要内容是：通过综合使用情报和高精度快速辐射源定位技术等非协作监视能力，实现入侵敌时敏目标网络(如战场弹道导弹发射架、移动地空导弹发射架)，由多平台通用数据链(MP-CDL)引导F-16CJ战斗机发射反辐射导弹或其他精确制导炸弹对敌雷达和通信设施进行硬摧毁。演示表明，“舒特Ⅲ”可以将上述两种非协作监视能力，通过可入侵时敏目标链路，扩展用于监控战场弹道导弹发射架或可移动的地空导弹发射架等时敏目标。从“舒特I”到“舒特Ⅲ”的发展过程中，可以看出“舒特”能力的两个进步：侦察能力和软件算法能力不断提高。因为欺骗越逼真，则要求侦察越翔实，算法越高明。

2006年，“舒特Ⅳ”系统直接在伊拉克和阿富汗的实战行动中进行了技术性能测试。根据作战需要，“舒特IV"对反叛武装力量和恐怖分子的指挥控制系统的信号特征进行了识别，并将目标信息快速地传输给指挥人员和战斗机机组的能力进行了功能测试。

JEFX-2008演习中，最新版本的“舒特V”系统进行了技术试验。“舒特V”是目前唯一、也是第一个能满足空军临时网络司令部(Cyber Command)任务需求的项目。该项目能提供战术信息战场空间的联合视图，以便同时使用动能武器、非动能武器以及进行ISR(情报、侦察、监视)作战来对付移动的、组网的敌方信息网络系统。据报道，“舒特V”系统重点演示了识别和定位敌C3系统的能力，能够融合多个情报源以生成通用作战视图，并利用联合数据网络态势图(JSTAB)向战术、作战和战略领导者提供态势感知数据，并在综合电子监视设施、网络中心目标瞄准(NCCT)和网络空间设施等支持下，干扰、瘫痪敌方信息网络。据报道，在JEFX-2008演习中，除了EC-130H、RC-135V／W飞

机外，EA-6B和EA-18G电子战飞机也参加了演习。

总的来说，与传统的电子战不同，“舒特”攻击系统综合利用电磁频谱域和网络域的综合攻击能力，应用更复杂算法攻击敌人防御网络，能够入侵敌防空雷达网和防空通信网络，具有突出的情报、监视和侦察综合能力及空间和信息利用能力。“舒特”系统通过多架装有网络中心协同目标瞄准定位的有／无人监视飞机的数据融合，可实现数秒内对目标辐射源高精度定位和识别，并在数分钟内，通过多平台通用数据链被传送到武器或地面引导站，对敌综合防空系统干扰、欺骗、控制和硬摧毁能力。

三、侦网电火一体的“舒特”攻击技术

由于任何网络、尤其是无线网络都存在薄弱环节，渗入敌防空系统网络的可能途径有通过传感器、通信系统、通信链路、中继链路、信息处理设备和网络节点等。就防空雷达网络而言，国外公开报道的进入途径就有多种。例如，使用辐射信号直接进入敌方雷达接收机；通过敌指挥中心和雷达或武器平台之间的通信链路，特别是无线通信链路进入其防空雷达网络；还可通过敌防空雷达网络中的信息处理设备进入。

“舒特”正是利用这个原理实施网络攻击的，它以敌方电子信息系统的雷达、通信系统的天线为人口，渗透进入敌方的防空网，实施网络攻击。装备“舒特”能力的飞机至少要加装“长矛”(spear)吊舱(一种功率强大的专用辐射源阵列)和“豹穴”等实施网络入侵的算法／程序。这样，实施攻击时，就可以通过“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，植入不同的软件算法。进入敌防空网后，操作人员就可以通过屏幕图像实时监视敌方雷达，并根据具体情况采取以下措施：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”对方的系统；追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。

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。其攻击过程如下：第一步，对目标实施电子侦察，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，及时掌握敌防空体系的无线电联络内容。如遇到不能实时破译的密码，可以立即通过全球信息系统送到美国国家安全局，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。第二步，根据作战日的选择攻击方式。“舒特”攻击系统可选择的攻击方式有三种。第一种方式是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；第二种方式是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反辐射攻击或精确火力打击；第三种方式是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“舒特”网络攻击。当地面指控中心决定以EC－130H专用电于战飞机对预定目标实施网络战攻击时，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(Nccr)，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”或能量淹没敌人的电子设备，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。故此，在“舒特”攻击下，叙利亚先进的俄制防空系统没能及时发现和拦截入侵的以色列空军也就不足为奇了。

从技术上讲，“舒特”攻击实际上是一种集战场侦察、电子干扰、网络攻击、精确打击于一体的综合性进攻技术。它是美国空军在网络中心战思想指导下，正在大力发展的侦察打击一体化作战系统的新模式。

四、俄制防空系统面临美军及其盟国的严峻挑战

目前，美军已有部分EC-130H电子战飞机、RC-135电子侦察飞机、F-16CJ战斗机以及无人机装备了“舒特”攻击系统，美国海军EA-18G新型电子战飞机也计划装备该系统。“舒特”攻击系统集战场侦察、电子干扰、精确打击和网络攻击于一体，对防空雷达网络实施无线攻击的独特作战方式，不仅使无线网络入侵攻击即将成为现实，而且也让多种军用信息网络面临新的挑战与威胁。 特别是以色列空军运用美军研发的“舒特”攻击系统偷袭叙利亚“核目标”的成功军事行动，说明美军及其盟国已经找到了俄制防空系统的“软肋”。笔者揣测，“舒特”攻击可怕之处在于这套系统及相关技术正是针对俄制防空武器系统研制，或者可以说是为其量身打造。十几年前，前苏联和华约体系的解体，为美国获得了大量了解前苏联防空武器系统的机会，美国不仅没有浪费这些机会，还持续拓展出新的途径将信息触角全面伸进了新发展的俄制防空武器系统中。利用的手段包括：从“民主化”的东欧国家直接购买先进俄制防空武器，研究其核心芯片并将这些武器用于“红旗”等研究性对抗演习；通过与配备先进俄制防空武器的国家如印度进行联合演习，充分了解它们的战技术性能。

购买装备俄制防空武器的国家要应对这一挑战，应切实加强网络化装备系统／体系的网络对抗(防御)能力。随着武器装备网络化的发展，像“舒特”这样的进攻性信息战手段的威胁将是致命的。因此，无论是机动的防空武器系统，还是指挥系统、通信系统及至装备体系，都必须进一步提高网络对抗(防御)能力。除了要提高雷达、电台等单个武器装备的生存、对抗能力外，更应采取安全性更高的联网技术，提高网络的攻击检测能力和快速恢复能力等。